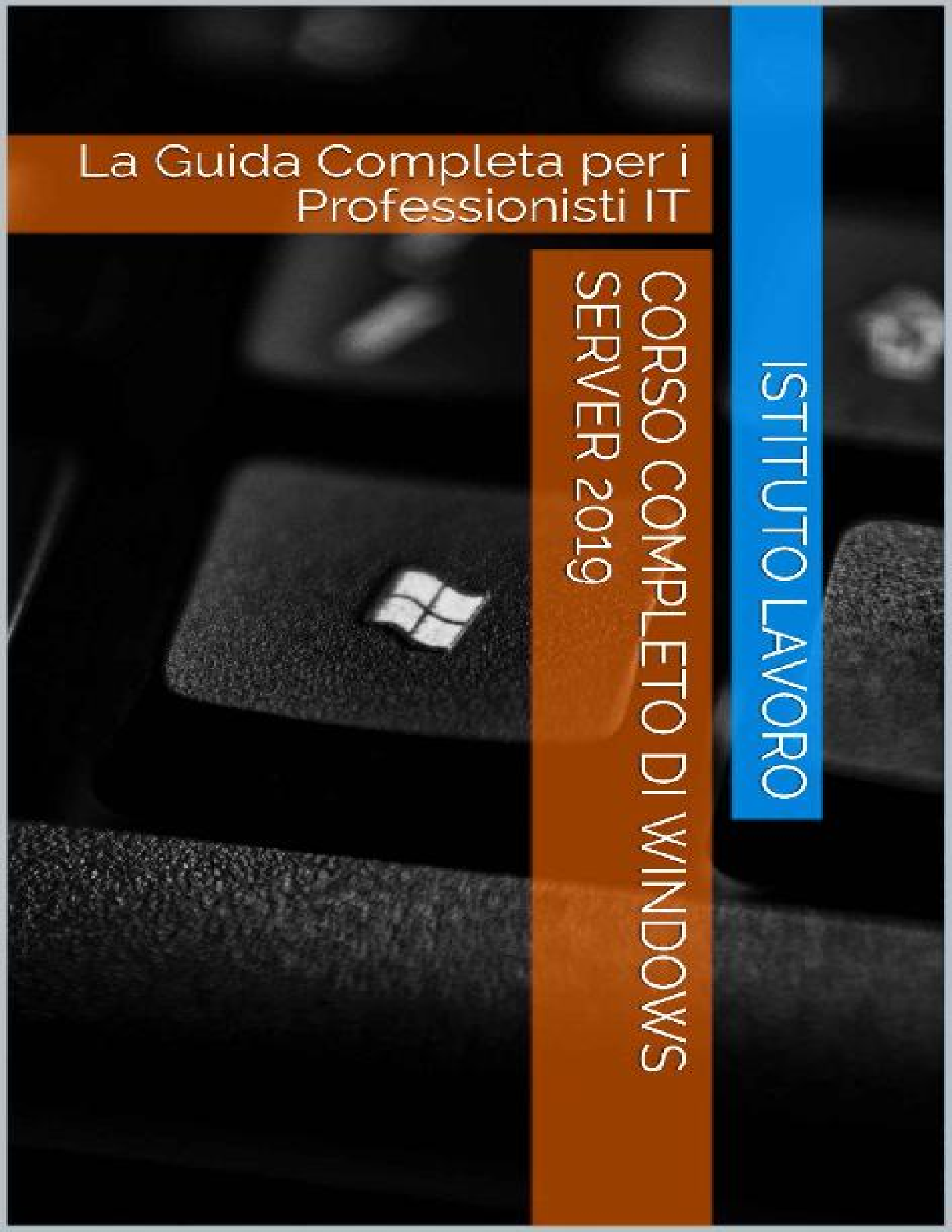
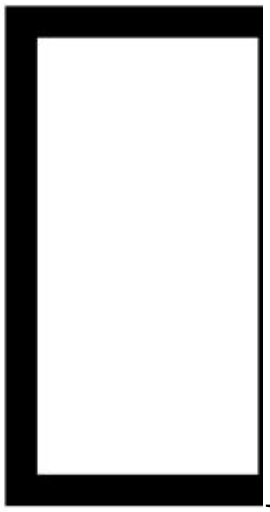

La Guida Completa per i Professionisti IT
CORSO COMPLETO DI WINDOWS SERVER 2019
ISTITUTO LAVORO

Corso Completo di Windows Server 2019

La guida completa per i professionisti IT:
- Installare e Gestire Windows Server 2019
- Distribuisci Nuove Funzionalit à

Sommario



Introduzione a Windows Server 2019

Circa 10 anni fa, Microsoft ha modificato la propria ideologia di rilascio del sistema operativo in modo che l'ultimo sistema operativo Windows Server sia sempre strutturato in modo molto simile al più recente sistema operativo client Windows. Questa è stata la tendenza da un po 'di tempo, con Server 2008 R2 che riflette da vicino Windows 7, Server 2012 che si sente molto simile a Windows 8 e molte delle stesse funzionalità di usabilità fornite con l'aggiornamento di Windows 8.1 sono incluse anche con Server 2012 R2. Questo, ovviamente, è stato trasferito anche a Server 2016, dandogli lo stesso aspetto e aspetto come se fossi connesso a una workstation Windows 10.

Ora che tutti abbiamo familiarità e ci sentiamo a nostro agio con l'interfaccia di Windows 10, in genere non abbiamo problemi a saltare direttamente all'interfaccia di Server 2016 e a fare un giro di prova.

Windows Server 2019 non fa ancora una volta eccezione a questa regola, tranne per il fatto che il rilascio dei sistemi operativi lato client è leggermente spostato. Ora, invece di rilasciare nuove versioni di Windows (11, 12, 13 e così via), per il momento stiamo semplicemente attenendoci a Windows 10 e fornendogli numeri di sotto-versione, indicativi delle date in cui quel sistema operativo è stato rilasciato. Ad esempio, la versione 1703 di Windows 10 è stata rilasciata intorno a marzo del 2017. La versione 1709 di Windows 10 è stata rilasciata a settembre del 2017. Quindi, abbiamo avuto anche il 1803 e il 1809, sebbene il 1809 sia stato leggermente ritardato e non sia stato rilasciato fino a un punto più vicino a Novembre, ma non era il piano originale. Il piano attuale prevede che il sistema operativo Windows venga rilasciato ogni sei mesi circa, ma aspettarsi che i reparti IT sollevino e spostino tutti i loro server solo allo scopo di passare a un sistema operativo più recente di sei mesi è pazzesco; a volte ci vuole più tempo solo per pianificare una migrazione.

Ad ogni modo, sto andando un po 'avanti con me stesso, poiché parleremo del controllo delle versioni di Windows Server più avanti in questo capitolo, durante le nostre versioni di Windows Server e la sezione delle licenze. Il punto qui è che Windows Server 2019 sembra e si sente come l'ultima versione del sistema operativo client Windows rilasciata all'incirca nello stesso periodo, ovvero Windows 10 1809. Prima di iniziare a parlare delle funzionalità di Windows Server, È importante stabilire una linea di base per l'usabilità e la familiarità del sistema operativo stesso prima di immergersi più a fondo nelle tecnologie in esecuzione sotto il cofano.

Dedichiamo alcuni minuti ad esplorare la nuova interfaccia grafica e le opzioni disponibili per orientarti in questa ultima versione di Windows Server, al fine di coprire i seguenti argomenti in questo capitolo:

- Lo scopo di Windows Server Sta diventando nuvoloso là fuori
- Versioni e licenze di Windows Server Panoramica delle funzionalità nuove e aggiornate Navigazione nell'interfaccia
- Utilizzando la nuova schermata Impostazioni Task Manager
- Visualizzazione attività

Lo scopo di Windows Server

Chiedersi qual è lo scopo di Windows Server è una domanda sciocca? Non credo proprio. È una buona domanda su cui riflettere, soprattutto ora che la definizione di server e carichi di lavoro del server cambia regolarmente. La risposta a questa domanda per i client Windows è più semplice. Un computer client Windows è un richiedente, consumatore e contributore di dati.

Da dove vengono spinti e estratti questi dati? Cosa consente ai meccanismi e alle applicazioni in esecuzione sui sistemi operativi client di interfacciarsi con questi dati? Cosa protegge questi utenti e i loro dati? Le risposte a queste domande rivelano lo scopo dei server in generale. Ospitano, proteggono e forniscono i dati che devono essere utilizzati dai clienti.

Tutto ruota intorno ai dati nel mondo degli affari di oggi. La nostra posta elettronica, documenti, database, elenchi di clienti: tutto ciò di cui abbiamo bisogno per lavorare bene sono i dati. Questi dati sono fondamentali per noi. I server sono ciò che utilizziamo per costruire il tessuto su cui confidiamo che i nostri dati risiedano.

Tradizionalmente pensiamo ai server che utilizzano una mentalità dell'interfaccia client-server. Un utente apre un programma sul proprio computer client, questo programma si rivolge a un server per recuperare qualcosa e il server risponde secondo necessità. Questa idea può essere applicata correttamente a quasi tutte le transazioni che potresti avere con un server. Quando il computer che fa parte del dominio deve autenticarti come utente, contatta Active Directory sul server per convalidare le tue credenziali e ottenere un token di autenticazione. Quando devi contattare una risorsa per nome, il tuo computer chiede a un server DNS come arrivarci. Se devi aprire un file, chiedi al file server di inviarlo a modo tuo.

I server sono progettati per essere il cervello delle nostre operazioni e spesso in modo trasparente. Negli ultimi anni sono stati compiuti passi da gigante per garantire che le risorse siano sempre disponibili e accessibili in modi che non richiedono formazione o un grande sforzo da parte dei nostri dipendenti.

Nella maggior parte delle organizzazioni, sono necessari molti server diversi per fornire alla tua forza lavoro le capacità di cui ha bisogno. Ogni servizio all'interno di Windows Server viene fornito come o come parte di un ruolo. Quando parli della necessità di nuovi server o della configurazione di un nuovo server per un'attività particolare, ciò a cui ti riferisci veramente è il ruolo o i ruoli individuali che verranno configurati su quel server per portare a termine il lavoro. Un server senza ruoli installati è inutile, anche se a seconda dello chassis può essere un ottimo fermacarte. Un dispositivo SAN 3U potrebbe pesare fino a 100 libbre e mantenere la tua scrivania ordinata anche nel mezzo di un uragano!

Se pensi ai ruoli come la carne e le patate di un server, la parte successiva che discuteremo è un po 'come l'aggiunta di sale e pepe. Oltre ai ruoli generali che installerai e configurerai sui tuoi server, Windows contiene anche molte funzionalità che possono essere installate, che a volte sono autonome, ma più spesso completano ruoli specifici nel sistema operativo. Le funzionalità possono essere qualcosa che completa e aggiunge funzionalità al sistema operativo di base come Telnet Client, oppure una funzionalità può essere aggiunta a un server per migliorare un ruolo esistente, come l'aggiunta della funzionalità di bilanciamento del carico di rete a un telecomando già dotato accesso o server IIS. La combinazione di ruoli e funzionalità all'interno di Windows Server è ciò che consente a quel pezzo di metallo di funzionare.

Questo libro, ovviamente, si concentrerà su un'infrastruttura incentrata su Microsoft. In questi ambienti, il sistema operativo Windows Server è il re ed è prevalente in tutti gli aspetti della tecnologia. Esistono alternative a Windows Server e diversi prodotti in grado di fornire alcune delle stesse funzioni a un'organizzazione, ma è abbastanza raro trovare un ambiente aziendale ovunque in esecuzione senza alcuna parvenza di infrastruttura Microsoft.

Windows Server contiene un'incredibile quantità di tecnologia, il tutto racchiuso in un piccolo disco di installazione. Con Windows Server 2019, Microsoft ci ha fatto pensare fuori dagli schemi a cosa significhi essere un server in primo luogo e viene fornito con alcune nuove entusiasmanti funzionalità che passeremo un po 'di tempo a coprire in queste pagine. Cose come PowerShell, Windows Admin Center e Storage Spaces Direct stanno cambiando il modo in cui gestiamo e dimensioniamo i nostri ambienti di elaborazione; questi sono tempi entusiasmanti per essere o diventare un amministratore di server!

Sta diventando nuvoloso là fuori

C'è questo nuovo termine là fuori, potresti anche averne sentito parlare ... cloud. Mentre la parola "cloud" si è certamente trasformata in una parola d'ordine che viene spesso utilizzata in modo improprio e di cui si parla in modo inappropriato, l'idea di infrastruttura cloud è incredibilmente potente. Un cloud fabric è quello che ruota attorno alle risorse virtuali: macchine virtuali, dischi virtuali e persino reti virtuali. Essere collegati al cloud in genere consente cose come la capacità di avviare nuovi server per capriccio, o anche la capacità per determinati servizi stessi di aumentare o diminuire automaticamente le risorse necessarie, in base all'utilizzo.

Pensa a un semplice sito di e-commerce in cui un consumatore può andare per ordinare merci. Forse il 75% dell'anno, possono gestire questo sito Web su un singolo server Web con risorse limitate, con un costo del servizio piuttosto basso. Tuttavia, il restante 25% dell'anno, forse durante le festività natalizie, l'utilizzo aumenta notevolmente, richiedendo molta più potenza di calcolo. Prima della mentalità cloud, ciò significherebbe che l'azienda avrebbe dovuto ridimensionare il proprio ambiente per soddisfare i requisiti massimi in ogni momento, nel caso in cui fosse mai necessario. Avrebbero pagato più server e molta più potenza di calcolo di quanto fosse necessario per la maggior parte dell'anno. Con un tessuto cloud, dando al sito Web la possibilità di aumentare o diminuire il numero di server a sua disposizione secondo necessità, il costo totale di tale sito Web o servizio può essere drasticamente ridotto.

Cloud pubblico

Il più delle volte, quando la tua vicina Suzzi Knowitall ti parla del cloud, parla semplicemente di Internet. Bene, più precisamente sta parlando di un servizio che usa, a cui si connette usando Internet. Ad esempio, Office 365, Google Drive, OneDrive, Dropbox: sono tutte risorse del cloud pubblico, poiché memorizzano i tuoi dati nel cloud. In realtà, i tuoi dati si trovano solo su server a cui accedi tramite Internet, ma non puoi

vedere quei server e non devi amministrare e mantenere quei server, motivo per cui sembra magico e viene quindi indicato come la nuvola.

Per i reparti IT, il termine "cloud" indica più spesso uno dei tre grandi provider di cloud hosting. Dal momento che questo è un libro guidato da Microsoft, e dato che mi sento davvero così, Azure è di prim'ordine in questa categoria. Azure stesso è un altro argomento per un altro (o molti altri) libro, ma è un'architettura di elaborazione cloud centralizzata che può ospitare i tuoi dati, i tuoi servizi o anche l'intera rete di server.

Spostare il tuo data center in Azure ti consente di smettere di preoccuparti o preoccuparti dell'hardware del server, sostituire i dischi rigidi e molto altro ancora. Piuttosto che acquistare server, rimuoverli dalla confezione, installarli su rack, installare Windows su di essi e quindi impostare i ruoli che si desidera configurare, è sufficiente fare clic su alcuni pulsanti per avviare nuovi server virtuali che possono essere ridimensionati in qualsiasi momento per la crescita. Quindi paghi costi op-ex più piccoli per questi server: canoni mensili o annuali per l'esecuzione di sistemi all'interno del cloud, piuttosto che i grandi costi di cap-ex per l'hardware del server in primo luogo.

Altri fornitori di cloud con funzionalità simili sono numerosi, ma i tre grandi sono Azure, Amazon (AWS) e Google. Per quanto riguarda le imprese, Azure prende semplicemente la torta e la mangia anche lei. Non sono sicuro che gli altri saranno mai in grado di mettersi al passo con tutte le modifiche e gli aggiornamenti che Microsoft apporta costantemente all'infrastruttura di Azure.

Cloud privato

Mentre la maggior parte delle persone che lavorano nel settore IT in questi giorni ha una comprensione abbastanza buona di cosa significhi far parte di un servizio cloud, e molti lo fanno davvero oggi, un termine che viene introdotto nelle aziende ovunque ed è ancora molte volte frainteso è un cloud privato. All'inizio, ho pensato che fosse uno sciocco stratagemma di marketing, un grossolano uso improprio del termine "cloud" per cercare di attirare coloro che sono agganciati dalle parole d'ordine. Ragazzo mi sbagliavo. Agli albori dei cloud privati, la tecnologia non era ancora pronta per resistere a ciò che veniva pubblicizzato.

Oggi, tuttavia, quella storia è cambiata. Ora è del tutto possibile prendere lo stesso fabric che è in esecuzione nel vero cloud pubblico e installarlo direttamente all'interno del tuo data center. Ciò ti consente di fornire alla tua azienda i vantaggi del cloud come la capacità di aumentare e

diminuire le risorse, di eseguire tutto virtualizzato e di implementare tutti i suggerimenti e i trucchi accurati degli ambienti cloud, con tutta la potenza di servizio e l'archiviazione dei dati rimanendo di proprietà locale e protetto da te. Affidarsi alle società di cloud storage per mantenere i dati al sicuro e protetti è in assoluto uno dei maggiori ostacoli all'implementazione sul vero cloud pubblico, ma, installando il proprio cloud privato, si ottiene il meglio di entrambi i mondi, in particolare ambienti di elaborazione estensibili con la sicurezza di sapendo che controlli e possiedi ancora tutti i tuoi dati.

Questo non è un libro sulle nuvole, pubbliche o private. Lo menziono per fornire una linea di base per alcuni degli elementi che discuteremo nei capitoli successivi, e anche per far venire l'acquolina in bocca un po 'per approfondire e leggere un po' sulla tecnologia cloud. Vedrai l'interfaccia di Windows Server 2019 in molti nuovi modi con il cloud e noterai che molti dei sistemi sottostanti disponibili in Server 2019 sono simili, se non uguali, a quelli che diventano disponibili all'interno di Microsoft Azure.

In queste pagine, non ci concentreremo sulle funzionalità di Azure, ma piuttosto su un senso più tradizionale di Windows Server che verrebbe utilizzato in sede. Con la grande spinta verso le tecnologie cloud, è facile rimanere scoperti con i paraocchi e pensare che tutto e tutti stiano rapidamente correndo verso il cloud per tutte le loro esigenze tecnologiche, ma semplicemente non è vero. La maggior parte delle aziende avrà bisogno di molti server in sede per molti anni a venire; in effetti, molti potrebbero non riporre mai la piena fiducia nel cloud e manterranno per sempre i propri data center. Questi data center avranno server locali che richiederanno agli amministratori di server di gestirli. È qui che entri in gioco tu.

Versioni e licenze di Windows Server

Chiunque abbia lavorato alla progettazione o all'installazione di un server Windows negli ultimi anni si starà probabilmente chiedendo quale direzione stiamo prendendo all'interno di questo libro. Vedete, ci sono diverse edizioni di funzionalità, diverse versioni tecniche e diversi modelli di licenza di Windows Server. Dedichiamo alcuni minuti per coprire queste differenze in modo che possiate avere una conoscenza completa delle diverse opzioni e in modo da poter definire quali parti intendiamo discutere nel corso di questo libro.

Standard contro Datacenter

Quando si installa il sistema operativo Windows Server 2019 su un componente hardware, come si verificherà in capitolo 2, Installando e gestendo Windows Server 2019, avrai due diverse scelte sulla capacità del server. Il primo è Server 2019 Standard, che è l'opzione predefinita e che include la maggior parte dei ruoli di Windows Server tradizionali. Anche se non posso fornirti dettagli sui prezzi perché potrebbe essere potenzialmente diverso per ogni azienda a seconda degli accordi con Microsoft, Standard è l'opzione più economica ed è utilizzata più comunemente per le installazioni di Windows Server 2019.

Datacenter, d'altra parte, è il modello di lusso. Esistono alcuni ruoli e funzionalità all'interno di Windows Server 2019 che funzionano solo con la versione Datacenter del sistema operativo e non sono disponibili all'interno di Standard. Se mai stai cercando un nuovo pezzo di tecnologia Microsoft per servire a uno scopo nel tuo ambiente, assicurati di controllare i requisiti per scoprire se dovrai costruire un server Datacenter. Tieni presente che Datacenter può costare molto di più rispetto a Standard, quindi generalmente lo usi solo nei luoghi in cui è effettivamente richiesto. Ad esempio, se sei interessato a ospitare VM schermate o lavorare con Spazi di archiviazione diretta, ti verrà richiesto di eseguire l'edizione Server 2019 Datacenter sui server correlati a tali tecnologie.

Una delle maggiori differenze funzionali tra Standard e Datacenter è il numero di macchine virtuali (VM) che possono ospitare. Server 2019 Standard può eseguire solo due VM su di esso in un dato momento, il che è un fattore piuttosto limitante se stavi cercando di creare un server Hyper-V. Datacenter ti consente di eseguire un numero illimitato di VM, il che lo rende un gioco da ragazzi durante la creazione dei tuoi server host di virtualizzazione. Per eseguire Hyper-V, Datacenter è la strada da percorrere.

Esperienza desktop / Server Core / Nano Server

Successivamente ci sono le diverse impronte e interfacce utente che puoi eseguire sui tuoi computer Windows Server 2019. Esistono tre diverse versioni di Windows Server che possono essere utilizzate e quella giusta per te dipende dalle funzionalità e dalla sicurezza che stai cercando.

Esperienza desktop

Questa è la scelta più comune tra i server Windows ovunque. Che tu stia creando un Windows Server 2019 Standard o Datacenter, puoi scegliere di eseguire Server con o senza un'interfaccia utente grafica. L'aspetto tradizionale, l'interfaccia punta e clicca è chiamata Esperienza desktop. Ciò consente cose come RDP nei tuoi server, avere un desktop tradizionale, essere in grado di utilizzare il Server Manager grafico direttamente dal tuo server connesso, e tutto sommato è il modo migliore se sei nuovo nell'amministrazione del server.

Se hai familiarità con la navigazione all'interno di Windows 10, dovresti essere in grado di spostarti almeno in Windows Server 2019 con Esperienza desktop. Questa è la versione di Windows Server 2019 su cui ci concentreremo per la maggior parte di questo libro e quasi tutti gli screenshot saranno presi da un ambiente Desktop Experience.

Server Core

Come vedrai quando installiamo Windows Server 2019 insieme, l'opzione predefinita per l'installazione non è Esperienza desktop. Ciò significa che la scelta del percorso di installazione predefinito collocherebbe invece una versione headless di Windows Server sulla macchina, più comunemente denominata Server Core. La natura dell'headless rende Server Core più veloce ed efficiente della versione desktop, il che ha senso perché non deve eseguire tutto quel codice extra e consumare tutte quelle risorse extra per l'avvio e la visualizzazione di un'enorme interfaccia grafica.

Quasi tutto ciò che vuoi fare in Windows Server è possibile farlo su Server Core o Desktop Experience, le differenze principali sono l'interfaccia e la sicurezza. Per poter utilizzare Server Core, devi assolutamente essere a tuo agio con un'interfaccia della riga di comando (ovvero PowerShell) e devi anche considerare la gestione del server remoto come un modo affidabile di interagire con i tuoi server. Parleremo molto di più di Server Core inCapitolo 8, Server Core.

Il più grande vantaggio offerto da Server Core, oltre alle prestazioni, è la sicurezza. La maggior parte del malware che tenta di attaccare i server Windows dipende da elementi presenti all'interno della GUI di Desktop Experience. Dal momento che queste cose non sono nemmeno in esecuzione all'interno di Server Core - purtroppo, non potresti arrivare a un desktop anche se lo volessi - gli attacchi contro le macchine Server Core hanno molto, molto meno successo.

Nano Server

Esiste una terza piattaforma per Windows Server 2019, nota come Nano Server. Questa è una versione minuscola di Windows Server, headless come Server Core ma con un'impronta ancora più piccola. L'ultima volta che ho avviato un Nano Server, ha consumato meno di 500 MB di dati per l'intero sistema operativo, il che è incredibile.

Sembrava che Nano Server fosse discusso molto di più riguardo al rilascio di Server 2016, perché a quel tempo Microsoft stava spingendo avanti con i piani per includere un intero gruppo di ruoli all'interno di Nano Server in modo da poter iniziare a sostituire alcuni dei nostri server quotidiani gonfiati e sovradimensionati con Nano, ma da allora quella mentalità è andata nel dimenticatoio.

Al momento della stesura di questo documento, Nano Server è abbastanza ben sposato con l'uso dei contenitori. In effetti, credo che l'unico modo supportato per eseguire Nano Server in questo momento sia eseguirlo come immagine all'interno di un contenitore. Discuteremo entrambi in modo più dettagliato all'internoCapitolo 11, Containers e Nano Server, ma, ai

fini di questo riepilogo, è sicuro affermare che, se sai cosa sono i container e sei interessato a usarli, trarrai vantaggio dall'imparare tutto ciò che c'è da sapere su Nano Server . Se non sei in grado di lavorare con i container, probabilmente non ti imbatterai mai in Nano Server nel tuo ambiente.

Modelli di licenza: SAC e LTSC

Un'altra decisione su come configurare i server Windows è il modello di licenza / supporto e la cadenza di rilascio che desideri seguire. Ci sono due diversi percorsi che puoi intraprendere. È possibile avere un mix di questi in un unico ambiente, se ne hai bisogno di entrambi.

Canale semestrale (SAC)

Se si sceglie di eseguire le versioni SAC di Windows Server, la convenzione di denominazione per il sistema operativo cambia. Invece di chiamarlo Server 2019, stai davvero eseguendo Windows Server 1803, 1809 e così via. Segue la stessa mentalità di Windows 10. Ciò implica che queste nuove versioni di Windows Server SAC vengono rilasciate a intervalli molto più brevi di quelli che abbiamo mai visto per i server in passato. Il canale SAC dovrebbe ricevere due importanti pubblicazioni ogni anno, generalmente in primavera e in autunno. A causa della rapida cadenza di rilascio, il supporto per le versioni SAC di Windows Server dura per un breve periodo di 18 mesi. Se usi SAC, faresti meglio ad abituarti a saltare sempre all'ultima versione subito dopo il rilascio.

Se sostituire i sistemi operativi del server due volte all'anno sembra scoraggiante, non sei il solo. Per fortuna, Microsoft lo riconosce e si rende conto che la popolazione di amministratori di server generali non utilizzerà questo modello per i loro server regolari e quotidiani. Piuttosto, le versioni SAC di Windows Server verranno utilizzate solo per l'esecuzione di contenitori. In questo nuovo mondo di hosting di applicazioni flessibile, in cui le applicazioni vengono scritte in modo tale che le risorse dell'infrastruttura alla base di tali applicazioni possano essere attivate o ridotte secondo necessità, i contenitori sono un pezzo molto importante di quel puzzle DevOps. Se ospiti o crei questo tipo di applicazioni, quasi certamente utilizzerai i contenitori, ora o in futuro. Quando ti trovi nella posizione di ricercare e capire i contenitori,

Canale di manutenzione a lungo termine (LTSC)

Alcuni di voi probabilmente pensano che LTSC sia un errore di battitura, poiché negli anni precedenti questo modello era chiamato Long-Term Servicing Branch (LTSB). Mentre puoi andare con entrambi e le persone generalmente sapranno di cosa stai parlando, LTSC è ora il termine corretto.

Windows Server 2019 è una versione LTSC. In sostanza, le versioni LTSC sono quelle che abbiamo sempre considerato le nostre versioni tradizionali del sistema operativo Windows Server. Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, Server 2016 e ora Server 2019 sono tutte versioni di LTSC. Ciò che è cambiato è che le versioni di LTSC ora arriveranno con meno cose che sono wow, è così fantastico e nuovo di zecca, perché vedremo e riceveremo suggerimenti su quelle cose nuove di zecca man mano che vengono create e implementate in un altro moda a breve termine attraverso le versioni SAC. Quindi, le tue versioni SAC usciranno all'incirca ogni sei mesi, e poi ogni due o tre anni sperimenteremo una nuova versione LTSC che include tutte queste modifiche.

Mentre SAC è generalmente incentrato su DevOps e contenitori, i server LTSC sono per eseguire praticamente tutto il resto. Non vorresti installare un controller di dominio, un server dei certificati o un file server e dovresti sostituire quel server ogni sei mesi. Quindi, per uno qualsiasi di questi scenari, guarderai sempre a LTSC.

Un'altra importante differenza tra i due è che, se si desidera utilizzare la versione Desktop Experience di Windows Server (con un'interfaccia grafica con cui interagire), si sta guardando LTSC. Le versioni SAC di Windows Server NON includono l'esperienza desktop: sei limitato solo a Server Core o Nano Server.

Con le versioni LTSC di Windows Server, continui a ricevere lo stesso supporto a cui siamo abituati: cinque anni di supporto mainstream seguiti da cinque anni di supporto esteso disponibile.

In questo libro lavoreremo e acquisiremo esperienza con Windows Server 2019 - versione LTSC.

Panoramica delle funzionalità nuove e aggiornate

La versione più recente del sistema operativo Windows Server è sempre un'evoluzione del suo predecessore. Ci sono certamente pezzi di tecnologia contenuti all'interno che sono nuovi di zecca, ma ci sono ancora più luoghi in cui le tecnologie esistenti sono state aggiornate per includere nuove caratteristiche e funzionalità. Dedichiamo alcuni minuti a fornire una panoramica di alcune delle nuove funzionalità presenti in Windows Server 2019.

L'esperienza con Windows 10 è continuata

Storicamente, una nuova versione di qualsiasi sistema operativo Microsoft ha significato l'apprendimento di una nuova interfaccia utente, ma Server 2019 è la prima eccezione a questa regola. Il rilascio di Windows 10 ci ha dato la prima occhiata all'attuale piattaforma grafica, che poi è stata introdotta in Windows Server 2016, ed è stata la prima volta che abbiamo visto l'interfaccia corrente su una piattaforma server. Ora che gli aggiornamenti di Windows 10 vengono rilasciati ma continuano essenzialmente con la stessa interfaccia desktop, lo stesso vale per Server 2019. L'accesso e l'utilizzo di Windows Server 2019 è, in molti modi, la stessa esperienza che hai avuto all'interno di Windows Server 2016. Anche così, alcuni che hanno letto questo libro non hanno mai sperimentato l'accesso a un server di alcun tipo prima d'ora, quindi esamineremo sicuramente quell'interfaccia e impareremo alcuni suggerimenti e trucchi per navigare in modo fluido ed efficiente all'interno di Server 2019.

Infrastruttura iperconvergente

Quando vedi la frase Hyper-Converged Infrastructure (HCI), è importante capire che non stiamo parlando di una tecnologia specifica che esiste all'interno del tuo ambiente server. Piuttosto, HCI è il culmine di una serie di tecnologie diverse che possono lavorare insieme ed essere gestite insieme, il tutto allo scopo di creare la mentalità di un data center definito dal software (SDDC come a volte viene chiamato). In particolare, HCI viene spesso definito come la combinazione di Hyper-V e Storage Spaces Direct (S2D) sullo stesso cluster di server. Il raggruppamento di questi servizi insieme consente alcuni grandi vantaggi in termini di velocità e affidabilità rispetto all'hosting di questi ruoli separatamente e sui propri sistemi.

Un altro componente che fa parte o è correlato a un data center definito dal software è il Software Defined Networking (SDN). Analogamente a come le piattaforme di virtualizzazione del calcolo (come Hyper-V) hanno cambiato completamente il panorama di come appariva il server computing circa dieci anni fa, ora ci troviamo in grado di sollevare il livello di rete dall'hardware fisico e spostare la progettazione e l'amministrazione delle nostre reti per essere virtuali e gestite dalla piattaforma Windows Server.

Un nuovo strumento disponibile che aiuta a configurare, gestire e mantenere i cluster nonché i cluster HCI è il nuovo Windows Admin Center (WAC). WAC può essere un hub da cui interfacciarsi con la tua infrastruttura iperconvergente.

Windows Admin Center

Finalmente rilasciato a titolo ufficiale, WAC è una delle cose più interessanti che abbia mai visto come parte della versione Server 2019. Si tratta di uno strumento gratuito, disponibile per tutti, che puoi utilizzare per iniziare a gestire centralmente la tua infrastruttura server. Sebbene non sia completamente in grado di sostituire tutti i tradizionali strumenti

di amministrazione della console PowerShell, RDP e MMC, ti consente di svolgere molte normali attività quotidiane con i tuoi server, il tutto da un'unica interfaccia.

Se questa capacità ti suona familiare, potrebbe essere perché hai testato qualcosa chiamato Project Honolulu ad un certo punto nell'ultimo anno. Sì, Windows Admin Center è Project Honolulu, ora in piena capacità di produzione.

Esamineremo più da vicino l'interfaccia di amministrazione di Windows nel Capitolo 2, Installazione e gestione di Windows Server 2019.

Protezione avanzata dalle minacce di Windows Defender

Se non hai letto nulla su Advanced Threat Protection (ATP), potresti vedere le parole Windows Defender e presumere che io stia semplicemente parlando delle funzionalità antivirus / anti-malware ora integrate anche nei sistemi operativi client Windows come server Windows a partire dal 2016. Anche se è vero che Windows Server 2019 viene fornito con antivirus integrato, il servizio ATP è molto, molto di più.

Ne discuteremo in modo più approfondito Capitolo 7, Protezione avanzata e sicurezza, ma il breve riepilogo è che Windows Defender Advanced Threat Protection è un servizio basato su cloud a cui puoi attingere le tue macchine. Il potere dell'ATP è che molte migliaia, o forse anche milioni, di dispositivi inviano dati e creano un enorme archivio di informazioni che può essere utilizzato con un po 'di intelligenza artificiale e apprendimento automatico per generare dati completi su nuove minacce, virus e intrusioni, in tempo reale. I clienti ATP ricevono quindi i vantaggi della protezione non appena si presentano queste nuove minacce. È quasi come funzionalità anti-minacce di crowdsourcing, con Azure che gestisce tutta l'elaborazione back-end.

Password vietate

Active Directory ha archiviato tutte le informazioni sui nostri account utente, comprese le password, per molti anni. Le ultime versioni del sistema operativo Windows Server non hanno incluso molti aggiornamenti o nuove funzionalità all'interno di AD, ma Microsoft sta ora lavorando con molti clienti all'interno del loro ambiente Azure AD basato su cloud e le nuove funzionalità vengono sempre lavorate nel cloud. Le password vietate sono una di quelle cose. Funzionalità nativamente di Azure AD, ora può essere sincronizzato di nuovo con i server del controller di dominio in sede, offrendoti la possibilità di creare un elenco di password che non possono essere utilizzate in alcun modo

dai tuoi utenti. Ad esempio, la parola password. Bandendo la password come password, si bandisce efficacemente qualsiasi password che includa la parola password. Ad esempio, P @ ssword, Password123! O qualsiasi altra cosa di simile portata.

Riavvio graduale

La possibilità di eseguire un riavvio graduale era in realtà nuova con Server 2016, ma doveva essere aggiunta manualmente in Server 2016 e non credo che nessuno abbia mai iniziato a usarlo. Negli ultimi tre anni, non ho mai visto una sola persona avviare un riavvio graduale, quindi presumo che non sia ben noto e lo includerò qui nel nostro elenco di funzionalità. Nel tentativo di accelerare i riavvii, è disponibile un interruttore di riavvio opzionale chiamato riavvio graduale, che ora è incluso automaticamente in Server 2019. Quindi, cos'è un riavvio graduale? È un riavvio senza inizializzazione hardware.

In altre parole, riavvia il sistema operativo senza riavviare l'intera macchina. Viene richiamato durante un riavvio aggiungendo un'opzione speciale al comando shutdown.
È interessante notare che in Server 2016 potresti anche richiamare un riavvio graduale con il cmdlet Restart-Computer in PowerShell, ma tale opzione sembra essere scomparsa in Server 2019. Quindi, se vuoi accelerare i tuoi riavvii, dovrai disattivare torna al buon vecchio prompt dei comandi, come mostrato di seguito:

- Tenere presente quanto segue utilizzando il comando shutdown:

  arresto / r / soft / t 0

Qui / r è per il riavvio, / soft è per il riavvio graduale e / t 0 è per zero secondi fino al riavvio inizia.

Integrazione con Linux

Eresia! Sotto la cui autorità ho digitato la parola Linux in un libro su Windows Server ?! Storicamente, gli ambienti informatici aziendali hanno eseguito Windows, o hanno eseguito Linux, o forse hanno eseguito entrambi, ma con una netta separazione tra i due. Windows Server 2019 offusca quella linea di separazione. Ora abbiamo la possibilità di eseguire VM Linux all'interno del nostro Microsoft Hyper-V e persino di essere in grado di interfacciarci correttamente con esse. Sapevi che alcuni sistemi

operativi Linux sanno effettivamente come interagire con un mouse? Prima d'ora, non avevi molte possibilità di farlo quando provavi a eseguire una VM basata su Linux su un server Windows, ma ora abbiamo una certa compatibilità implementata in Hyper-V.

I contenitori basati su Linux possono anche essere eseguiti su Server 2019, il che è un grosso problema per chiunque desideri implementare applicazioni di ridimensionamento tramite contenitori.

Puoi persino proteggere le tue macchine virtuali Linux crittografandole, attraverso l'uso di macchine virtuali schermate!

Macchine virtuali schermate avanzate

Così tante aziende oggi eseguono la maggior parte dei loro server come macchine virtuali. Uno dei grandi problemi con questo è che ci sono alcune falle di sicurezza intrinseche che esistono nelle piattaforme host di virtualizzazione di oggi. Uno di questi buchi è l'accesso backdoor ai file del disco rigido delle macchine virtuali. È abbastanza facile per chiunque disponga dei diritti di amministratore sull'host virtuale essere in grado di vedere, modificare o interrompere qualsiasi macchina virtuale in esecuzione all'interno di tale host. E queste modifiche possono essere apportate in modi quasi irrintracciabili. Dai un'occhiata all'internoCapitolo 12, Virtualizzazione del data center con Hyper-V, per scoprire in che modo la nuova capacità di creare macchine virtuali schermate chiude questa falla di sicurezza implementando la crittografia completa del disco su quei file VHD.

Server 2019 offre alcuni vantaggi specifici al mondo delle VM schermate: ora possiamo proteggere sia le macchine virtuali basate su Windows che quelle basate su Linux schermandole e non dipendiamo più dalla comunicazione con il servizio Host Guardian quando proviamo ad avviare VM protette dai nostri server host sorvegliati. Ne discuteremo ulteriormente inCapitolo 12, Virtualizzazione del data center con Hyper-V.

Scheda di rete di Azure

Cloud ibrido: non è fantastico quando puoi prendere due parole d'ordine separate e combinarle per creare una parola d'ordine ancora più grande e potente? Il cloud ibrido è l'oggetto dei sogni del CIO. Spero che tu sappia che sto scherzando su questo; l'idea del cloud ibrido è incredibilmente potente ed è il ponte che rende possibile l'utilizzo del cloud. Possiamo avere sia server in sede che server ospitati in Azure e rendere tutto un unico grande network felice in cui puoi accedere a qualsiasi risorsa da qualsiasi luogo.

Ora, esistono già una miriade di tecnologie che consentono di collegare la rete locale alla rete Azure, vale a dire VPN da sito a sito e Azure

Express Route. Tuttavia un'altra opzione non fa mai male, soprattutto per le piccole aziende che non vogliono la complessità della creazione di una VPN da sito a sito, né il costo di Express Route.

Immettere l'adattatore di rete di Azure. Questa nuova funzionalità consente di aggiungere molto rapidamente e facilmente una scheda di rete virtuale a un server Windows (anche una che risale al 2012 R2), quindi connettere quella scheda di rete virtuale direttamente alla rete di Azure! Windows Admin Center è necessario per l'esecuzione di questa transazione; daremo uno sguardo più da vicinoCapitolo 5, Collegamento in rete con Windows Server 2019.

Sempre su VPN

Gli utenti odiano avviare connessioni VPN. Lo so perché sento quel tipo di feedback ogni giorno. Dover stabilire manualmente una connessione alla propria rete di lavoro è una perdita di tempo che altrimenti potrebbero dedicare al lavoro effettivo. Nel Capitolo 6, Abilitazione della forza lavoro mobile, discuteremo delle diverse tecnologie di accesso remoto disponibili all'interno di Windows Server 2019. In realtà ci sono due diverse tecnologie che consentono una connessione completamente automatica alla rete aziendale, dove gli utenti non devono prendere alcun manuale azione per mettere in atto tali connessioni. Una di queste tecnologie è DirectAccess ed è disponibile da Server 2008 R2. Descriveremo in dettaglio DirectAccess perché è ancora un'opzione di connettività praticabile e popolare e tratteremo anche la versione più recente della connettività remota automatizzata: Always On VPN.

Navigare nell'interfaccia

Sfortunatamente, Microsoft ha respinto molte persone con l'introduzione di Windows 8 e Server 2012, non perché mancassero funzionalità o affidabilità, ma perché l'interfaccia era molto diversa da quella che era stata prima. Era quasi come eseguire due sistemi operativi separati contemporaneamente. Hai avuto la normale esperienza desktop, in cui tutti noi abbiamo trascorso il 99,9% del nostro tempo, ma poi ci sono stati anche quei pochi momenti in cui ti sei trovato a dover visitare il menu Start a pagina intera. Più probabilmente, ti sei imbattuto in esso senza volerlo. Comunque sei finito lì, all'interno di quell'interfaccia simile a un tablet a schermo intero, per il restante 0,01% della tua esperienza con Server 2012 sei rimasto confuso, disturbato e desiderando di essere tornato al desktop tradizionale. Naturalmente sto parlando solo per esperienza qui. Potrebbero esserci variazioni nelle tue percentuali personali di tempo trascorso, ma, in base alle conversazioni in cui sono stato coinvolto, non sono solo in queste opinioni. E non ho nemmeno menzionato la magica barra degli incantesimi autoapparente. È meglio lasciare alcuni brutti ricordi nei recessi del cervello.

Il principale aggiornamento di Windows 8.1 e Server 2012 R2 ha fornito un gradito sollievo a questi sintomi. C'era di nuovo un vero pulsante Start nell'angolo e si poteva scegliere di avviare principalmente nella normale modalità desktop. Tuttavia, se dovessi mai avere la necessità di fare clic su quel pulsante Start, ti ritroverai subito nella schermata Start a pagina intera, che trovo ancora quasi tutti gli amministratori di server che fanno del loro meglio per evitare a tutti i costi.

Bene, si scopre che Microsoft ha ascoltato e ha portato un po 'di sollievo tanto necessario in Windows 10 e Windows Server 2016. Anche se non del tutto tornato al tradizionale menu Start che esisteva nel 2008, abbiamo un buon mix di vecchi e nuovi modi di lanciare gli strumenti a cui dobbiamo accedere sulle nostre piattaforme server.

Per quanto riguarda l'interfaccia grafica, Windows Server 2019 è per lo più invariato rispetto a Server 2016, perché non abbiamo visto un aggiornamento importante dell'interfaccia sul sistema operativo client. Come già saprai, ogni nuova versione di Windows Server ha ricevuto aggiornamenti all'interfaccia punta e clicca in base a quello che è l'ultimo sistema operativo client Windows in quel momento, e questa è la prima volta in molti anni che un nuovo server è operativo Il sistema è stato rilasciato mentre il sistema operativo client è ancora in sospeso con la stessa versione: Windows 10. Se ti senti a tuo agio a navigare in Windows 10, sarai adatto a Windows Server 2019.

Per chiunque sia nuovo a lavorare in Windows o stia solo cercando alcuni suggerimenti e trucchi per iniziare, questa sezione è per te.

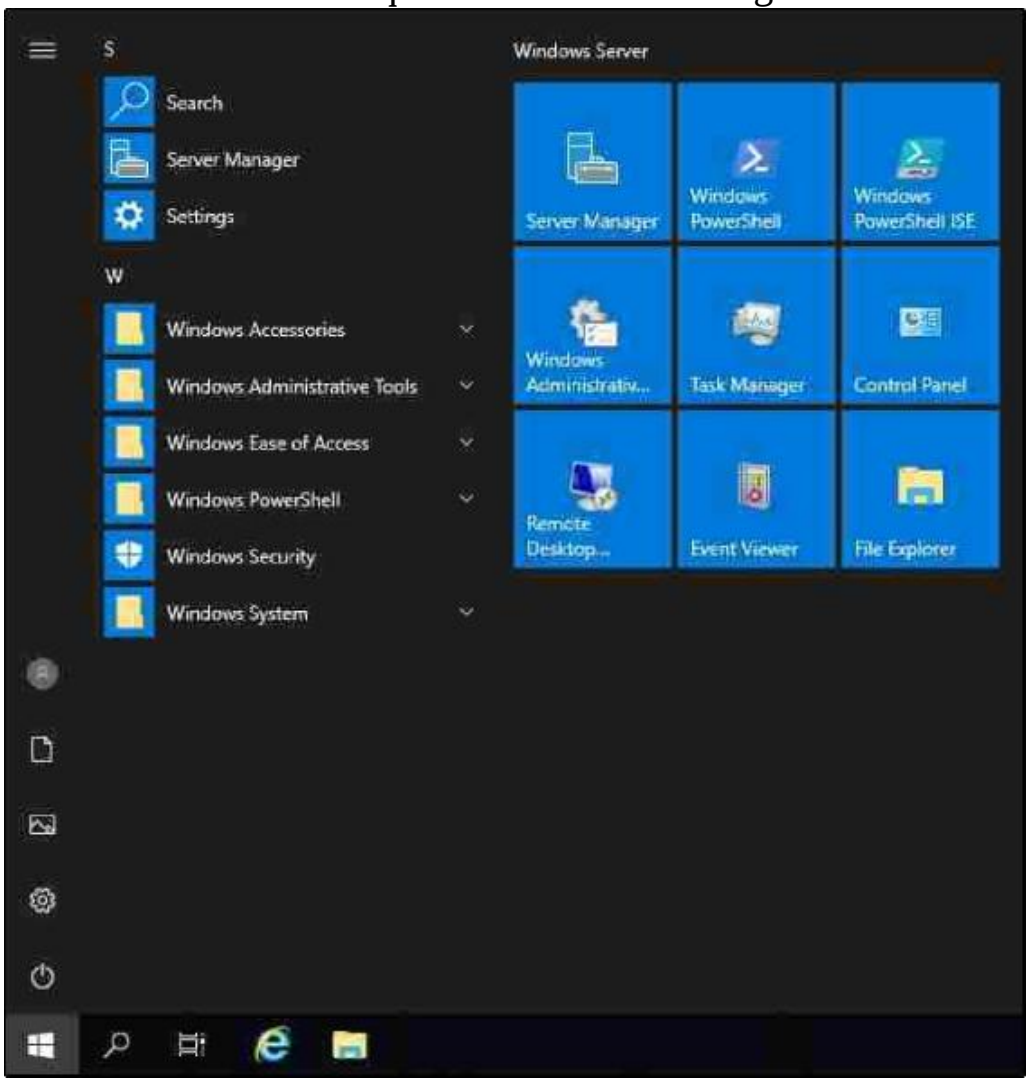
Il menu Start aggiornato

Poiché sono state rilasciate sotto-versioni di Windows 10, sono state apportate piccole modifiche in corso al menu Start. Tutto sommato, ritengo che molte delle modifiche stiano facendo marcia indietro rispetto al fiasco di Windows 8. Siamo ora tornati a un vero pulsante Start che lancia un vero menu Start, uno che non occupa l'intero desktop. Ad essere onesti, personalmente non apro quasi mai il menu Start, tranne che per cercare l'applicazione o la funzionalità che desidero. Ne parleremo di più molto presto. Tuttavia, quando apro il menu Start e lo guardo, ci sono alcune cose carine che risaltano.

- Tutte le applicazioni installate sul server sono elencate qui, in ordine alfabetico. Ciò è molto utile per avviare un'applicazione o per eseguire un rapido controllo per scoprire se una particolare app o funzionalità è installata o meno sul tuo server.
- Il lato sinistro del menu Start include alcuni pulsanti per l'accesso rapido agli elementi. Probabilmente i pulsanti più utili qui sono i controlli di alimentazione per spegnere o riavviare il server e l'ingranaggio Impostazioni che avvia le impostazioni di sistema.

- Per impostazione predefinita, il lato destro del menu Start mostra alcuni pulsanti più grandi, a volte chiamati live tile. Il blocco degli elementi da mostrare qui, ti offre una posizione di facile accesso per gli elementi che normalmente avvii sul tuo server e avere i pulsanti più grandi è utile quando controlli il tuo server da un laptop touchscreen o qualcosa di simile.

Puoi vedere tutte e tre queste funzioni nella seguente schermata:

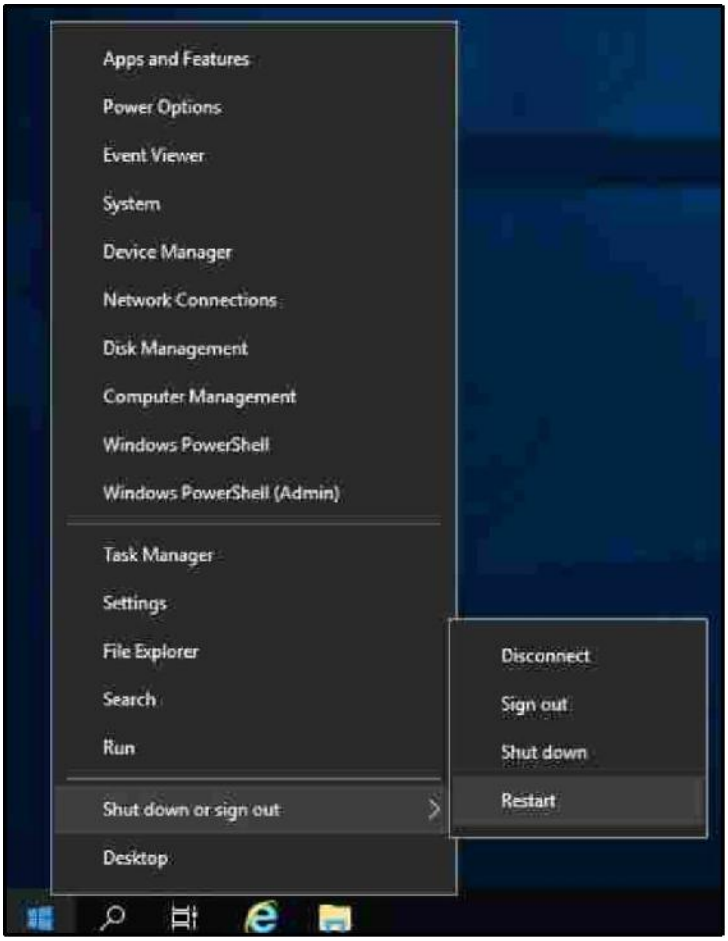


Questa è una boccata d'aria fresca. Un menu Start semplice ma utile e, cosa più importante, che si carica rapidamente tramite connessioni remote come console RDP o Hyper-V.

Il menu Attività amministrative rapide

Per quanto sia bello avere un menu di avvio funzionale, come amministratore del server mi trovo ancora molto raramente a dover accedere al menu tradizionale per le mie funzioni quotidiane. Questo perché molti elementi a cui devo accedere sono rapidamente disponibili nel menu delle attività rapide, che si apre semplicemente facendo clic con il pulsante destro del mouse sul pulsante Start. Questo menu è disponibile sin dal rilascio di Windows 8, ma molti professionisti IT non sono ancora a conoscenza di questa funzionalità. Questo menu è diventato una parte importante della mia interazione con i sistemi operativi Windows Server e spero che lo sia anche per te. Facendo clic con il pulsante destro del mouse sul pulsante Start ci vengono mostrati collegamenti rapidi immediati per eseguire operazioni come aprire il Visualizzatore eventi, visualizzare le proprietà del sistema, controllare Gestione dispositivi e persino Arresta o Riavvia il server. Le due funzioni più comuni che chiamo in questo menu contestuale sono la funzione Esegui e il suo utilizzo per avviare rapidamente un prompt di PowerShell. Ancora meglio è la possibilità da questo menu di aprire un prompt di PowerShell con contesto utente normale o un prompt di PowerShell con privilegi elevati / amministrativo. L'utilizzo corretto di questo menu consente di risparmiare molti clic del mouse e riduce i tempi di risoluzione dei problemi.

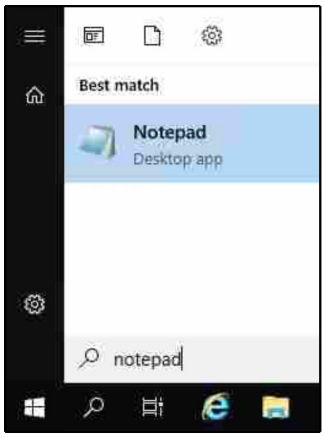
In alternativa, questo menu può essere richiamato utilizzando la scorciatoia da tastiera WinKey + X!



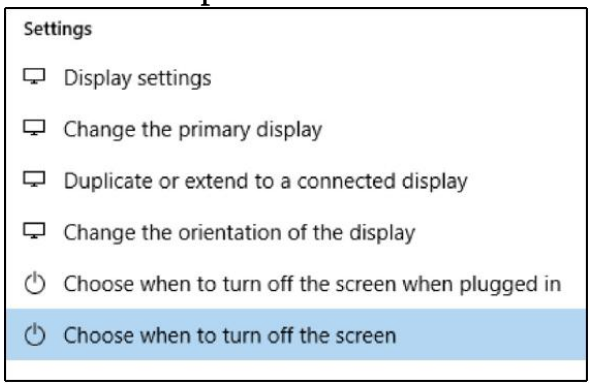
Utilizzo della funzione di ricerca

Mentre il menu Quick Admin nascosto dietro il pulsante Start è utile per chiamare attività amministrative comuni, l'utilizzo della funzione di ricerca all'interno del menu Start è un potente strumento per interfacciarsi letteralmente con qualsiasi cosa sul tuo Windows Server. A seconda di chi ha installato applicazioni e ruoli sui tuoi server, potresti o meno avere scorciatoie disponibili per avviarli nel menu Start. Potresti anche avere o meno collegamenti sul desktop o collegamenti per aprire questi programmi dalla barra delle applicazioni. Trovo che spesso sia difficile trovare impostazioni specifiche che potrebbero dover essere modificate per far funzionare i nostri server come vogliamo. Il pannello di controllo viene lentamente sostituito dal menu Impostazioni più recente nelle versioni più recenti di Windows, e talvolta questo rende difficile il rilevamento di impostazioni particolari. Tutti questi problemi vengono alleviati con la barra di ricerca all'interno del menu Start. Facendo semplicemente clic sul pulsante Start, o ancora più facilmente premendo il tasto Windows (WinKey) sulla tastiera, puoi semplicemente iniziare a digitare il nome di qualsiasi programma o impostazione o documento che desideri aprire. La barra di ricerca cercherà tutto sul tuo server locale e ti presenterà le opzioni per l'applicazione, l'impostazione o persino il documento da aprire.

Come esempio più semplice, premi WinKey sul tuo file tastiera, quindi digitare Blocco note e premere il tasto Invio. Vedrai che il buon vecchio Blocco note si apre per noi. Non abbiamo mai dovuto navigare da nessuna parte nella cartella Programmi per trovarla e aprirla. In effetti, non abbiamo mai nemmeno dovuto toccare il mouse, che è musica per le orecchie per uno come me che ama fare tutto ciò che può possibilmente tramite la tastiera:


Best match
Notepad
Desktop app
notepad

Un esempio ancora migliore è scegliere qualcosa che sarebbe sepolto abbastanza in profondità nelle Impostazioni o nel Pannello di controllo. Che ne dici di cambiare la quantità di tempo prima che lo schermo passi al risparmio energetico e si spenga? L'amministratore del server tradizionale aprirà il Pannello di controllo (se riesci a trovarlo), probabilmente naviga nella sezione Aspetto e personalizzazione perché nient'altro sembra ovviamente corretto e non trova ancora quello che stavano cercando. Dopo aver frugato in giro per qualche altro minuto, avrebbero iniziato a pensare che Microsoft avesse dimenticato di aggiungere del tutto questa impostazione. Ma ahimè, queste impostazioni di alimentazione vengono semplicemente spostate in un nuovo contenitore e non sono più accessibili tramite il Pannello di controllo. Discuteremo momentaneamente la nuova schermata Impostazioni in questo capitolo, ma alla fine per gli scopi di questo esempio sei attualmente bloccato nel punto in cui non riesci a trovare l'impostazione che desideri modificare. Qual è una soluzione rapida? Premi il tuo WinKey per aprire il menu Start e digita monitor (o power, o qualsiasi altra cosa che si riferisca all'impostazione che stai cercando). Nell'elenco delle opzioni disponibili viene visualizzato nel menu di ricerca quello chiamato Scegli quando spegnere lo schermo. Fai clic su questo e hai trovato l'impostazione che stavi cercando da sempre:

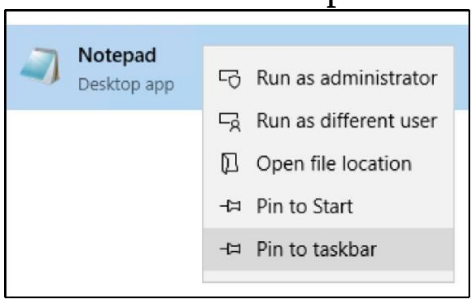


Noterai anche che hai molte più opzioni in questa schermata di ricerca rispetto a quelle che stavi cercando originariamente. La ricerca mi ha fornito molti elementi diversi che potevo realizzare, tutti relativi al monitor di parole che ho digitato. Non conosco un modo più potente per aprire applicazioni o impostazioni su Windows Server 2019 rispetto

all'utilizzo della barra di ricerca all'interno del Menu iniziale. Provalo oggi!

Blocco dei programmi sulla barra delle applicazioni

Mentre Windows Server 2019 offre ottime funzionalità di ricerca in modo che l'avvio di applicazioni difficili da trovare sia molto semplice, a volte è più facile avere scorciatoie veloci per gli elementi di uso comune da rendere disponibili con un solo clic, nella barra delle applicazioni tradizionale. Sia che tu abbia cercato una particolare applicazione navigando manualmente attraverso il menu Start, o abbia utilizzato la funzione di ricerca per visualizzare il programma che desideri, puoi semplicemente fare clic con il tasto destro sul programma e scegliere Aggiungi alla barra delle applicazioni per attaccare un collegamento permanente a tale applicazione nella barra delle applicazioni nella parte inferiore dello schermo. Fatto ciò, durante i futuri accessi alla tua sessione sul server, le tue applicazioni preferite e più utilizzate ti aspetteranno con un solo clic. Come puoi vedere nello screenshot seguente,



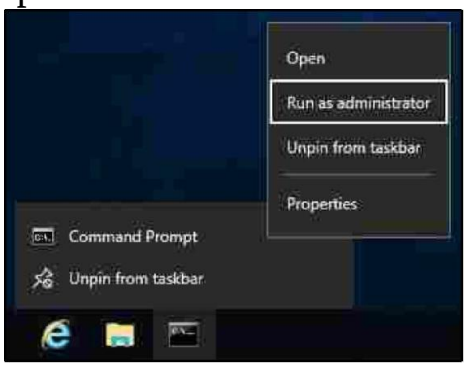
Molti lettori avranno già molta familiarità con il processo di blocco dei programmi sulla barra delle applicazioni, quindi facciamo un ulteriore passo avanti per rappresentare una funzione aggiuntiva di cui potresti non essere a conoscenza quando hai delle applicazioni bloccate.

Il potere del clic destro

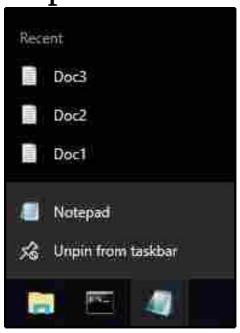
Conosciamo tutti abbastanza bene il clic con il tasto destro in una determinata area di un sistema operativo Windows per eseguire alcune funzioni più avanzate. Da quando il mouse è uscito dalla catena di montaggio sono esistiti piccoli menu contestuali visualizzati con un clic destro. Spesso facciamo clic con il pulsante destro del mouse per copiare

testo, copiare documenti, incollare lo stesso o entrare in un insieme più approfondito di proprietà per un particolare file o cartella. Molte attività quotidiane vengono eseguite con quel pulsante del mouse. Quello che voglio sottolineare è che i produttori di software, Microsoft e non, hanno aggiunto ancora più funzionalità di clic con il tasto destro negli stessi lanciatori di applicazioni, il che rende ancora più vantaggioso averli a portata di mano, come all'interno del barra delle applicazioni.

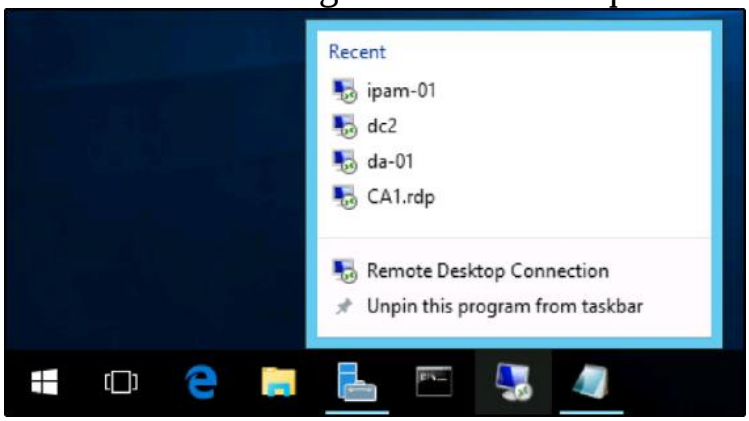
La quantità di funzionalità fornite quando si fa clic con il pulsante destro del mouse su un'applicazione nella barra delle applicazioni varia a seconda dell'applicazione stessa. Ad esempio, se dovessi fare clic con il pulsante destro del mouse sul prompt dei comandi, ho le opzioni per aprire il prompt dei comandi o per sbloccare dalla barra delle applicazioni. Cose molto semplici. Se faccio di nuovo clic con il pulsante destro del mouse sull'opzione di menu più piccola per il prompt dei comandi, ho la possibilità di eseguire le stesse funzioni, ma potrei anche andare oltre in Proprietà o Esegui come amministratore. Quindi, ottengo funzionalità un po 'più avanzate man mano che vado in profondità:



Tuttavia, con altri programmi vedrai più risultati. E più utilizzi i tuoi server, più dati e opzioni inizierai a vedere in questi menu contestuali cliccabili con il tasto destro. Due ottimi esempi sono Blocco note e Client Desktop remoto. Sul mio server, ho lavorato su alcuni file di configurazione di testo e ho utilizzato il mio server per passare ad altri server per eseguire alcune attività remote. L'ho fatto utilizzando il client desktop remoto. Ora, quando faccio clic con il pulsante destro del mouse su Blocco note elencato nella barra delle applicazioni, ho collegamenti rapidi ai documenti più recenti su cui ho lavorato:



Quando faccio clic con il pulsante destro del mouse sulla mia icona RDP, ora sono elencati i collegamenti rapidi proprio qui per i server recenti a cui mi sono connesso. Non so voi, ma ogni giorno faccio RDP su molti server diversi. Avere un collegamento per il client desktop remoto nella barra delle applicazioni che tiene automaticamente traccia dei server più recenti che ho visitato, mi fa sicuramente risparmiare tempo e clic del mouse mentre svolgo le mie attività quotidiane:

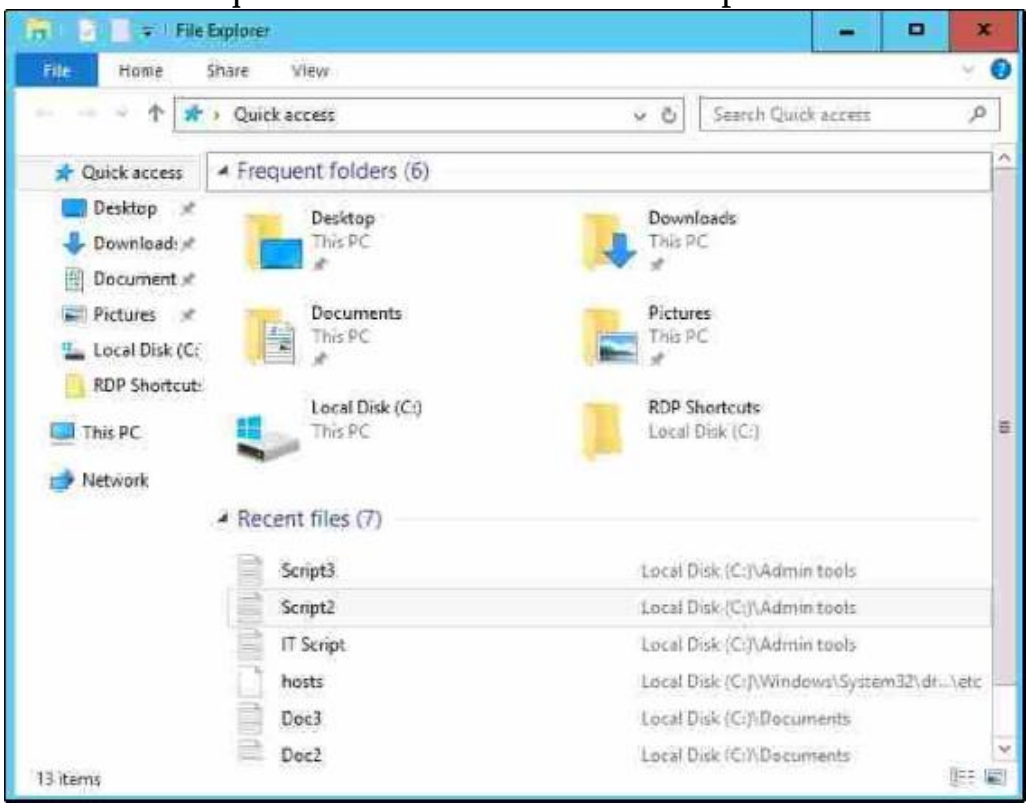


Queste funzioni di clic con il pulsante destro del mouse esistono per un paio di versioni del sistema operativo ora, quindi non è una nuova tecnologia, ma viene ampliata regolarmente man mano che vengono rilasciate nuove versioni delle applicazioni. È anche una funzionalità che non vedo utilizzare molti amministratori di server, ma forse dovrebbero iniziare a farlo per lavorare in modo più efficiente, motivo per cui ne stiamo discutendo qui.

Qualcosa che è migliorato nelle piattaforme Windows 10 e Server 2019 che è anche molto utile su base giornaliera è la vista di accesso rapido che viene presentata per impostazione predefinita quando si apre Esplora file. Conosciamo tutti e usiamo Esplora file e lo facciamo da molto tempo, ma in genere quando vuoi raggiungere un punto particolare del disco rigido o un file specifico, hai molti clic del mouse da eseguire per raggiungere la tua destinazione. La visualizzazione Accesso rapido di Windows Server 2019 ci mostra immediatamente file e cartelle recenti e frequenti, a cui comunemente accediamo dal server. Noi, in qualità di amministratori, dobbiamo spesso visitare gli stessi punti sul disco rigido e aprire gli stessi file più e più volte. Non sarebbe fantastico se File Explorer raggruppasse

tutti quei percorsi comuni e collegamenti ai file in un unico posto? Questo è esattamente ciò che fa Accesso rapido.

Nella schermata seguente puoi vedere che l'apertura di Esplora file offre collegamenti rapidi per aprire sia le cartelle a cui si accede di frequente sia i collegamenti ai file recenti. Una caratteristica come questa può farti risparmiare molto tempo e, facendo regolarmente uso di questi piccoli pezzi a tua disposizione per aumentare la tua efficienza, dimostra ai colleghi e alle persone intorno a te che hai una reale familiarità e livello di comfort con questo ultimo ciclo di sistemi operativi:



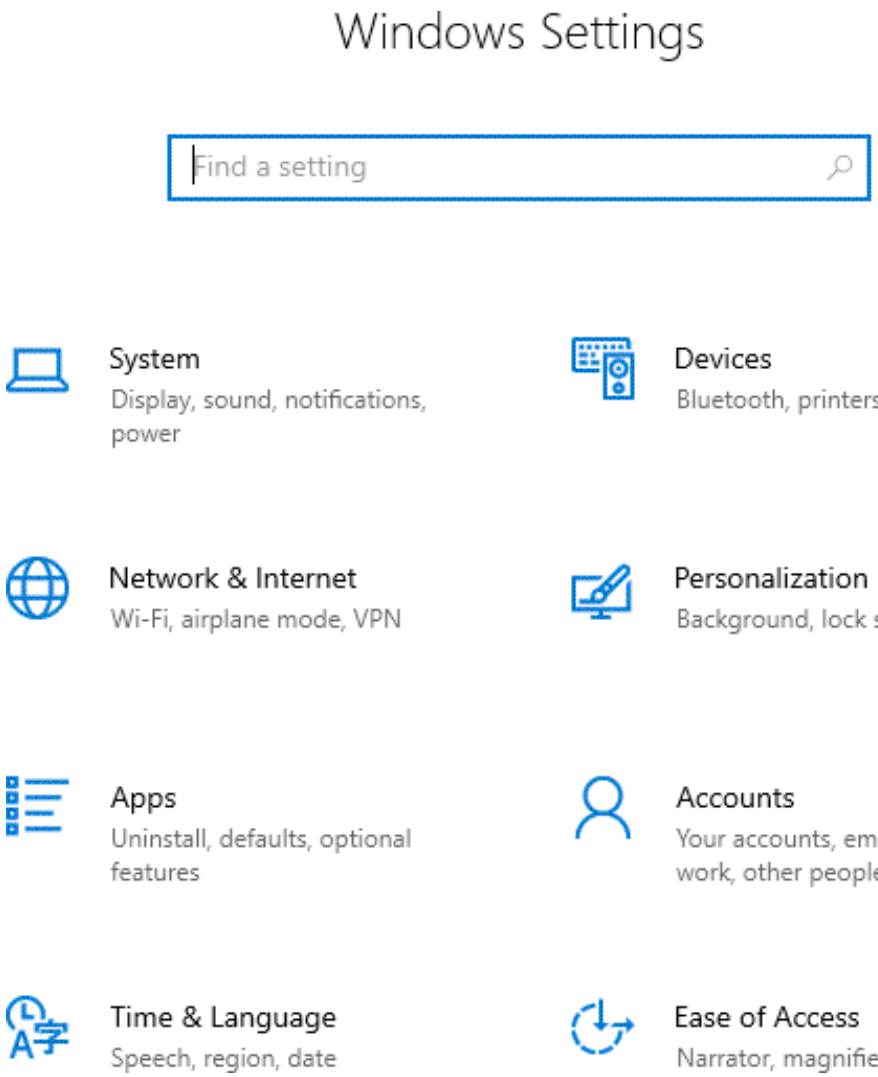
Utilizzando la schermata Impostazioni più recente

Se lavori nel settore IT e utilizzi Windows 10 su una macchina client per un certo periodo di tempo, è una scommessa sicura che ti sei imbattuto nella nuova interfaccia delle impostazioni, forse accidentalmente, come è stato per me, la prima volta che ho visto esso. Ho visto un certo numero di persone ora imbattersi nell'interfaccia Impostazioni per la prima volta durante il tentativo di visualizzare o configurare gli aggiornamenti di Windows. Vedi, le impostazioni in Windows Server 2019 sono proprio ciò che suggerisce il nome, un'interfaccia da cui configurare varie impostazioni all'interno del sistema operativo. Cosa c'è di così difficile o di confuso in questo? Bene, abbiamo già una piattaforma di atterraggio per tutte le impostazioni contenute in Windows che esiste da milioni di anni. Si chiama Pannello di controllo.

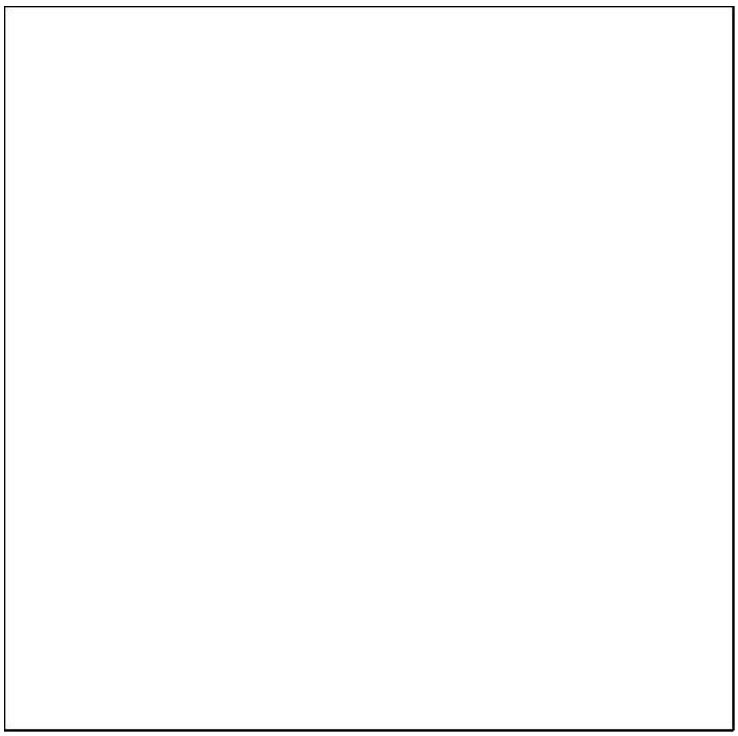
Il menu Impostazioni all'interno di Windows non è un'idea nuova di zecca, ma sembra abbastanza nuovo rispetto al Pannello di controllo. Windows Server 2012 e 2012 R2 avevano una quasi presenza di impostazioni che, per quanto ne so, sono rimaste in gran parte inutilizzate dagli amministratori di sistema. Credo che questo sia l'effetto di una cattiva esecuzione poiché il menu Impostazioni nel 2012 è stato accessibile e nascosto dietro la barra degli accessi, che la maggior parte delle persone ha deciso che fosse un'idea terribile. Non passeremo troppo tempo sulla tecnologia del passato, ma la barra degli accessi in Server 2012 era un menu che si presentava quando si faceva scorrere il dito dal bordo destro dello schermo. Sì, hai ragione, i server di solito non hanno touchscreen. Non a nessuno su cui abbia mai lavorato, comunque. Quindi, la barra degli accessi si è presentata anche quando hai spostato il mouse in alto a destra dello schermo.

Ti sto solo dando queste informazioni di base per passare a questa prossima idea. Gran parte dell'interfaccia utente in Windows 10, e quindi Windows Server 2016 e 2019, può essere considerata un piccolo passo indietro rispetto al regno dei passaggi con le dita e dei touchscreen.

Windows 8 e Server 2012 erano così concentrati sui pulsanti delle app grandi e sui passaggi delle dita che molte persone si sono perse nel mescolamento. Era così diverso da quello che avevamo mai visto prima e difficile da usare a livello amministrativo. A causa del feedback ricevuto da quella versione, l'interfaccia grafica e i controlli utente, inclusi sia il menu Start che il menu Impostazioni in Windows Server 2019, sono una sorta di smack-dab a metà tra Server 2008 e Server 2012. Questo passaggio all'indietro è stato il quello giusto da prendere, e finora non ho sentito altro che elogi sulla nuova interfaccia utente.



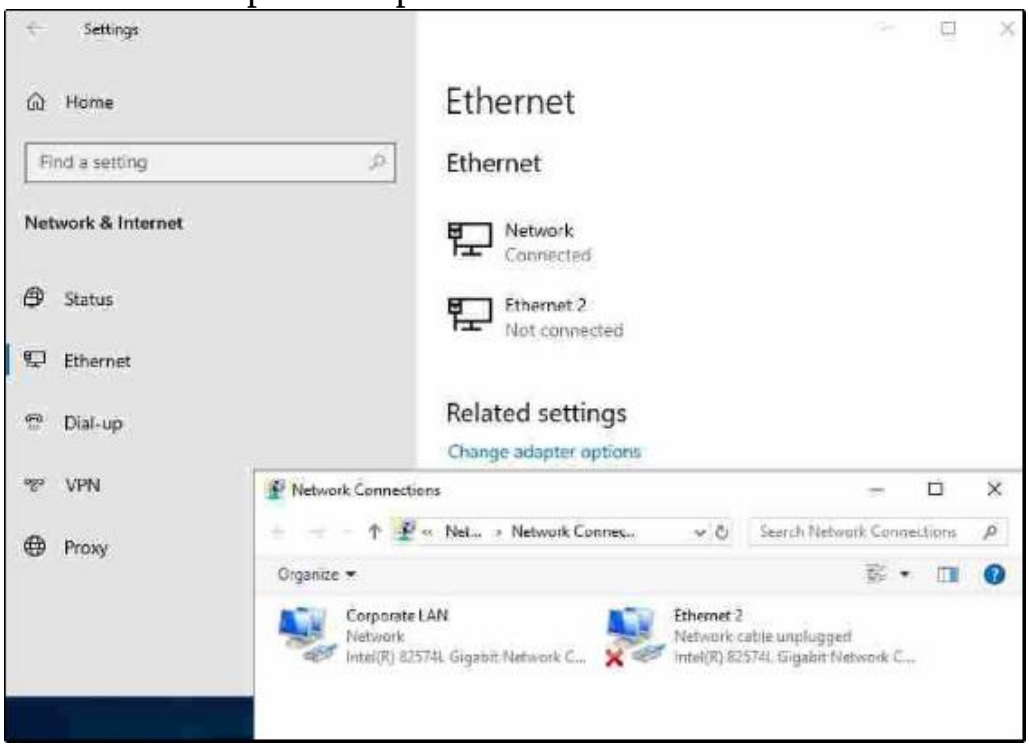
Quindi, tornando al menu Impostazioni, se fai clic sul pulsante Start, quindi fai clic su quel piccolo pulsante a forma di ingranaggio appena sopra i controlli di alimentazione, vedrai questa nuova interfaccia:



Ci sono molte impostazioni e parti del sistema operativo che puoi configurare in questo nuovo menu Impostazioni. Alcune impostazioni in Windows ora esistono solo in questa interfaccia, ma molte sono ancora accessibili qui o tramite il pannello di controllo tradizionale. L'obiettivo sembra essere uno spostamento verso tutte le configurazioni eseguite tramite il nuovo menu nelle versioni future, ma, per ora, possiamo ancora amministrare la maggior parte delle modifiche alle impostazioni tramite i nostri metodi tradizionali, se lo desideriamo. Ho menzionato gli aggiornamenti di Windows in precedenza e questo è un buon esempio da esaminare. Tradizionalmente, configureremmo le nostre impostazioni di Windows Update tramite il Pannello di controllo, ma ora sono state completamente migrate nel nuovo menu Impostazioni in Windows Server 2019. Cerca nel Pannello di controllo per Windows Update e l'unico risultato è che puoi visualizzare attualmente installato aggiornamenti. Ma,

Ricorda, puoi sempre utilizzare la funzione di ricerca di Windows per cercare qualsiasi impostazione! Premi il tuo WinKey e digitaaggiornamento Windowse ti verranno forniti collegamenti rapidi che ti porteranno direttamente ai menu Impostazioni appropriati.

Per il momento, dovrai utilizzare una combinazione di Pannello di controllo e menu Impostazioni per svolgere il tuo lavoro. Di tanto in tanto diventa confuso. A volte, farai persino clic su qualcosa all'interno del menu Impostazioni e verrà avviata una finestra del pannello di controllo! Provalo. Apri il menu Impostazioni e fai clic su Rete e Internet. Fare clic su Ethernet nella colonna di sinistra. Qui puoi vedere lo stato delle tue schede di rete, ma non puoi cambiare nulla, come cambiare un indirizzo IP. Quindi, si nota il collegamento per Modifica opzioni adattatore. Oh sì, suona come quello che voglio fare. Fai clic su Modifica opzioni adattatore e verrai reindirizzato alla tradizionale schermata Connessioni di rete con l'aspetto del pannello di controllo:



Due modi per fare la stessa cosa

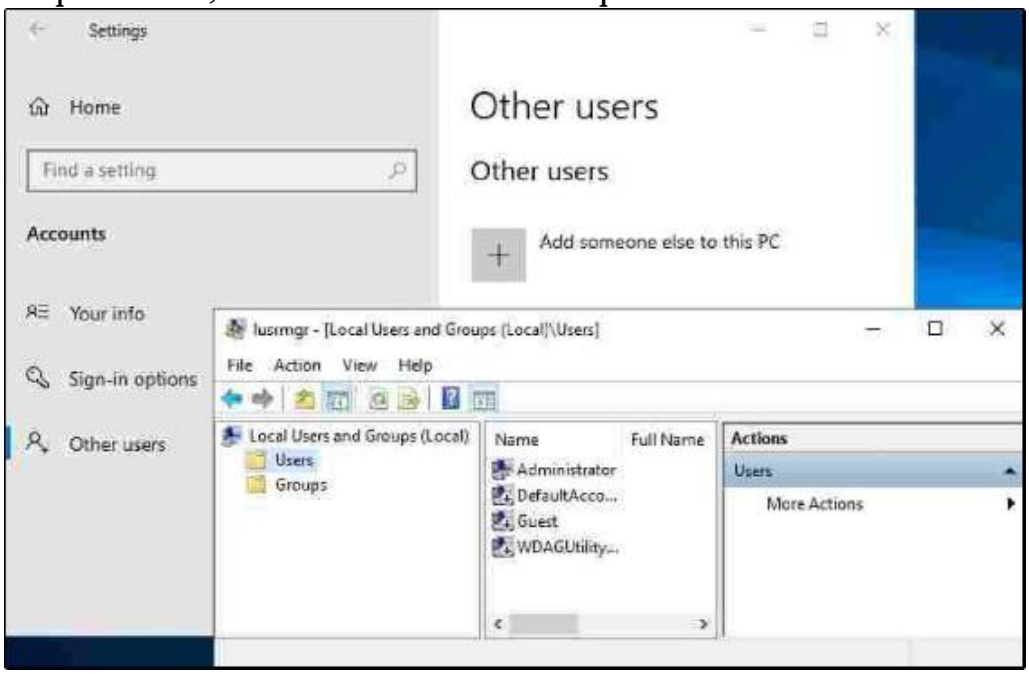
Potenzialmente anche fonte di confusione, fino a quando non ti abitui a navigare qui, è che a volte puoi svolgere la stessa attività nel Pannello di controllo o nel menu Impostazioni, ma il processo che segui in ciascuna interfaccia può avere un aspetto molto diverso . Diamo un'occhiata a questo in prima persona provando a creare un nuovo account utente sul nostro server, una volta tramite il Pannello di controllo e di nuovo tramite Impostazioni.

Creazione di un nuovo utente tramite il pannello di controllo

Probabilmente hai abbastanza familiarità con questo. Apri il Pannello di controllo e fai clic su Account utente. Quindi, fai clic sull'intestazione Account utente. Ora, fai clic sul collegamento per gestire un altro account. All'interno di questa schermata c'è la tua opzione per aggiungere un account utente. Fare clic su di esso e si apre la finestra di dialogo in cui si immette un nome utente e una password per il nuovo utente:

Creazione di un nuovo utente tramite il menu Impostazioni

Prendiamo questa nuova interfaccia Impostazioni per un test drive. Apri il menu Impostazioni e fai clic su Account. Ora, fai clic su Altri utenti nella colonna di sinistra. C'è un'opzione qui per aggiungere qualcun altro a questo PC; vai avanti e fai clic su quello:



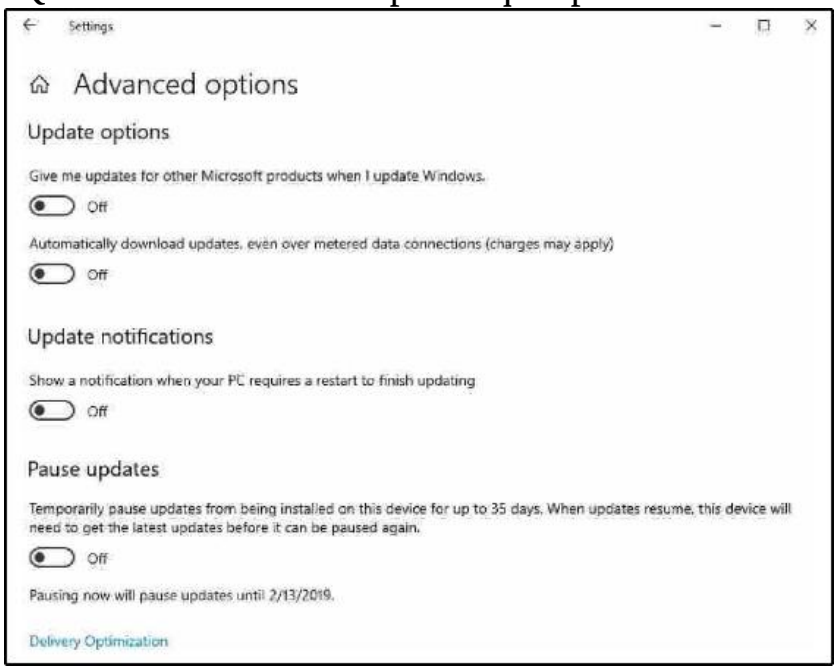
Che diavolo è quello? Non quello che mi aspettavo, purtroppo. Con mia grande sorpresa, il vecchio account utente del pannello di controllo lancia un'interfaccia piacevole e dall'aspetto fresco da cui posso creare nuovi account utente. L'accesso agli account utente tramite la console Impostazioni più recente mi avvia nel vecchio gestore di utenti e gruppi locali. Tecnicamente, da qui potrei sicuramente andare avanti e creare nuovi account utente, ma sembra che qui ci sia una sorta di disconnessione. Penseresti naturalmente che le nuove Impostazioni avvierebbero la schermata più nuova e più bella per l'aggiunta di nuovi account utente, ma abbiamo riscontrato che è vero il contrario.

Abbiamo esaminato questo semplice esempio di tentativo di eseguire la stessa funzione attraverso due diverse interfacce per mostrare che ci sono alcuni elementi che possono e devono essere eseguiti all'interno del nuovo contesto del menu Impostazioni, ma ci sono molte funzioni all'interno di Windows che devono ancora essere realizzate attraverso le nostre interfacce tradizionali. Mentre il Pannello di controllo continua ad esistere, e probabilmente lo sarà per molto tempo, dovresti iniziare a navigare nel menu Impostazioni e capire cosa è disponibile all'interno, in modo da poter iniziare a plasmare le tue idee per la migliore combinazione di entrambi i mondi per gestire i tuoi server in modo efficace.

Solo un'ultima cosa da sottolineare quando iniziamo a prendere confidenza con il modo in cui appaiono i nuovi menu Impostazioni: molte delle impostazioni che configuriamo nei nostri server sono tipi di impostazioni on / off. Con questo intendo che stiamo impostando qualcosa su un'opzione o su un'altra.
Storicamente, questi tipi di configurazioni erano gestiti da menu a discesa o da pulsanti di opzione. Questo è normale; quello è previsto; questo è Windows. Ora inizierai a vedere piccole barre di scorrimento, o cursori, che ti consentono di attivare o disattivare le impostazioni, come un interruttore della luce.
Chiunque abbia utilizzato l'interfaccia delle impostazioni di qualsiasi smartphone sa esattamente di cosa sto parlando. Questo comportamento dell'interfaccia utente si è ora fatto strada nei sistemi operativi Windows

completi ed è probabilmente destinato a rimanere. Solo per darti un'idea di come appare nel contesto del nuovo menu Impostazioni, ecco uno screenshot della pagina delle impostazioni di Windows Update corrente all'interno delle impostazioni di aggiornamento e sicurezza.

Questo è un buon esempio di quei pulsanti di scorrimento on / off:



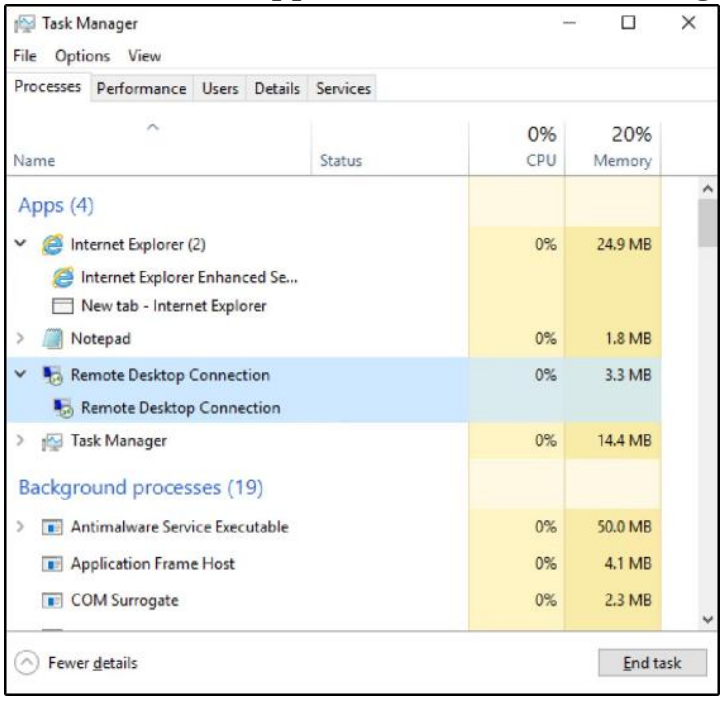
Task Manager

Task Manager è uno strumento che è esistito in tutti i sistemi operativi Windows sin dai primi giorni dell'interfaccia grafica, ma si è evoluto parecchio nel corso degli anni. Uno degli obiettivi di Windows Server 2019 è essere ancora più utile e affidabile rispetto a qualsiasi versione precedente di Windows Server. Quindi, ha senso solo rimuovere del tutto Task Manager, dal momento che semplicemente non sarà più necessario, giusto?

Sto scherzando, ovviamente! Mentre si spera che Server 2019 si dimostrerà davvero il sistema operativo più stabile e meno bisognoso che abbiamo mai visto da Microsoft, Task Manager esiste ancora e sarà ancora necessario agli amministratori di server ovunque. Se non guardi da vicino Task Manager da un po ', è cambiato in modo significativo nelle ultime versioni.

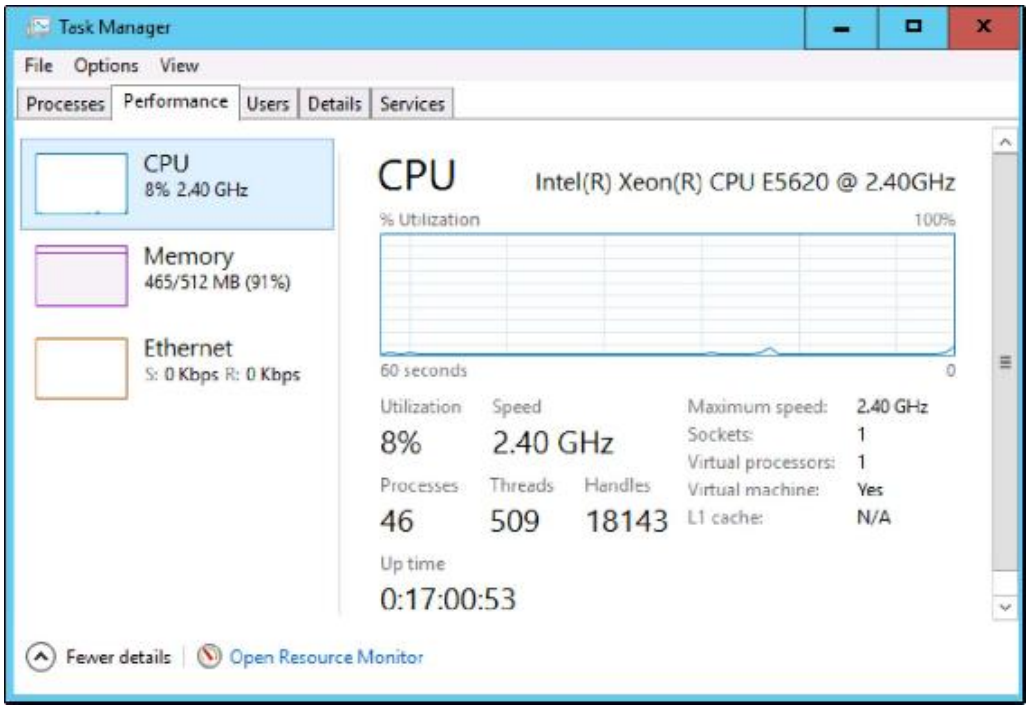
Task Manager viene ancora normalmente richiamato da Ctrl + Alt + Canc sulla tastiera, quindi facendo clic su Task Manager o facendo clic con il pulsante destro del mouse sulla barra delle applicazioni e quindi scegliendo Task Manager. Puoi anche avviare Task Manager con la combinazione di tasti Ctrl + Maiusc + Esc o digitando taskmgr nelle finestre di dialogo Esegui o Cerca. La prima cosa che noterai è che esistono pochissime informazioni in questa visualizzazione predefinita, solo un semplice elenco di applicazioni attualmente in esecuzione. Questa è un'interfaccia utile per forzare la chiusura di un'applicazione che potrebbe essere bloccata, ma non per molto altro. Vai avanti e fai clic sul collegamento Ulteriori dettagli e inizierai a vedere le informazioni reali fornite in questa potente interfaccia.

Notiamo immediatamente che le informazioni visualizzate sono più user-friendly rispetto agli anni precedenti, con le app e i processi in background classificati in modo più intuitivo e più istanze della stessa applicazione condensate per una facile visualizzazione. Ciò offre una visione generale più rapida di ciò che sta accadendo con il nostro sistema, dando comunque la possibilità di espandere ogni applicazione o processo per vedere quali singoli componenti o finestre sono in esecuzione all'interno dell'applicazione, come nella seguente schermata:



Assicurati di controllare anche le altre schede disponibili all'interno di Task Manager. Gli utenti ci mostreranno un elenco degli utenti attualmente connessi e la quantità di risorse hardware che le loro sessioni utente stanno consumando. Questo è un bel modo per identificare su un server Host sessione Desktop remoto, ad esempio, una persona che potrebbe causare un rallentamento sul server.
La scheda Dettagli è una visualizzazione un po 'più tradizionale della scheda Processi, che suddivide gran parte delle stesse informazioni ma nel modo vecchio stile che eravamo abituati a vedere nelle versioni del sistema operativo molto tempo fa. Quindi, la scheda Servizi è piuttosto autoesplicativa; mostra i servizi di Windows attualmente installati sul server, il loro stato e la possibilità di avviare o arrestare questi servizi secondo necessità, senza dover aprire la console dei servizi separatamente.

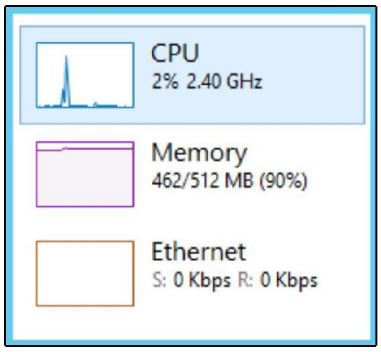
La scheda che ho saltato in modo da poterlo menzionare più specificamente qui è la scheda Prestazioni. Questo è piuttosto potente. All'interno è possibile monitorare rapidamente l'utilizzo di CPU, memoria e Ethernet. Come puoi vedere nello screenshot seguente, non ho fatto un ottimo lavoro di pianificazione delle risorse su questa particolare macchina virtuale, poiché la mia CPU viene appena toccata ma ho quasi esaurito la memoria di sistema:


Task Manager
File Options View
Processes Performance Users Details Services
CPU
8% 2.40 GHz
Memory
465/512 MB (91%)
Ethernet
S: 0 Kbps R: 0 Kbps
CPU
Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
% Utilization
100%
60 seconds
0
Utilization
8%
Speed
2.40 GHz
Processes
46
Threads
509
Handles
18143
Up time
0:17:00:53
Maximum speed: 2.40 GHz
Sockets: 1
Virtual processors: 1
Virtual machine: Yes
L1 cache: N/A
Fewer details
Open Resource Monitor

Un'altra utile informazione disponibile all'interno di questa schermata è il tempo di attività del server. Trovare queste informazioni può essere fondamentale durante la risoluzione di un problema e osservo ripetutamente gli amministratori che calcolano il tempo di attività del sistema in base ai timestamp dei log. Usare Task Manager è un modo molto più semplice per

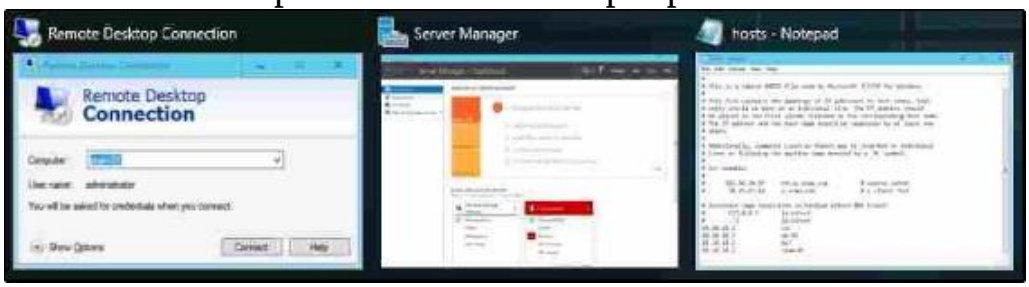
Se sei interessato a visualizzare dati più approfonditi sulle prestazioni del server, c'è un collegamento nella parte inferiore di questa finestra del Task Manager dove puoi aprire Monitoraggio risorse. Due tecnologie fornite in Server 2019 per il monitoraggio dello stato del sistema, in particolare per le prestazioni dell'hardware, sono Resource Monitor e Performance Monitor. Sicuramente apri questi strumenti e inizia a testarli, in quanto possono fornire sia informazioni sulla risoluzione dei problemi che dati di base essenziali quando avvii un nuovo server. Questa linea di base può quindi essere confrontata con i dati di test futuri in modo da poter monitorare in che modo le nuove applicazioni o servizi installati su un determinato server hanno influenzato il consumo di risorse.

Tornando a Task Manager, c'è solo un altro piccolo trucco che vorrei provare. Sempre all'interno della scheda Prestazioni, vai avanti e fai clic con il pulsante destro del mouse su qualsiasi dato particolare a cui sei interessato. Farò clic con il pulsante destro del mouse sulle informazioni sulla CPU vicino al lato sinistro della finestra. Si apre una finestra di dialogo con alcune opzioni, di cui farò clic sulla visualizzazione Riepilogo. Questo condensa i dati che in precedenza occupavano circa la metà del mio spazio sullo schermo, in una minuscola finestra, che posso spostare nell'angolo dello schermo. Questo è un bel modo per mantenere i dati sull'utilizzo dell'hardware sullo schermo in ogni momento mentre navighi e lavori sul tuo server in modo da poter osservare eventuali picchi o aumenti nel consumo di risorse quando apporti modifiche al sistema:


CPU
2% 2.40 GHz
Memory
462/512 MB (90%)
Ethernet
S: 0 Kbps R: 0 Kbps

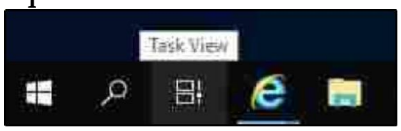
Visualizzazione attività

Visualizzazione attività è una nuova funzionalità di Windows 10 e Windows Server 2016, che viene trasferita a Server 2019. È un'idea simile a quella di tenere premuto il tasto Alt e quindi premere Tab per scorrere le applicazioni attualmente in esecuzione. Per chiunque non l'abbia mai provato, vai avanti e tieni premuti quei due tasti sulla tastiera in questo momento. A seconda della versione di Windows in esecuzione, lo schermo potrebbe apparire leggermente diverso da questo, ma, in effetti, sono le stesse informazioni. Puoi vedere tutti i programmi che hai attualmente aperto e puoi scorrerli da sinistra a destra usando ulteriori pressioni del pulsante Tab. In alternativa, usa Alt + Maiusc + Tab per scorrerli in ordine inverso. Quando hai molte finestre aperte, è forse più facile usare semplicemente il mouse per passare a una finestra specifica:



Task View è un po 'più potente di questo, perché aggiunge la capacità di gestire più desktop completi di finestre e applicazioni. Ad esempio, se stavi lavorando su due progetti diversi sullo stesso server e ogni progetto richiedeva che tu avessi molte finestre diverse aperte contemporaneamente, inizieresti a bruciare molto tempo passando avanti e indietro tra tutti i tuoi diversi app e finestre per trovare quello che stavi cercando. Usando Task View, puoi lasciare tutte le finestre aperte per il primo progetto sul tuo primo desktop e aprire tutte le finestre che si occupano del secondo progetto su un secondo desktop. Quindi, con due clic puoi facilmente passare avanti e indietro tra i diversi desktop, utilizzando il pulsante Visualizzazione attività. Per impostazione predefinita, Task View è il piccolo pulsante in basso nella barra delle applicazioni, immediatamente a destra della lente di ingrandimento Cerca

vicino al pulsante Start. Vai avanti e fai clic su di esso ora, assomiglia a questo:



Ora vedi un elenco delle finestre attualmente aperte; questo è molto simile alla funzionalità Alt + Tab che abbiamo visto in precedenza. La differenza è il piccolo pulsante vicino all'angolo in alto a sinistra che dice Nuovo desktop. Vai avanti e fai clic su quello ora:

Ora vedrai Desktop 1 e Desktop 2 disponibili per l'uso. Puoi fare clic su Desktop 2 e aprire alcuni nuovi programmi, oppure puoi anche trascinare e rilasciare le finestre esistenti tra diversi desktop, direttamente in questa schermata Visualizzazione attività:

Task View è un ottimo modo per rimanere organizzati ed efficienti utilizzando più desktop sullo stesso server. Suppongo che sia un po 'come eseguire due monitor, o tre o quattro o più, tutti da un singolo monitor fisico.

Se vuoi evitare di dover cliccare sull'icona per Task View, premi *WinKey* + Tab sulla tastiera fa la stessa cosa!

Sommario

Questo primo capitolo sul nuovo Windows Server 2019 è incentrato sull'acquisizione di familiarità e comodità durante la navigazione nell'interfaccia. Esistono vari modi per interagire con Server 2019 e ne discuteremo molti in questo libro, ma la maggior parte degli amministratori di server si interfaccerà con questo nuovo sistema operativo tramite l'interfaccia grafica completa, utilizzando sia il mouse che la tastiera per svolgere le proprie attività. Se hai lavorato con versioni precedenti del sistema operativo Windows Server, molti degli strumenti che utilizzerai per guidare questa nuova piattaforma saranno gli stessi, o almeno simili, a quelli che hai utilizzato in passato. I nuovi sistemi operativi dovrebbero essere sempre un'evoluzione dei loro predecessori e mai tutti nuovi. Penso che questa sia stata una lezione appresa con il rilascio di Windows 8 e Server 2012.

Con Server 2019, troviamo un ottimo compromesso tra la tradizionale familiarità delle versioni precedenti di Windows e i nuovi vantaggi che derivano dai bordi arrotondati e dagli schermi touch-friendly che verranno utilizzati sempre più spesso man mano che ci spostiamo verso il futuro di Windows dispositivi basati. Nel prossimo capitolo esamineremo l'installazione e la gestione di Windows Server.

Domande

1. In Windows Server 2019, come è possibile avviare un prompt di PowerShell con privilegi elevati con due clic del mouse?
2. Qual è la combinazione di tasti per aprire questo menu Attività di amministrazione rapida?
3. Qual è il nome dell'offerta di servizi cloud di Microsoft?
4. Quali sono le due versioni di licenza di Windows Server 2019?

5. Quante macchine virtuali possono essere eseguite su un host Windows Server 2019 Standard?
6. Quale opzione di installazione per Windows Server 2019 non dispone di un'interfaccia utente grafica?
7. Qual è il linguaggio corretto per l'ultima versione di Windows Server 2019, Long-Term Servicing Branch (LTSB) o Long-Term Servicing Channel (LTSC)?
8. Qual è lo strumento corretto da cui modificare le configurazioni su Windows Server 2019, Impostazioni di Windows o Pannello di controllo?

Installazione e gestione di Windows Server 2019

Ora che abbiamo dato un'occhiata ad alcune delle funzionalità all'interno dell'interfaccia grafica di Windows Server 2019, mi rendo conto che alcuni di voi potrebbero essere seduti a pensare È fantastico leggere, ma come posso davvero iniziare a giocare con questo per me stessa? Leggere di tecnologia non è mai così bello come sperimentarlo di persona, quindi vogliamo che un po 'di gomma si adatti alla strada in questo capitolo. Uno dei principali obiettivi di questo libro è assicurarci di consentirti di utilizzare il prodotto. Spiegare fatti su nuove funzionalità ed efficienze va bene e va bene, ma alla fine è inutile se non sei in grado di farlo funzionare nella vita reale. Quindi, facciamo in modo che questo pezzo di metallo grezzo del server lavori per noi.

n questo capitolo tratteremo quanto segue:

- Requisiti per l'installazione
- Installazione di Windows Server 2019 Installazione di ruoli e funzionalità
- Gestione e monitoraggio centralizzati
- **Windows Admin Center (WAC)**
- Abilitazione delle implementazioni rapide del server con Sysprep

Requisiti tecnici

Quando si pianifica la creazione di un nuovo server, molte delle decisioni che è necessario prendere riflettono le decisioni sul tipo di licenza. Quali ruoli intendi installare su questo server? Può Server 2019 Standard gestirlo o abbiamo bisogno di Datacenter Edition per questo ragazzo? Server Core sarà vantaggioso dal punto di vista della sicurezza o abbiamo bisogno dell'esperienza desktop completa? In questi giorni di server Hyper-V con la possibilità di far girare macchine virtuali per un capriccio, spesso si procede senza troppa considerazione dell'hardware di un server, ma ci sono certamente ancora casi in cui l'apparecchiatura fisica ospiterà il Windows Server 2019 operativo sistema. In questi casi è necessario essere consapevoli dei requisiti per questa nuova piattaforma, quindi dedichiamoci un minuto per elencare quelle specifiche.[https: //documenti.microsoft.com /en-noi/ finestre-server/ottenere-iniziato-19 /sys-richieste-19):]

- **processore**: 1,4 GHz 64 bit che supporta una serie di cose: NX, DEP, CMPXCHG16b, LAHF / SAHF, PrefetchW e SLAT.
- **RAM**: 512 MB di memoria ECC minimo o minimo 2 GB consigliato per un server che esegue Esperienza desktop. Posso dirti che è possibile installare ed eseguire Desktop Experience con molto meno di 2 GB (come all'interno di un laboratorio di prova), ma devi capire che le prestazioni non saranno alla pari con quelle che potrebbero essere.
- **Disco**: Server 2019 richiede un adattatore di archiviazione PCI Express (PCIe). ATA / PATA / IDE non sono consentiti per le unità di avvio. Il requisito di spazio di archiviazione minimo è di 32 GB, ma Desktop Experience consuma circa 4 GB di spazio in più rispetto a Server Core, quindi tienilo in considerazione.

Queste sono una sorta di specifiche minime, se vuoi solo avviare Server 2019 e darci un'occhiata. Per i sistemi di produzione, aumentare molto questi numeri. Non c'è una risposta magica qui, le specifiche di cui hai bisogno dipendono dai carichi di lavoro che ti aspetti di lanciare sul tuo server. Ci sono componenti aggiuntivi che sarebbe utile cercare quando si

crea un nuovo sistema che sono necessari anche per ruoli e funzionalità particolari. Cose come UEFI e un chip TPM stanno rapidamente diventando mainstream e utilizzate da sempre più servizi con ogni aggiornamento del sistema operativo. In particolare, se sei interessato alla sicurezza e alla protezione tramite BitLocker, o lavori con certificati forti o le nuove VM schermate, vorrai assicurarti che i tuoi sistemi includano chip TPM 2.0.

Installazione di Windows Server 2019

Il processo di installazione per i sistemi operativi Microsoft in generale è migliorato notevolmente negli ultimi 15 anni. Presumo che molti di voi, in quanto professionisti IT, siano anche de facto il ragazzo dei computer di quartiere, a cui amici e parenti chiedono costantemente di riparare o ricostruire i loro computer. Se sei come me, significa che occasionalmente stai ancora ricostruendo sistemi operativi come Windows XP. Guardare le schermate di configurazione blu brillante e trovare una tastiera con il tasto F8 sono fondamentali per questo processo. Trascorrere 2 ore semplicemente installando il sistema operativo di base e portandolo al livello di service pack più alto è abbastanza normale. Rispetto a quella sequenza temporale, l'installazione di un sistema operativo moderno come Windows Server 2019 è quasi incredibilmente veloce e semplice.

È molto probabile che la maggior parte dei lettori abbia già completato questo processo numerose volte e, in tal caso, non esitare a saltare un paio di pagine. Ma per chiunque sia nuovo nel mondo Microsoft o nuovo nell'IT in generale, vorrei prendere solo un paio di pagine veloci per assicurarmi di avere una linea di base con cui iniziare. Senza guadagnare il badge Installazione di un OS 101 sulla cintura degli attrezzi, non arriverai da nessuna parte in fretta.

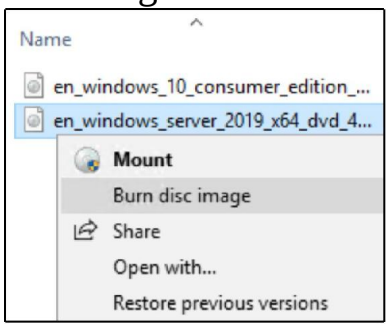
Bruciando quell'ISO

La prima cosa che devi fare è acquisire alcuni supporti di installazione. Il modo più semplice per implementare un singolo nuovo server è scaricare un file .ISO da Microsoft, masterizzarlo su un disco DVD e inserire il DVD da utilizzare per l'installazione. Poiché i collegamenti e gli URL del sito Web sono soggetti a modifiche nel tempo, il modo più affidabile per acquisire il tuo dominio
File .ISO da utilizzare per l'installazione è aprire un motore di ricerca, come Bing, e digitare Download Windows Server 2019. Una volta arrivati

alla pagina ufficiale dei download di Microsoft, fare clic sul collegamento per scaricare il file .ISO e salvarlo sul disco rigido del proprio computer.

La parte più difficile di ottenere un file .ISO per essere un DVD funzionante era necessario scaricare un qualche tipo di strumento di terze parti per masterizzarlo su un disco mentre lo rendeva avviabile. Se stai utilizzando un vecchio sistema operativo client sul tuo computer, questo potrebbe essere ancora il tuo caso. Ho visto molti nuovi a questo processo prendere il file .ISO, trascinarlo sull'unità disco e iniziare a masterizzare il disco. Questo crea un DVD con l'estensione
File .ISOsu di esso, ma quel .ISO è ancora impacchettato e non avviabile in alcun modo, quindi il disco sarebbe inutile per il tuo nuovo pezzo di hardware del server. Fortunatamente, le versioni più recenti dei sistemi operativi client Windows hanno funzioni integrate per gestire i file .ISO che rendono molto semplice il corretto processo di masterizzazione.

Una volta che hai il tuo .ISO file per l'installazione di Windows Server 2019 scaricato sul tuo computer, inserisci un nuovo DVD nell'unità disco e cerca il nuovo file. Basta fare clic con il pulsante destro del mouse sul file .ISO, quindi scegliere l'opzione di menu per Masterizza immagine disco. Questo avvia una semplice procedura guidata che estrarrà e masterizzerà il nuovo file .ISO nel modo corretto sul DVD, rendendolo un supporto di installazione avviabile per il nuovo server. Questo è mostrato nella seguente schermata:



È probabile che, se si tenta di scaricare Windows Server 2019 e utilizzare questa utilità di Windows Disc Image Burner con un DVD estratto dalla pila di DVD vuoti standard, verrà visualizzato il seguente messaggio di errore: Il file immagine del disco è troppo grande e non si adatterà al disco registrabile.

Questo non dovrebbe sorprendere, perché i file di installazione del nostro sistema operativo sono diventati sempre più grandi nel corso degli anni. Abbiamo ora raggiunto il punto critico in cui il programma di installazione ISO standard di Server 2019 è più grande di un disco DVD standard da 4,7 GB. Per masterizzare questa ISO su un DVD, dovrai visitare il negozio e trovare alcuni dischi a doppio strato in grado di gestire più dati.

Creazione di una chiavetta USB avviabile

I DVD possono essere ingombranti e fastidiosi e ora sono anche troppo piccoli per i nostri scopi. Pertanto, quando si installano i sistemi operativi più recenti e più grandi, sta diventando comune preparare una chiavetta

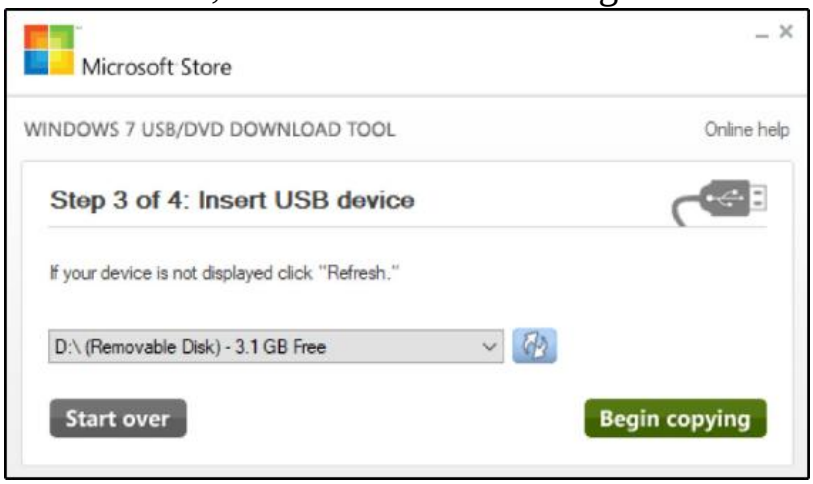
USB da utilizzare per l'installazione del sistema operativo, piuttosto che fare affidamento su un DVD.

Per fare ciò, tutto ciò di cui hai bisogno è un computer Windows, una chiavetta USB di almeno 8 GB e l'accesso a Internet. Dovrai scaricare la stessa ISO di cui abbiamo discusso in precedenza, poiché contiene tutti i file di installazione per Server 2019. Quindi dovrai anche scaricare e installare una sorta di strumento di creazione USB avviabile. Ce ne sono vari gratuiti disponibili (Rufus è piuttosto popolare), ma quello direttamente da Microsoft si chiama Windows 7 USB / DVD Download Tool. Perché ha questo nome pazzo che include le parole Windows 7 proprio nel nome? Non chiedermelo. Ma funziona comunque ed è un modo rapido, facile e gratuito per preparare le tue chiavette USB avviabili per nuove installazioni operative. Vorrei sottolineare che questo strumento non ha nulla a che fare con Windows 7. Richiederà qualsiasi file ISO e lo trasformerà in una chiavetta USB avviabile.

Una volta installato USB DVD Download Tool, avvia l'applicazione e segui semplicemente i passaggi.

Questo processo cancellerà e formatterà la tua chiavetta USB. Assicurati che non ci sia nulla di importante!

Dovrai identificare l'ISO da cui vuoi che lo strumento prenda le informazioni, quindi scegliere la tua chiavetta USB da un elenco a discesa. Dopodiché, premi semplicemente il pulsante Inizia copia e questo strumento trasformerà la tua chiavetta USB in una chiavetta avviabile in grado di installare l'intero sistema operativo Windows Server 2019, come mostrato nella seguente schermata:



Esecuzione del programma di installazione

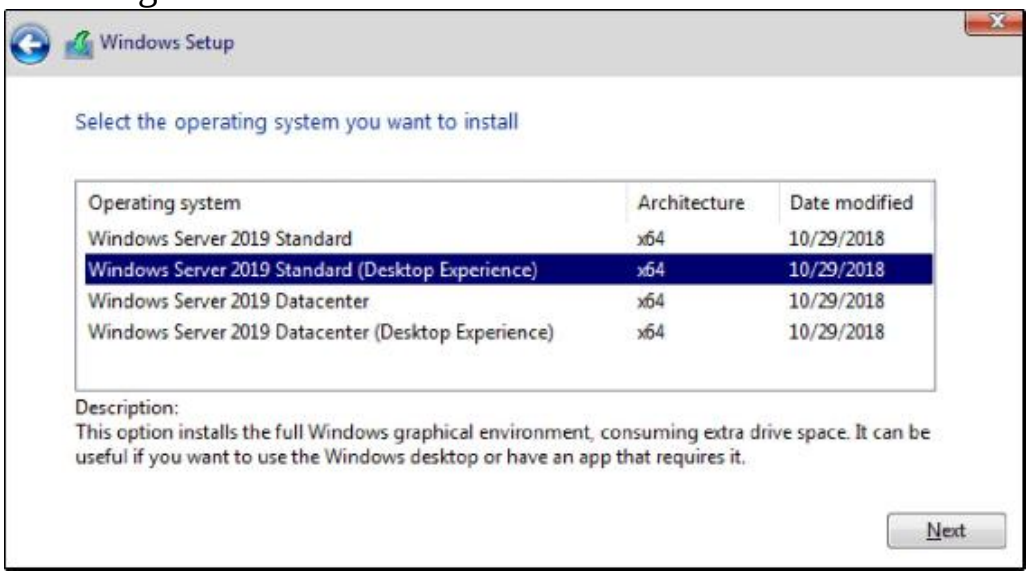
Ora vai avanti e collega il tuo DVD appena creato o USB avviabile al nuovo hardware del server. Avvialo e vedrai finalmente la procedura guidata di installazione per Windows Server 2019. Ora, non ci sono davvero molte opzioni tra cui scegliere all'interno di queste procedure guidate, quindi non passeremo molto tempo qui. Per la maggior parte, fai semplicemente clic sul pulsante Avanti per avanzare tra le schermate, ma ci sono alcuni punti specifici in cui dovrai prendere decisioni lungo il percorso.

Dopo aver scelto la lingua di installazione, la schermata successiva sembra piuttosto semplice. C'è solo un singolo pulsante che dice Installa ora. Sì, è quello su cui vuoi fare clic, ma voglio che tu noti il testo nell'angolo inferiore sinistro dello schermo. Se ti trovi in una posizione in cui hai un server che non può essere avviato e stai tentando di eseguire alcune funzioni di ripristino o diagnostica per risolvere il problema, puoi fare clic su Ripara il tuo computer per avviare quella console di ripristino. Ma per la nostra nuova installazione del server, vai avanti e fai clic su Installa ora. Questo è mostrato nella seguente schermata:

Ti verrà ora chiesto di inserire un codice Product Key per attivare Windows. Se hai già le tue chiavi disponibili, vai avanti e inseriscine una ora. Altrimenti, se lo stai semplicemente installando per testare Server

2019 e desideri eseguire in modalità di prova per un po ', puoi fare clic sul collegamento che dice che non ho un codice Product Key per bypassare questa schermata.

La schermata successiva è interessante e il primo posto in cui devi davvero iniziare a prestare attenzione. Vedrai quattro diverse opzioni di installazione per Windows Server 2019. Ci sono quelli che sembrano essere i programmi di installazione regolari sia per Server 2019 Standard che per Server 2019 Datacenter, e poi una seconda opzione per ciascuno che include le parole Esperienza desktop. In genere, nel mondo del programma di installazione Microsoft, facendo clic su Avanti in ogni opzione si ottiene il percorso di installazione più tipico e comune per qualunque cosa si stia installando. Non così con questa procedura guidata. Se scorri semplicemente da questa schermata facendo clic su Avanti, ti ritroverai alla fine con un'installazione di Server Core. Parleremo di più di Server Core in un capitolo successivo del libro,Capitolo 1, Iniziando con Windows Server 2019, questa opzione predefinita non sarà quella che ti porterà lì. L'esperienza desktop di cui parla la procedura guidata con la seconda opzione è l'interfaccia grafica completa di Windows Server, che molto probabilmente ti aspetti di vedere una volta terminata la nostra installazione. Quindi, ai fini della nostra installazione qui, dove vogliamo interagire con il server utilizzando tutti i colori e il nostro mouse, vai avanti e decidi se vuoi l'edizione Standard o Datacenter, ma assicurati di scegliere prima l'opzione che include Desktop Experience facendo clic sul pulsante Avanti. Questo è mostrato nella seguente schermata:

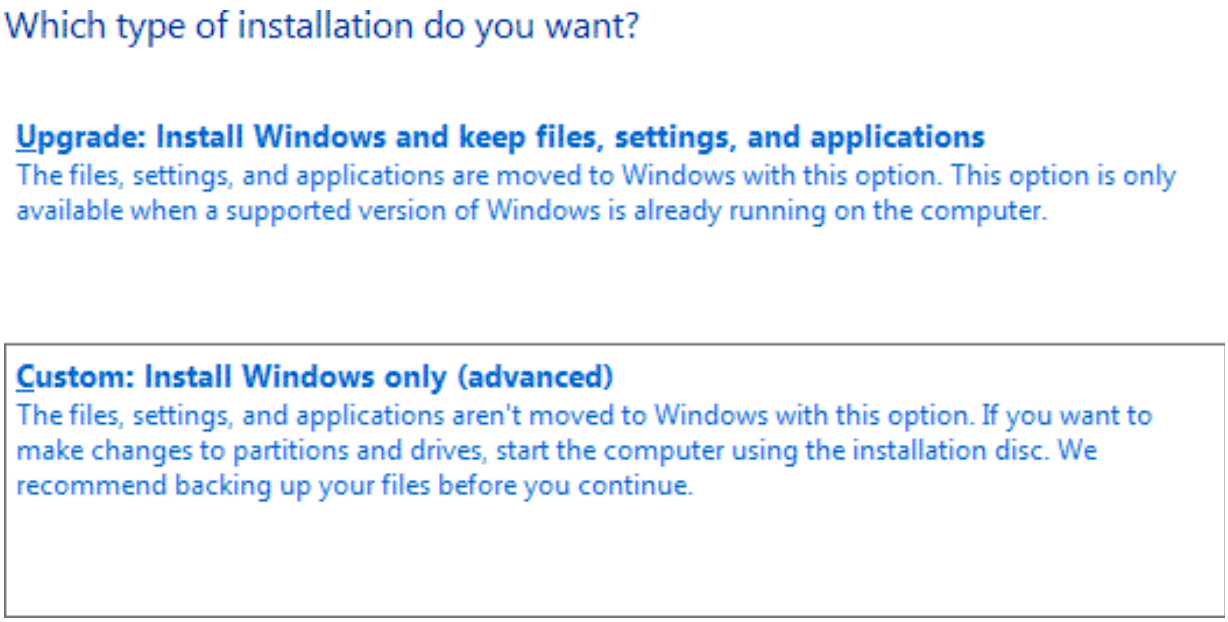


In alcune versioni precedenti di Windows Server, avevamo la possibilità di migrare avanti e indietro da un'esperienza desktop completa a Server Core e viceversa, anche dopo l'installazione del sistema operativo. Questo non funziona in Windows Server 2019! La possibilità di passare da una modalità all'altra è scomparsa, quindi è ancora più importante pianificare correttamente i server dall'inizio.

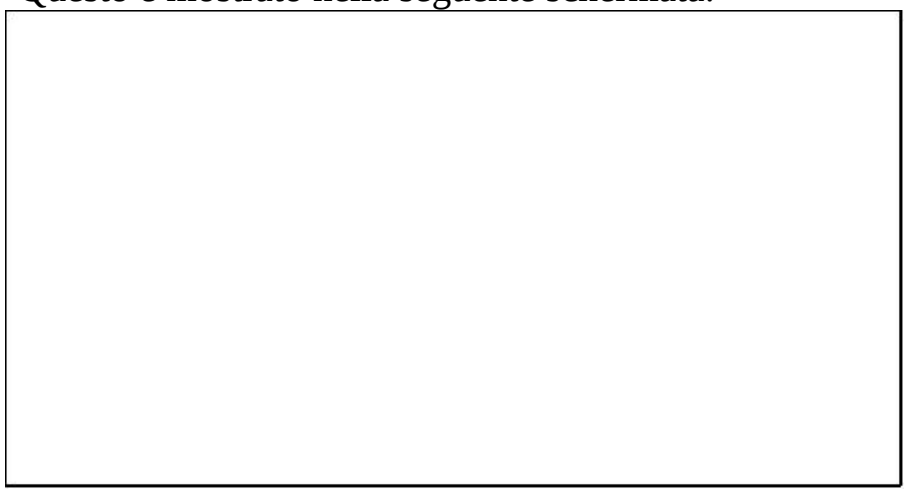
La schermata successiva descrive in dettaglio i termini di licenza che devi accettare, quindi arriviamo a un'altra schermata in cui l'opzione in alto è molto probabilmente non quella su cui intendi fare clic. Capisco perché la funzione di aggiornamento è elencata per prima per un computer Windows 10 di classe consumer, ma nessuno esegue aggiornamenti sul posto ai server Windows. In un mondo perfetto in cui tutto funziona sempre perfettamente dopo gli aggiornamenti, questo sarebbe un ottimo modo per andare.
Potresti avere molti server che svolgono il loro lavoro e ogni volta che viene rilasciato un nuovo sistema operativo, devi semplicemente eseguire il programma di installazione e aggiornarli. Voilà, magia! Sfortunatamente, non funziona in questo modo e non vedo quasi mai amministratori di server disposti a correre dei rischi nel fare un aggiornamento sul posto a un server di produzione esistente. È molto più comune che costruiamo sempre server nuovi di zecca insieme ai server di produzione attualmente in esecuzione. Una volta che il nuovo server è configurato e pronto ad accettare le sue responsabilità, allora, e solo allora, il carico di lavoro effettivo migrerà al nuovo server da quello vecchio. In un processo di migrazione pianificato e accuratamente scolpito, una volta terminata la migrazione dei compiti, il vecchio server viene spento e portato via. Se fossimo in grado di aggiornare semplicemente i server esistenti al sistema operativo più recente, risparmieremmo un sacco di tempo e pianificazione. Ma questo è fattibile solo quando sai che l'aggiornamento funzionerà effettivamente senza intoppi, e la maggior parte delle volte non siamo preparati a correre questo rischio. Se un processo di aggiornamento va di lato e si finisce con un server guasto, ora si sta osservando un costoso processo di riparazione e ripristino su un server di produzione critico per l'azienda. Potresti anche pensare di lavorare tutta la notte o anche nel fine settimana.

Preferiresti dedicare il tuo tempo alla pianificazione di un cutover accuratamente formato o al ripristino di un server critico con l'attività al fiato sul collo perché non possono funzionare? I miei soldi sono per il primo.

Microsoft ha annunciato che il programma di installazione di Windows Server 2019 gestisce gli aggiornamenti da Windows Server 2016 molto meglio di qualsiasi altro percorso di aggiornamento sul posto di Windows Server nella storia. L'aggiornamento da qualsiasi versione precedente del sistema operativo è ancora raccomandato per essere un passaggio e un cambiamento, preparare un server nuovo di zecca e spostare il carico di lavoro, ma a quanto pare ora stanno suggerendo che le persone inizino a testare gli aggiornamenti sul posto dal



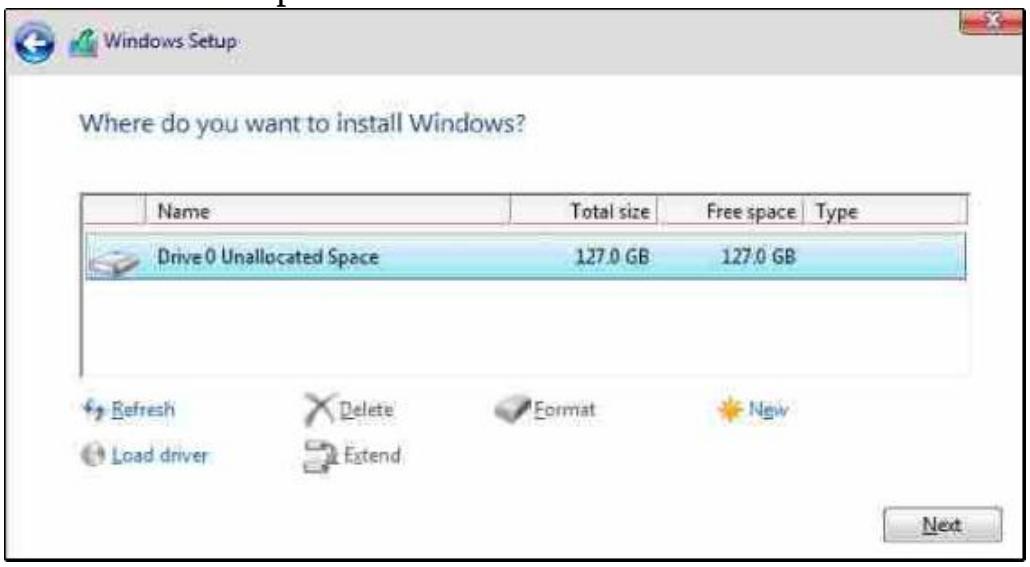
Detto questo, torniamo all'argomento in questione. Nel mondo Windows Server, raramente tocchiamo l'opzione Aggiorna. Quindi vai avanti e scegli l'opzione Personalizzato: Installa solo Windows (avanzata), che è dove entreremo nelle nostre opzioni per l'installazione di questa copia di Windows Server 2019 fresca in una nuova posizione sul disco rigido. Questo è mostrato nella seguente schermata:



Ora decidiamo dove vogliamo installare la nostra nuova copia di Windows Server 2019. In molti casi, farai semplicemente clic su Avanti qui, perché il tuo server avrà solo un singolo disco rigido, o forse un singolo array RAID di dischi, e , in entrambi i casi, vedrai un unico pool di spazio libero su cui puoi installare il sistema operativo. Se hai più dischi rigidi installati sul tuo server e non sono stati ancora collegati insieme in alcun modo,

allora avrai più scelte qui su dove installare Windows Server. Abbiamo solo un singolo disco rigido collegato qui, che non è mai stato utilizzato, quindi posso semplicemente fare clic su Avanti per continuare. Nota qui che se le tue unità contenevano dati esistenti o vecchi, hai l'opportunità qui, con alcuni strumenti di gestione del disco, di formattare il disco o eliminare singole partizioni.

Inoltre, è importante notare in questa schermata che non è necessario fare nulla qui con la maggior parte delle nuove installazioni di server. Puoi vedere, nello screenshot seguente, che c'è un pulsante Nuovo che può essere utilizzato per creare manualmente le partizioni del disco rigido, e così tanti amministratori presumono di doverlo fare per installare il loro nuovo sistema operativo.



Questo non è il caso. Non è necessario creare partizioni a meno che non si desideri configurarle manualmente per qualche motivo specifico. Se il tuo disco rigido è solo un mucchio di spazi vuoti e non allocati, tutto ciò che devi fare è fare clic su Avanti e l'installazione di Windows Server 2019 configurerà le partizioni per te.

Questo è tutto! Vedrai che il programma di installazione del server inizierà ad andare in città a copiare file, installare funzionalità e preparare tutto sul disco rigido. Questa parte del programma di installazione viene eseguita da sola per alcuni minuti e la prossima volta che dovrai interagire con il server sarà all'interno dell'interfaccia grafica in cui potrai definire la password dell'amministratore. Una volta scelta una password, ti troverai sul desktop di Windows. Ora sei davvero pronto per iniziare a utilizzare il tuo nuovo Windows Server 2019.

Installazione di ruoli e funzionalità

L'installazione del sistema operativo mette il piede nella porta, per così dire, utilizzando il server come un server. Tuttavia, a questo punto non puoi effettivamente fare nulla di utile con il tuo server. Su un sistema desktop client, il sistema operativo di base è generalmente tutto ciò che è necessario per iniziare a lavorare e consumare dati. Il compito del server è di fornire quei dati in primo luogo e, fino a quando non dici al server qual è il suo scopo nella vita, non c'è davvero nulla di utile che accade in quel sistema operativo di base. È qui che dobbiamo utilizzare ruoli e funzionalità. Windows Server 2019 contiene molte opzioni diverse per i ruoli. Un ruolo è proprio ciò che il nome implica: l'installazione di un particolare ruolo su un server definisce il ruolo di quel server nella rete. In altre parole, un ruolo dà a un server uno scopo nella vita. Una caratteristica, d'altra parte, è più un sottoinsieme di funzioni che puoi installare su un server. Le funzionalità possono integrare ruoli particolari o stare in piedi da sole. Ci sono parti di tecnologia disponibili in Windows Server 2019 che non sono installate o attivate per impostazione predefinita, perché queste funzionalità non verrebbero utilizzate in tutte le circostanze. Tutto nei capitoli successivi di questo libro ruota attorno alla funzionalità fornita da ruoli e caratteristiche. Sono il pane quotidiano di un server Windows e, senza la loro installazione, i tuoi server fanno buoni fermacarte, ma non molto altro. Poiché in ogni capitolo non dedicheremo tempo per coprire l'installazione di ogni particolare ruolo o caratteristica che verrà utilizzata all'interno del capitolo, lascia '

Installazione di un ruolo utilizzando la procedura guidata

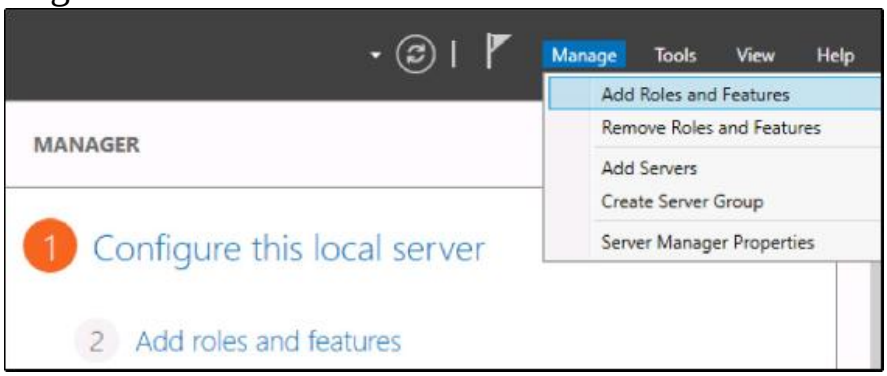
Senza dubbio, il luogo più comune in cui vengono installati ruoli e funzionalità è proprio all'interno delle procedure guidate grafiche disponibili non appena il sistema operativo è stato installato. Per impostazione predefinita, uno strumento chiamato Server Manager si avvia automaticamente ogni volta che accedi a Windows Server 2019.

Daremo un'occhiata più da vicino a Server Manager stesso più avanti in questo capitolo, ma, per i nostri scopi qui, lo useremo semplicemente come piattaforma di lancio per arrivare al nostro wizard che ci guiderà attraverso l'installazione del nostro primo ruolo su questo nuovo server che stiamo mettendo insieme.

Dato che hai appena effettuato l'accesso a questo nuovo server, dovresti iniziare a guardare il Server Manager Dashboard. Proprio al centro della dashboard, vedrai alcuni link disponibili su cui fare clic, un elenco di avvio rapido di elementi di azione numerati da uno a cinque. Se non l'hai già fatto, metti in atto qualsiasi configurazione del server locale di cui potresti aver bisogno su questa macchina attraverso il primo collegamento che si chiama Configura questo server locale.

Gli elementi che probabilmente vorrai posizionare sono cose come un nome host permanente per il server, indirizzi IP e, se stai unendo questo server a un dominio esistente, in genere gestisci quel processo prima di implementare qualsiasi nuovo ruolo sul server. Ma, nel nostro caso, siamo più specificamente interessati all'installazione del ruolo stessa, quindi presumeremo che tu abbia già configurato questi piccoli bit e pezzi in modo che il tuo server sia identificato e instradato sulla tua rete.

Vai avanti e fai clic sul passaggio 2, Aggiungi ruoli e funzionalità. Un altro modo per avviare la stessa procedura guidata è fare clic sul menu Gestisci dalla barra in alto all'interno di Server Manager, quindi scegliere Aggiungi ruoli e funzionalità dall'elenco a discesa. Selezionando uno dei collegamenti si accederà alla nostra procedura guidata per l'installazione del ruolo stesso. Questo è mostrato nella seguente schermata:



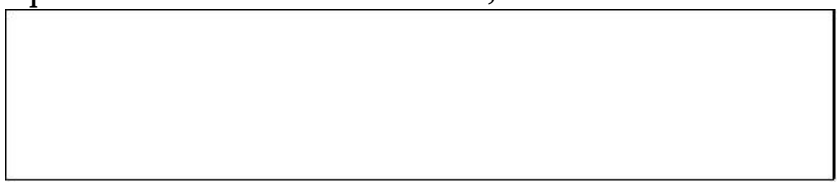
Si viene prima portati a una schermata di riepilogo sull'installazione dei ruoli. Vai avanti e fai clic su Avanti per ignorare questa schermata. Ora passiamo alla nostra prima opzione, che è interessante. Innanzitutto ci viene chiesto se vogliamo continuare con un'installazione basata sui ruoli o basata sulle funzionalità, che è esattamente ciò di cui abbiamo parlato. Ma la seconda opzione qui, l'installazione di Servizi Desktop remoto, è importante da notare. La maggior parte di noi considera i componenti di Servizi Desktop remoto (RDS) di un server Windows come un altro ruolo che possiamo scegliere durante la configurazione del nostro server, simile all'installazione di qualsiasi altro ruolo. Sebbene ciò sia fondamentalmente vero, è importante notare che RDS è così funzionalmente diverso dagli altri tipi di ruoli che il percorso di ingresso

nell'installazione di qualsiasi componente RDS richiama la propria procedura guidata, scegliendo qui la seconda opzione. Quindi, se ti trovi mai alla ricerca dell'opzione per installare RDS e hai guardato su questa schermata perché sei così abituato a fare clic su Avanti come me, ricorda che devi tornare lì per dire alla procedura guidata che si desidera gestire un componente RDS e il resto delle schermate si adatterà di conseguenza.

Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.

Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Al momento, sto lavorando alla creazione di un nuovo laboratorio di test pieno di scatole di Windows Server 2019 e ho ancora bisogno di un controller di dominio per gestire Active Directory nel mio ambiente. Prima di installare Active Directory su un server, è fondamentale disporre di alcuni prerequisiti, quindi ho già completato questi elementi sul mio nuovo server. Gli elementi che devo avere in atto prima dell'installazione del ruolo di Servizi di dominio Active Directory sono: avere un indirizzo IP statico assegnato e assicurarmi che l'impostazione del server DNS nelle mie proprietà NIC punti da qualche parte, anche se solo all'indirizzo IP di questo server. Devo anche assicurarmi che il nome host del mio server sia impostato sul suo nome finale, perché una volta trasformato in un controller di dominio non è supportato per cambiare il nome host. Ho già realizzato questi elementi sul mio server,



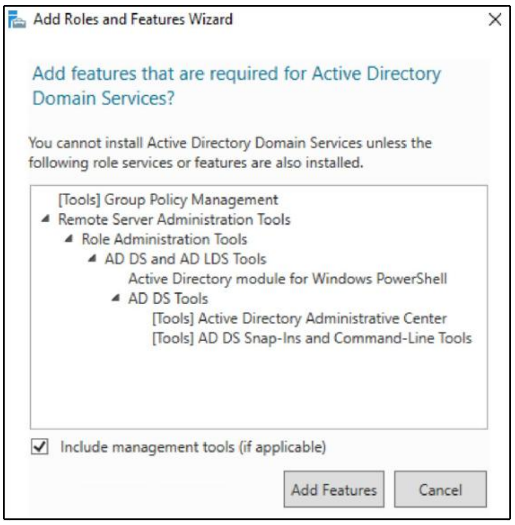
La nostra schermata di selezione del server è molto potente. Se hai già eseguito questo processo in precedenza, probabilmente hai passato in rassegna questa schermata, facendo semplicemente clic sul pulsante Avanti per procedere. Ma, essenzialmente, ciò che questa schermata sta facendo è chiederti dove vorresti installare questo nuovo ruolo o funzionalità. Per impostazione predefinita, ogni server avrà solo se stesso elencato in questa schermata, quindi fare clic su Avanti per continuare è più che probabile quello che farai. Ma ci sono un paio di ottime opzioni qui. Prima di tutto, se il tuo Server Manager è a conoscenza di altri server nella tua rete ed è stato configurato per monitorarli, qui avrai la possibilità di installare un ruolo o una funzionalità in remoto su uno degli altri server. Approfondiremo a breve questa capacità. Un'altra caratteristica in questa pagina, che non ho Visto che molte persone utilizzano, è la possibilità di specificare che si desidera installare un ruolo o una funzionalità su un disco rigido virtuale.

Molti di noi lavorano con la maggior parte dei server virtuali al giorno d'oggi e non è nemmeno necessario che il server virtuale sia in esecuzione per installare un ruolo o una funzionalità! Se hai accesso al file .VHDX, il file del disco rigido, da cui stai eseguendo Server Manager, puoi scegliere questa opzione che ti consentirà di inserire il nuovo ruolo o funzionalità direttamente nel disco rigido. Ma, come nel caso del 99% delle volte che vagherai per questa schermata, siamo collegati direttamente al server in cui intendiamo installare il ruolo, quindi facciamo semplicemente clic su Avanti. Molti di noi lavorano con la maggior parte dei server virtuali al giorno d'oggi e non è nemmeno necessario che il server virtuale sia in esecuzione per installare un ruolo o una funzionalità! Se hai accesso al file .VHDX, il file del disco rigido, da cui stai eseguendo Server Manager, puoi scegliere questa opzione che ti consentirà di inserire il nuovo ruolo o funzionalità direttamente nel disco rigido. Ma, come nel caso del 99% delle volte che vagherai per questa schermata, siamo collegati direttamente al server in cui intendiamo installare il ruolo, quindi facciamo semplicemente clic su Avanti. Molti di noi lavorano con la maggior parte dei server virtuali al giorno d'oggi e non è nemmeno necessario che il server virtuale sia in esecuzione per installare un ruolo o una funzionalità! Se hai accesso al file .VHDX, il file del disco rigido, da cui stai eseguendo Server Manager, puoi scegliere questa opzione che ti consentirà di inserire il nuovo ruolo o funzionalità direttamente nel disco rigido. Ma, come nel caso del 99% delle volte che vagherai per questa schermata, siamo collegati direttamente al server in cui intendiamo installare il ruolo, quindi facciamo semplicemente clic su Avanti. puoi scegliere questa opzione che ti permetterà di inserire il nuovo ruolo o funzionalità direttamente nel disco rigido. Ma, come nel caso del 99% delle volte che vagherai per questa schermata, siamo collegati direttamente al server in cui intendiamo installare il ruolo, quindi facciamo semplicemente clic su Avanti. puoi scegliere questa opzione che ti permetterà di inserire il nuovo ruolo o funzionalità direttamente nel disco rigido. Ma, come nel caso del 99% delle volte che vagherai per questa schermata, siamo collegati direttamente al server in cui intendiamo installare il ruolo, quindi facciamo semplicemente clic su Avanti.

Questo è mostrato nella seguente schermata:

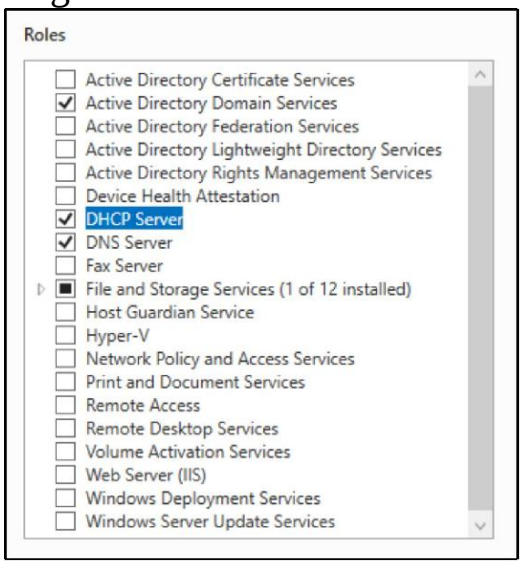
Ora abbiamo il nostro elenco di ruoli disponibili per essere installati. Fare clic su ciascun ruolo ti darà una breve descrizione dello scopo di quel ruolo se hai domande, e parleremo anche di più dei pezzi infrastrutturali fondamentali nel nostro prossimo capitolo per darti ancora più informazioni su ciò che fanno i ruoli. Tutto quello che dobbiamo fare qui per installare un ruolo sul nostro nuovo server è selezionare la casella e fare clic su Avanti. Poiché questo sarà un controller di dominio, sceglierò il ruolo Servizi di dominio Active Directory e utilizzerò questo server in modo che sia anche un server DNS e un server DHCP. Con questi ruoli, non è necessario rieseguire questa procedura guidata tre volte separate per installare tutti questi ruoli, posso semplicemente controllarli tutti qui e lasciare che la procedura guidata esegua i programmi di installazione insieme.

Spiacenti, quando ho fatto clic sulla mia prima casella di controllo, ho ricevuto un messaggio popup che il ruolo di Servizi di dominio Active Directory richiede alcune funzionalità aggiuntive per funzionare correttamente. Questo è un comportamento normale e noterai che molti dei ruoli installati richiederanno l'installazione di alcuni componenti o funzionalità aggiuntivi. Tutto quello che devi fare è fare clic sul pulsante Aggiungi funzionalità e aggiungerà automaticamente questi pezzi extra per te durante il processo di installazione. Un esempio di ciò è mostrato nella seguente schermata:



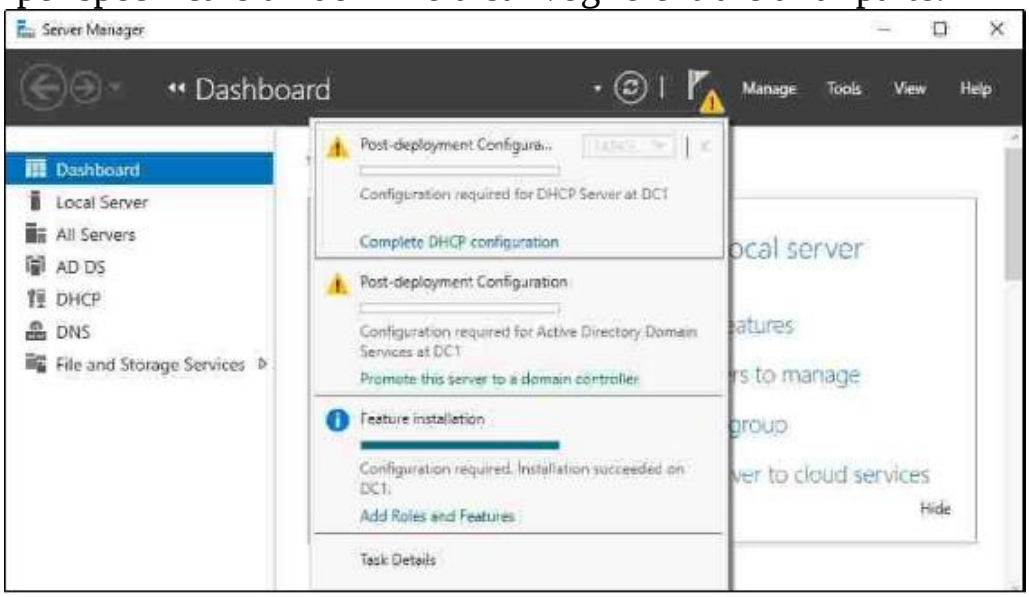
Ora che abbiamo controllato tutti e tre i nostri ruoli, è il momento di fare clic su Avanti. E, giusto per chiarire a tutti voi lettori, non mi è stato richiesto di installare tutti questi ruoli contemporaneamente, non sono tutti dipendenti l'uno dall'altro. È molto comune vedere questi ruoli tutti installati sullo stesso server, ma potrei suddividerli sui loro server se lo desiderassi. In un ambiente più ampio, potresti avere AD DS e DNS installati insieme, ma potresti scegliere di inserire il ruolo DHCP nei propri server, e questo va benissimo.

Sto configurando questo server per supportare un piccolo ambiente di laboratorio, quindi, per me, ha senso mettere insieme questi servizi di infrastruttura di base nella stessa scatola, come mostrato nello screenshot seguente:



Dopo aver fatto clic su Avanti, siamo ora arrivati alla pagina in cui possiamo installare funzionalità aggiuntive per Windows Server 2019. In alcuni casi, potresti aver originariamente inteso solo per aggiungere una funzionalità particolare, e in questi casi, avresti bypassato il Server Schermata dei ruoli e si passa immediatamente alla schermata di installazione delle funzionalità. Proprio come con la schermata di installazione del ruolo, vai avanti e seleziona tutte le funzionalità che desideri installare e fai di nuovo clic su Avanti. Per il nostro nuovo controller di dominio, attualmente non richiediamo l'aggiunta specifica di funzionalità aggiuntive, quindi finirò semplicemente la procedura guidata che avvia l'installazione dei nostri nuovi ruoli.

Al termine del processo di installazione, potrebbe essere richiesto o meno di riavviare il server, a seconda dei ruoli o delle funzionalità installate e se richiedono o meno un riavvio. Una volta rientrato in Server Manager, noterai che ora ti viene richiesto in alto con un punto esclamativo giallo. Facendo clic qui vengono visualizzati messaggi su ulteriori configurazioni che potrebbero essere necessarie per completare l'impostazione dei nuovi ruoli e renderli attivi sul server. I ruoli per Servizi di dominio Active Directory, DNS e DHCP sono ora installati correttamente, ma ora è necessaria una configurazione aggiuntiva per consentire a tali ruoli di svolgere il proprio lavoro. Ad esempio, per completare la trasformazione del mio server in un controller di dominio, devo eseguire un processo di promozione per definire il mio dominio o per specificare un dominio a cui voglio entrare a far parte.

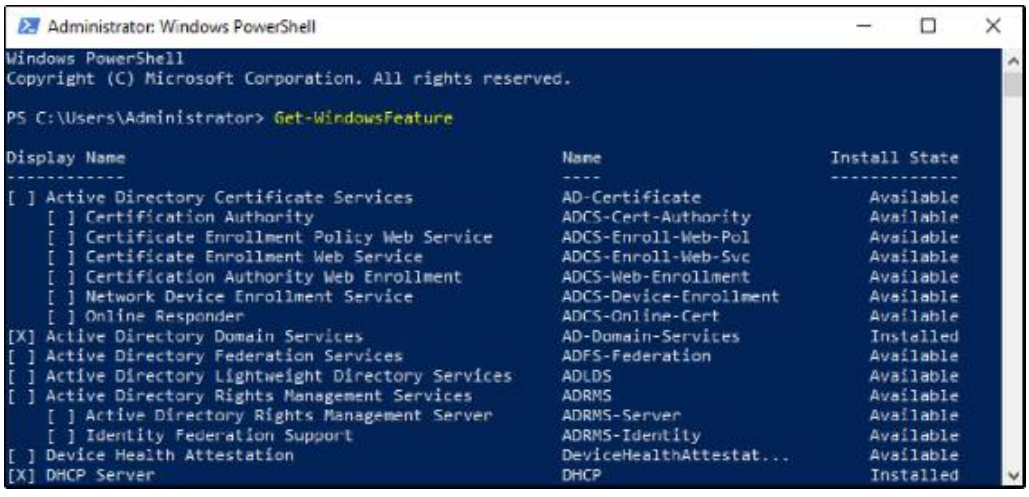


Installazione di una funzionalità tramite PowerShell

Ora che hai visto le procedure guidate grafiche per l'installazione di ruoli e funzionalità, potresti sicuramente usarle sempre per mettere questi componenti in posizione sui tuoi server. Ma Microsoft si è impegnata molto nella creazione di un ambiente Windows Server in cui quasi tutto all'interno del sistema operativo può essere manipolato utilizzando PowerShell e l'aggiunta di ruoli e funzionalità è certamente inclusa in tali funzionalità. Diamo un'occhiata ai comandi appropriati che possiamo usare per manipolare ruoli e funzionalità sul nostro server direttamente da un prompt di PowerShell. Visualizzeremo l'elenco disponibile di ruoli e funzionalità e invieremo anche un comando per installare una funzione rapida sul nostro server.

Apri un prompt di PowerShell con privilegi elevati, più facilmente eseguibile tramite il menu delle attività di amministrazione rapide, accessibile facendo clic con il pulsante destro del mouse sul pulsante Start. Quindi utilizzare il seguente comando per visualizzare tutti i ruoli e le funzionalità disponibili che possiamo installare sul nostro server. Ti mostrerà anche quali sono attualmente installati:

Get-WindowsFeature

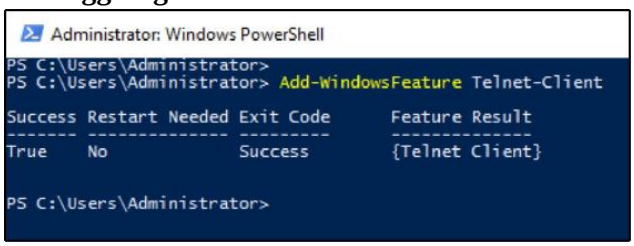


Quello che vorrei fare su questo server è installare la funzionalità del client Telnet. Uso Telnet Client abbastanza regolarmente per testare le connessioni di rete, quindi è utile averlo su questa macchina. Sfortunatamente, la mia finestra di PowerShell contiene attualmente pagine e pagine con ruoli e funzionalità diversi e non sono sicuro di quale sia il nome esatto della funzionalità del client Telnet per installarla. Quindi, eseguiamo di nuovo Get-WindowsFeature, ma, questa volta, utilizziamo una sintassi aggiuntiva nel comando per ridurre la quantità di informazioni visualizzate. Voglio vedere solo le caratteristiche che iniziano con le lettere TEL, come mostrato nei seguenti esempi:

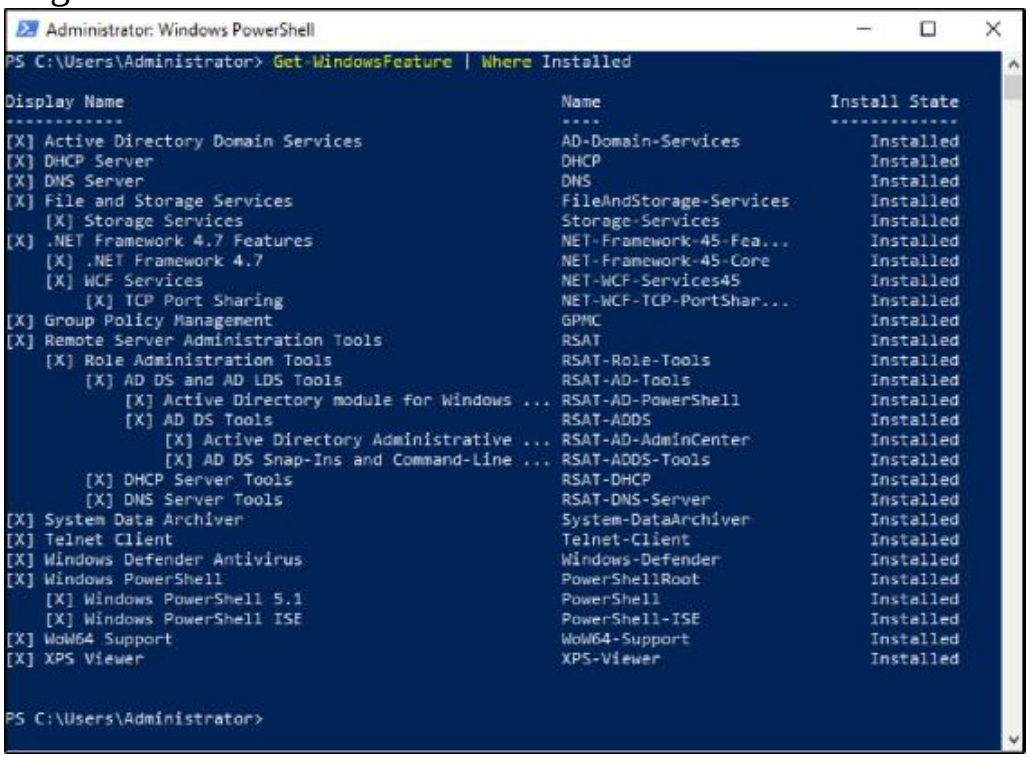
Get-WindowsFeature -Name TEL *

Eccolo! Ok, quindi ora che conosco il nome corretto della funzione, eseguiamo il comando per installarla, come mostrato nei seguenti esempi:

Aggiungi-WindowsFeature Telnet-Client



Un'ultima cosa da mostrarti qui, c'è anche un modo per manipolare il cmdlet Get- WindowsFeature per mostrare rapidamente solo i ruoli e le funzionalità attualmente installati su un server. Digitando Get-WindowsFeature | Where Installed ci presenta un elenco dei componenti attualmente installati. Se lo eseguo sul mio controller di dominio, puoi vedere tutte le parti e le parti dei miei ruoli per Servizi di dominio Active Directory, DNS e DHCP, come mostrato nello screenshot seguente:



Gestione e monitoraggio centralizzati

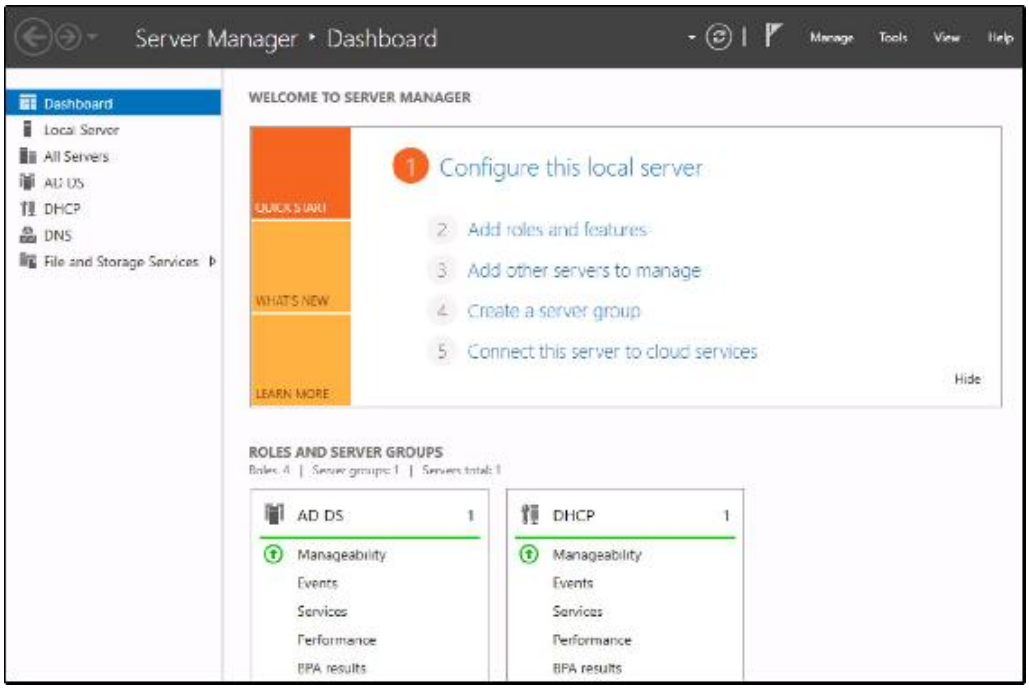
Che tu stia installando nuovi ruoli, eseguendo backup e programmi di manutenzione o risolvendo problemi e riparando un server, è logico che tu acceda al server specifico su cui lavorerai. Molto tempo fa questo significava avvicinarsi al server stesso e accedere con la tastiera e il mouse che erano collegati direttamente a quell'hardware. Poi, un bel po 'di anni fa, questo è diventato complicato e la tecnologia è avanzata al punto in cui ora avevamo a disposizione il protocollo RDP (Remote Desktop Protocol). Siamo passati rapidamente per accedere ai nostri server in remoto utilizzando RDP. Anche se esiste da molti anni, RDP è ancora un protocollo incredibilmente potente e sicuro, che ci offre la possibilità di connettersi rapidamente ai server dalla comodità della nostra scrivania. E, purché si disponga di una topologia di rete e di un instradamento adeguati, puoi lavorare su un server dall'altra parte del mondo con la stessa rapidità di uno seduto nel cubicolo accanto a te. In effetti, ho letto di recente che i diritti di mining venivano concessi nello spazio. Parla di una co-locazione per il tuo datacenter! Forse un giorno useremo RDP per connetterci ai server nello spazio. Anche se questo potrebbe essere un limite nella nostra vita, ho l'opportunità di lavorare con dozzine di nuove aziende ogni anno e, sebbene siano disponibili altri strumenti per la gestione remota della tua infrastruttura server, RDP è la piattaforma preferita per il 99% di noi là fuori. Forse un giorno useremo RDP per connetterci ai server nello spazio. Anche se questo potrebbe essere un allungamento della nostra vita, ho l'opportunità di lavorare con dozzine di nuove aziende ogni anno e, sebbene siano disponibili altri strumenti per la gestione remota della tua infrastruttura server, RDP è la piattaforma preferita per il 99% di noi là fuori. Forse un giorno useremo RDP per connetterci ai server nello spazio. Anche se questo potrebbe essere un limite nella nostra vita, ho l'opportunità di lavorare con dozzine di nuove aziende ogni anno e, sebbene siano disponibili altri strumenti per la gestione remota della tua infrastruttura server, RDP è la piattaforma preferita per il 99% di noi là fuori.

Perché parlare di RDP? Perché ora ti dirò che Windows Server 2019 include alcuni strumenti che lo rendono molto meno necessario per il nostro flusso di lavoro quotidiano. L'idea della gestione centralizzata nel mondo dei server è cresciuta grazie alle ultime implementazioni del sistema operativo Windows Server. La maggior parte di noi ha così tanti server in esecuzione che il check-in con loro tutti i giorni richiederebbe troppo tempo. Abbiamo bisogno di alcuni strumenti che possiamo utilizzare per rendere più efficienti i nostri processi di gestione e monitoraggio, e persino di configurazione, al fine di liberare tempo per progetti più importanti.

Server Manager

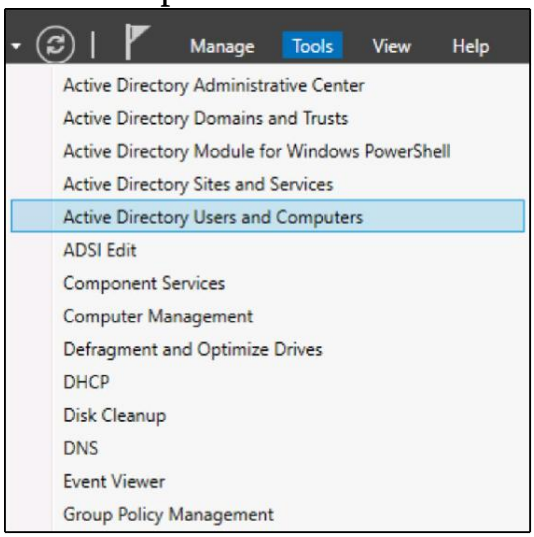
Se hai lavorato di recente su un server Windows, hai familiarità con l'idea che l'accesso a uno dei tuoi server richiami automaticamente questa grande finestra nella parte superiore del desktop. Questo programma ad avvio automatico è Server Manager. Come suggerisce il nome, è qui per aiutarti a gestire il tuo server. Tuttavia, in base alla mia esperienza, la maggior parte degli amministratori di server non utilizza Server Manager. Invece, lo chiudono il più velocemente possibile e lo bestemmiano sottovoce, perché è spuntato fuori e li ha infastiditi durante ogni accesso al server negli ultimi 10 anni.

Smettila! È qui per aiutarti, lo prometto. Lo screenshot seguente mostra la visualizzazione predefinita di Server Manager sul mio nuovo controller di dominio:



Quello che mi piace di questa apertura automatica è che mi dà una rapida occhiata a ciò che è attualmente installato sul server. Guardando la colonna sul lato sinistro viene visualizzato l'elenco dei ruoli installati e disponibili per la gestione. Facendo clic su ciascuno di questi ruoli si accede ad alcune configurazioni e opzioni più particolari per il ruolo stesso. Spesso mi ritrovo a saltare avanti e indietro tra molti server diversi mentre lavoro a un progetto, e lasciando Server Manager aperto mi dà un modo rapido per ricontrollare che sto lavorando sul server corretto. Molto interessante anche la sezione Ruoli e gruppi di server in basso. Potresti non essere in grado di vedere i colori nell'immagine, ma questo ti dà una visione molto rapida del fatto che i servizi in esecuzione su questo server stiano funzionando correttamente o meno. Proprio adesso, entrambe le mie funzioni AD DS e DHCP funzionano normalmente, ho una bella barra verde che le attraversa. Ma, se qualcosa non andava con uno di questi ruoli, sarebbe stato contrassegnato in rosso brillante e potevo fare clic su uno qualsiasi dei collegamenti elencati sotto quelle intestazioni di ruolo per rintracciare qual è il problema.

In alto vicino all'angolo in alto a destra vedi alcuni menu, il più utile dei quali, per me, è il menu Strumenti. Fare clic su questo e verrà visualizzato un elenco di tutti gli strumenti di amministrazione disponibili da avviare su questo server. Sì, si tratta essenzialmente della stessa cartella Strumenti di amministrazione che esisteva in ciascuna delle versioni precedenti di Windows Server, ora archiviata in una posizione diversa. Sulla base della mia esperienza, Server Manager è ora il modo più semplice per accedere a questa miriade di strumenti tutti da un'unica posizione:

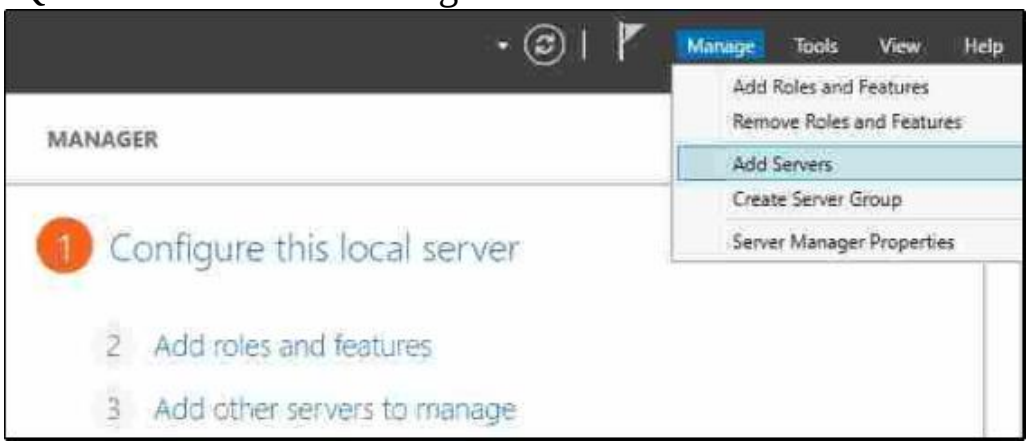


Finora le funzioni all'interno di Server Manager che abbiamo discusso sono disponibili su qualsiasi Windows Server 2019, sia esso autonomo o parte di un dominio. Tutto ciò che abbiamo fatto riguarda solo il server locale a cui abbiamo effettuato l'accesso. Ora, esploriamo le opzioni disponibili in Server Manager per la centralizzazione della gestione su più server. La nuova mentalità di gestire molti server da un singolo server viene spesso definita gestione da un unico pannello di controllo. Useremo Server Manager su uno dei nostri server nella rete per effettuare connessioni a server aggiuntivi, e dopo averlo fatto dovremmo avere molte più informazioni all'interno di Server Manager che possiamo usare per tenere sotto controllo tutti quei server.

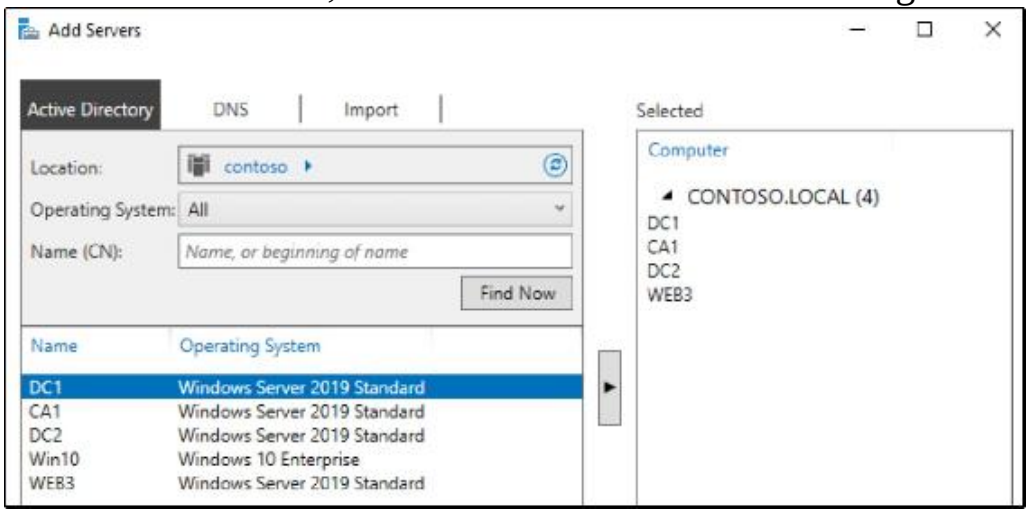
Davanti e al centro all'interno della console di Server Manager si trova la sezione intitolata Benvenuti in Server Manager. Sotto di ciò abbiamo una serie di passaggi o collegamenti su cui è possibile fare clic. Il primo

consente di configurare impostazioni specifiche solo per questo server locale. Abbiamo già lavorato con il secondo passaggio quando abbiamo aggiunto un nuovo ruolo al nostro server. Ora testeremo il terzo passaggio, Aggiungi altri server da gestire.

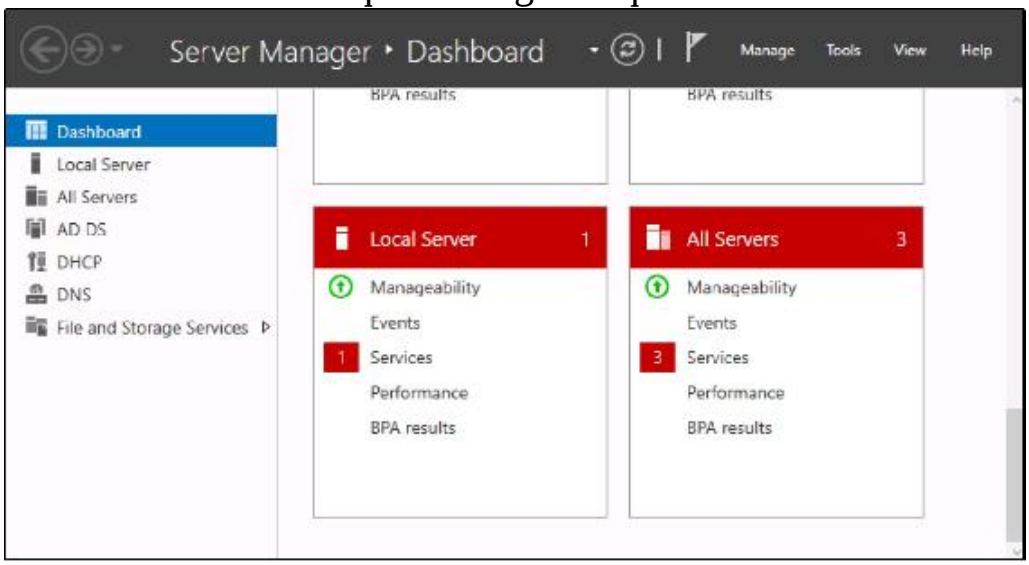
A proposito, questa stessa funzione può essere chiamata anche facendo clic sul menu Gestisci in alto e quindi scegliendo Aggiungi server. Questo è mostrato nella seguente schermata:



La maggior parte di voi lavorerà all'interno di un ambiente di dominio in cui i server sono tutti aggiunti a un dominio, il che rende questa parte successiva davvero semplice. È sufficiente fare clic sul pulsante Trova ora e verranno visualizzate le macchine disponibili nella rete. Da qui, puoi scegliere i server che desideri gestire e spostarli nella colonna Selezionati a destra, come mostrato nello screenshot seguente:

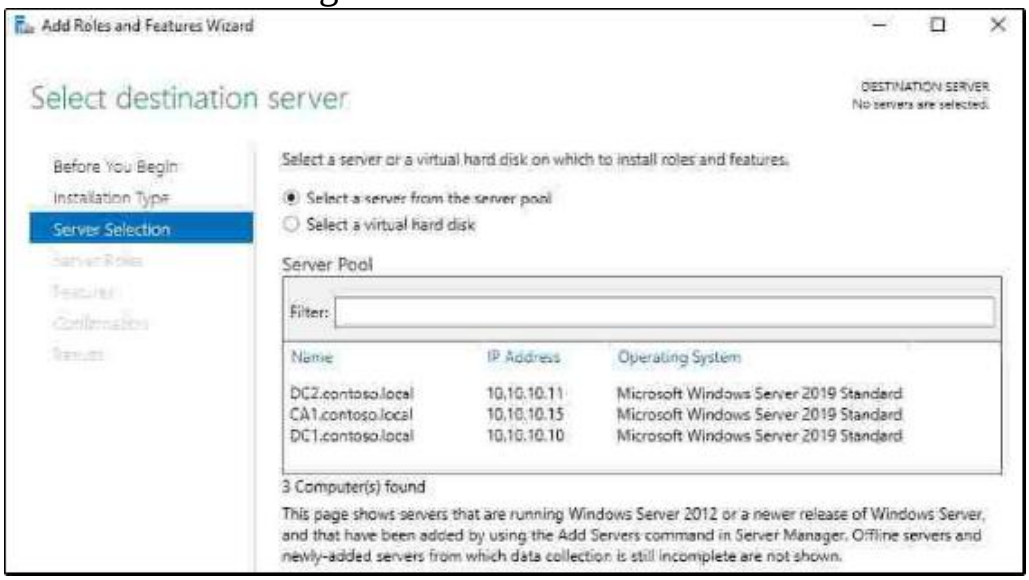


Dopo aver fatto clic su OK, vedrai che Server Manager si è trasformato per darti maggiori informazioni su tutti questi server e ruoli installati su di essi. Ora, quando accedi a questo singolo server, visualizzi immediatamente le informazioni di manutenzione critiche su tutti i sistemi che hai scelto di aggiungere qui. È anche possibile utilizzare un server separato, destinato esclusivamente ai fini di questa gestione. Ad esempio, sono attualmente connesso a un server nuovo di zecca chiamato CA1. Non ho alcun ruolo installato su questo server, quindi, per impostazione predefinita, Server Manager sembra piuttosto semplice. Non appena aggiungo altri server (i miei controller di dominio) da gestire, il mio Server Manager sul server CA1 ora contiene tutti i dettagli su CA1 e sui miei controller di dominio, quindi posso visualizzare tutti gli aspetti della mia infrastruttura da questo singolo riquadro.



Facendo clic sul collegamento Tutti i server o su uno dei ruoli specifici, si ottengono informazioni ancora più complete raccolte da questi server remoti. L'aggiunta di più server in Server Manager non è utile solo per il monitoraggio, ma anche per configurazioni future. Ricordi poche pagine fa quando abbiamo aggiunto un nuovo ruolo utilizzando la procedura guidata? Questo processo si è ora evoluto per diventare più completo, poiché ora abbiamo inserito questo server negli altri nostri server nella rete.

Se ora scelgo di aggiungere un nuovo ruolo, quando arrivo alla schermata che mi chiede dove voglio installare quel ruolo, vedo che posso scegliere di installare un nuovo ruolo o funzionalità su uno dei miei altri server, anche se lo sono non funziona dalla console di quei server, come mostrato nello screenshot seguente:



Se volessi installare il ruolo di Servizi di dominio Active Directory su DC2, un server che sto preparando come secondo controller di dominio nel mio ambiente, non dovrei accedere al server DC2. Proprio qui, da Server Manager in esecuzione su CA1, potrei eseguire la procedura guidata Aggiungi ruoli, definire DC2 come il server che voglio manipolare e potrei installare il ruolo direttamente da qui.

Strumenti di amministrazione remota del server (RSAT)

Usare Server Manager per accedere a un singolo server e avere accesso per gestire e monitorare tutti i tuoi server è piuttosto utile, ma cosa succederebbe se potessimo fare un ulteriore passo fuori da quel processo? E se ti dicessi che non devi accedere a nessuno dei tuoi server, ma puoi eseguire tutte queste attività dal computer seduto sulla tua scrivania?

Ciò è possibile installando un set di strumenti di Microsoft denominato RSAT (Remote Server Administration Tools). Ho un normale computer client Windows 10 online e in esecuzione nella nostra rete, anch'esso aggiunto a un dominio. Su questo computer voglio scaricare e installare gli strumenti RSAT dal seguente percorso:

https://www.microsoft.com/en-us/download/details.aspx?id=45520.

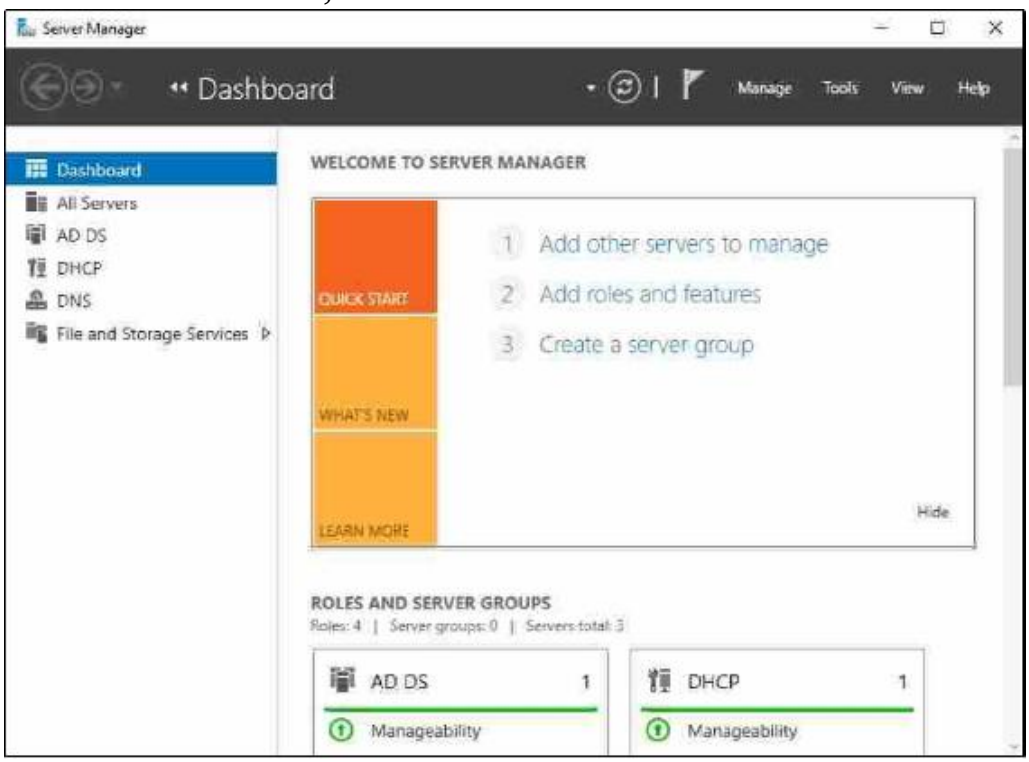
Se ti capita di eseguire Windows 10 1809 o versioni successive, il set di strumenti RSAT è ora incluso in Windows, ma è una funzionalità opzionale che devi abilitare. Ciò si ottiene dalle Impostazioni di Windows, all'interno della categoria App tramite un pulsante chiamato Gestisci funzionalità opzionali

Dopo aver eseguito il programma di installazione sul mio computer client Windows 10, non riesco a trovare alcun programma chiamato Strumento di amministrazione remota del server. Sarebbe corretto. Anche se il nome di questo durante il download e l'installazione è RSAT, dopo l'installazione il programma che viene effettivamente inserito nel computer si chiama Server Manager. Questo ha senso, tranne per il fatto che se non ti rendi conto della discrepanza nel nome, potrebbero essere necessari alcuni minuti per capire perché non riesci a trovare ciò che hai appena installato.

Quindi, vai avanti e avvia Server Manager trovandolo nel menu Start, o usando la barra di ricerca, o anche dicendo Ehi Cortana, apri Server Manager. Scusa, non ho potuto resistere. Ma qualunque sia il tuo metodo, apri Server Manager sul tuo computer desktop e vedrai che sembra e si sente proprio come Server Manager in Windows Server 2019. E, nello stesso modo in cui lavori e lo manipoli all'interno del

sistema operativo del server, puoi eseguire la stessa procedura qui per aggiungere i tuoi server per la gestione.

Nello screenshot seguente, puoi vedere che, all'interno del mio Windows 10 Server Manager, ora ho accesso per gestire e monitorare tutti i server nel mio laboratorio, senza nemmeno doverli accedere:

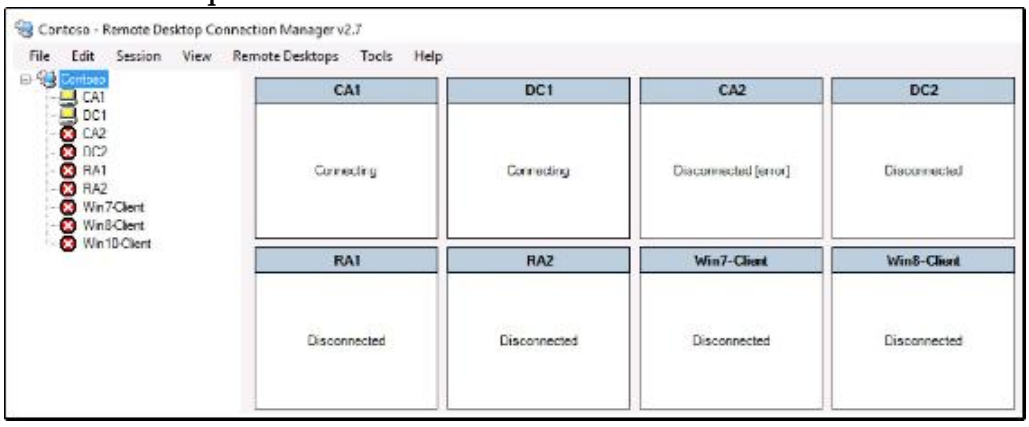


Questo significa che RDP è morto?

Con questi modi nuovi e migliorati per gestire i componenti sottostanti dei tuoi server senza doverli accedere direttamente, significa che il nostro vecchio amico RDP se ne andrà? Certamente no! A volte avremo ancora la necessità di accedere direttamente ai nostri server, anche se andiamo all-in utilizzando i nuovi strumenti di gestione. E mi aspetto anche che molti amministratori continueranno a utilizzare RDP e l'accesso completo basato su desktop per tutta la gestione e il monitoraggio dei loro server semplicemente perché questo è ciò con cui sono più a loro agio, anche se ora esistono modi più nuovi ed efficienti per realizzare il stessi compiti.

Gestione connessione desktop remoto

Poiché la maggior parte di noi utilizza ancora RDP occasionalmente (o spesso) quando rimbalza tra i nostri server, diamo una rapida occhiata a uno strumento che può almeno rendere questa attività più gestibile e centralizzata. Non trascorrerò molto tempo a esaminare le singole funzionalità o capacità di questo strumento, poiché è uno strumento lato client e non qualcosa di specifico di Windows Server 2019. Puoi usarlo per gestire le connessioni RDP per tutti dei tuoi server, o anche tutti i computer client nella tua rete. Tuttavia, Remote Desktop Connection Manager è una piattaforma incredibilmente utile per archiviare tutte le diverse connessioni RDP effettuate all'interno del proprio ambiente. Puoi salvare le connessioni in modo da non dover perdere tempo a cercare di ricordare i nomi dei server, ordinare i server in categorie, e persino memorizzare le credenziali in modo da non dover digitare le password durante la connessione ai server. Sebbene un disclaimer dovrebbe venire con quello, i tuoi addetti alla sicurezza potrebbero non essere contenti se scegli di utilizzare la funzione di memorizzazione della password. Vi lascio con un link per scaricare l'applicazione,https: //www.microsoft.com /en-noi/Scarica/dettagli.aspx?id =44989, così come la seguente schermata, quindi lascia che sia tu a decidere se questo strumento sarebbe utile o meno nelle tue attività quotidiane:



Windows Admin Center (WAC)

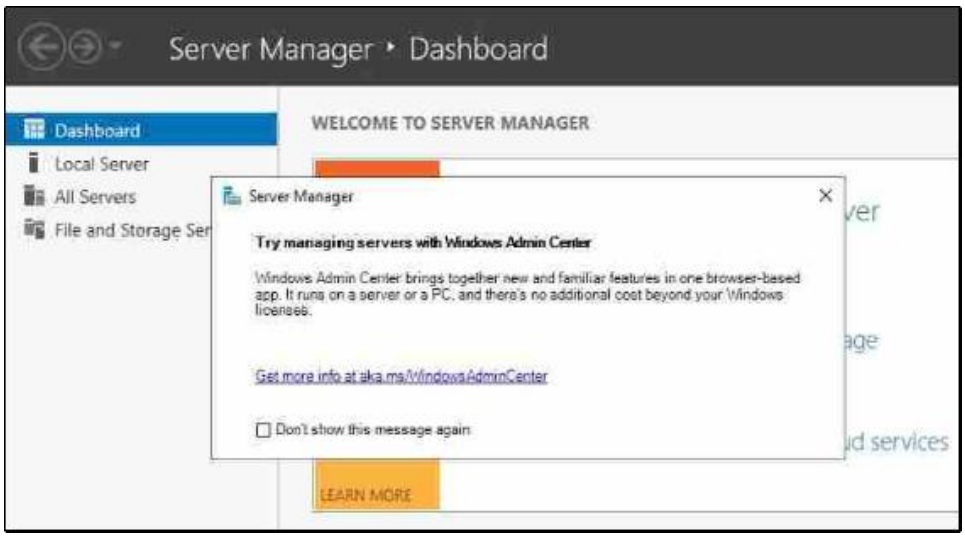
Ora dimentica tutto ciò che ti ho appena detto sulla gestione del server remoto e concentrati invece qui. Sto solo scherzando, più o meno. Tutti gli strumenti che abbiamo già discusso sono ancora stabili, pertinenti e ottimi modi per interagire e gestire i tuoi gruppi di server Windows. Tuttavia, c'è un nuovo ragazzo in città e Microsoft si aspetta che diventi molto popolare.

Windows Admin Center (WAC) è una piattaforma di gestione client e server progettata per aiutarti ad amministrare le tue macchine in modo più efficiente. Questo è uno strumento basato su browser, il che significa che, una volta installato, accedi a WAC da un browser web, il che è fantastico. Non è necessario installare uno strumento di gestione o un'applicazione sulla workstation, è sufficiente sedersi e toccarlo con un URL.

WAC può gestire i tuoi server (fino a Server 2008 R2), i tuoi cluster di server e ha anche alcune funzionalità speciali per la gestione dei cluster dell'infrastruttura iperconvergente. Puoi anche gestire le macchine client nella versione Windows 10.

Qual è il costo per uno strumento così straordinario e potente? GRATUITO! E è probabile che se hai seguito l'attività di Microsoft nell'ultimo anno, potresti persino averlo già visto in una forma o nell'altra. Le parole Project Honolulu suonano familiari? Sì, Windows Admin Center è un progetto rinominato Honolulu, finalmente pronto per l'uso in produzione.

Windows Admin Center ha anche il supporto per i fornitori di terze parti per essere in grado di creare estensioni per l'interfaccia WAC, quindi questo strumento continuerà a crescere. Se finora hai seguito la configurazione del laboratorio di test nel libro, riconoscerai Windows Admin Center da una finestra pop-up che viene visualizzata ogni volta che Server Manager viene aperto. Microsoft vuole che gli amministratori conoscano il WAC così tanto che ti stanno ricordando che dovresti iniziare a usarlo ogni volta che accedi a una casella Server 2019, come mostrato nello screenshot seguente:

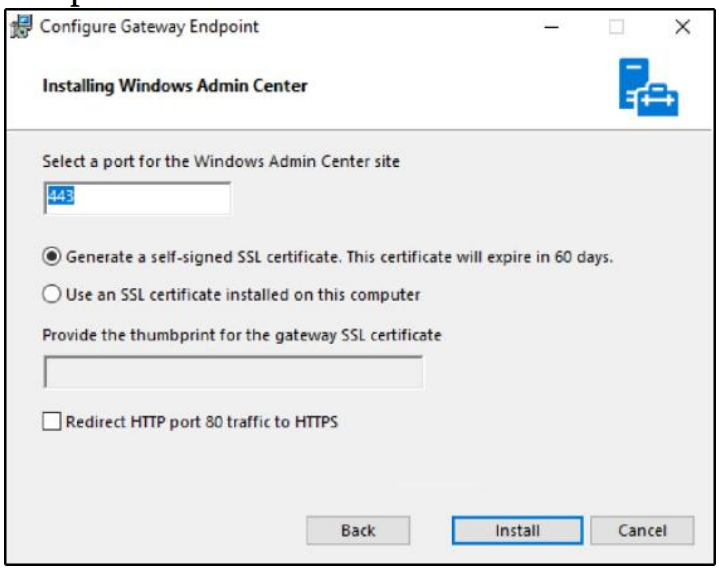

Server Manager ▸ Dashboard
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Server Manager
Try managing servers with Windows Admin Center
Windows Admin Center brings together new and familiar features in one browser-based app. It runs on a server or a PC, and there's no additional cost beyond your Windows licenses.
Get more info at aka.ms/WindowsAdminCenter
Don't show this message again
LEARN MORE

Installazione di Windows Admin Center

Basta parlare, proviamolo! Per prima cosa dobbiamo scegliere una posizione in cui installare i componenti di WAC. È vero, ho detto che uno dei vantaggi era che non avevamo bisogno di installarlo, ma quello che volevo dire era che una volta implementato il WAC, attingerlo è facile come aprire un browser. Quel sito web deve essere installato e funzionante da qualche parte, giusto? Sebbene tu possa lanciare l'intero sistema WAC su un client Windows 10, prendiamo l'approccio che sarà più comunemente utilizzato sul campo e installiamolo su un server nella nostra rete. Ho un sistema in esecuzione chiamato WEB3 che non ospita ancora alcun sito Web, sembra un buon posto per qualcosa del genere.

Scarica WAC da qui: https: //www.microsoft.com /en-noi/nube-piattaforma/finestre-admin-centro.

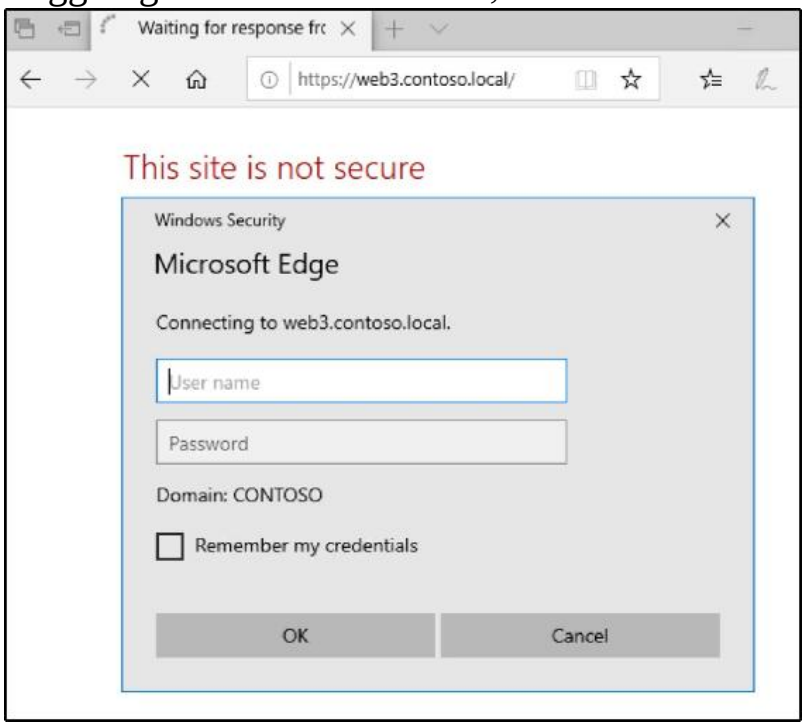
Una volta scaricato, esegui semplicemente il programma di installazione sulla macchina host. Ci sono alcune semplici decisioni che devi prendere durante la procedura guidata, la più evidente è la schermata in cui definisci le impostazioni della porta e del certificato. In un ambiente di produzione, sarebbe meglio eseguire la porta 443 e fornire un certificato SSL valido qui in modo che il traffico da e verso questo sito Web sia adeguatamente protetto tramite HTTPS, ma, per il mio piccolo laboratorio di test, eseguirò 443 con un certificato autofirmato, solo a scopo di test. Non utilizzare certificati autofirmati in produzione!



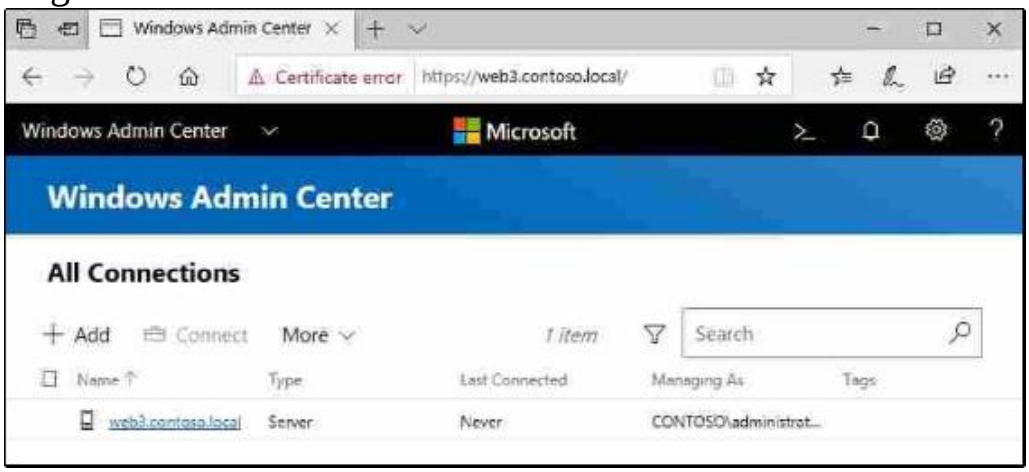
Al termine del programma di installazione, ora ospiterai il sito Web di Windows Admin Center su questo server. Per la mia particolare installazione, quell'indirizzo web
è: https: //WEB3.contoso.local .

Avvio di Windows Admin Center

Ora per la parte divertente, controllando questa cosa. Per accedere a Windows Admin Center, è sufficiente aprire un browser supportato da qualsiasi macchina nella rete e accedere all'URL WAC. Ancora una volta, il mio è https: //WEB3.contoso.local. È interessante notare che Internet Explorer non è un browser supportato, Microsoft consiglia Edge ma funziona anche con Chrome. Ho effettuato l'accesso alla mia workstation Windows 10 e aprirò semplicemente il browser Edge e proverò a raggiungere il mio nuovo sito, come mostrato nello screenshot seguente:

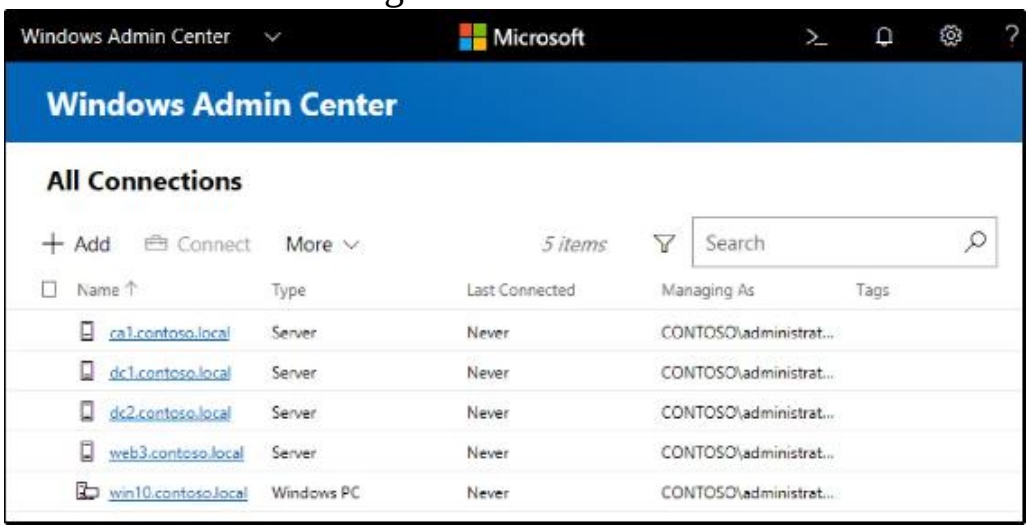


Come puoi vedere, ho a che fare con un avviso di certificato. C'è da aspettarselo perché sto usando un certificato autofirmato, il che, ancora una volta, è una cattiva idea. Lo giustifico solo perché corro in un laboratorio di prova. Ma la parte più interessante dello screenshot precedente è che mi viene presentata una richiesta di credenziali. Anche se ho effettuato l'accesso a un computer Windows 10 che fa parte di un dominio e ho effettuato l'accesso con le credenziali di dominio, il sito Web WAC non tenta automaticamente di iniettare quelle credenziali per il proprio uso, ma piuttosto si ferma per chiedere chi sei. Se inserisco semplicemente le mie credenziali di dominio qui, ora mi viene presentata l'interfaccia di Windows Admin Center, come mostrato nello screenshot seguente:



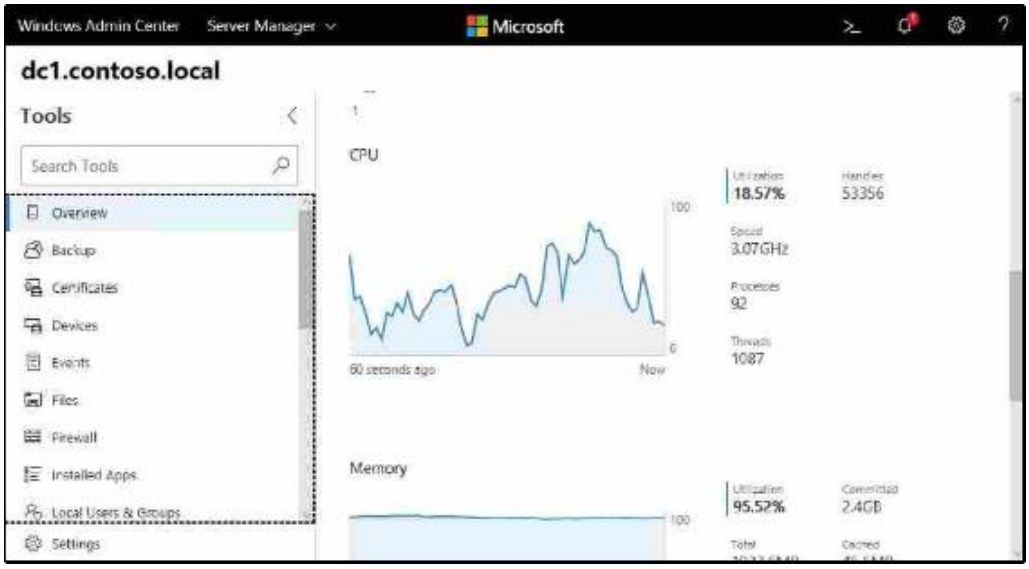
Aggiunta di più server a Windows Admin Center

L'accesso a WAC è ottimo, ma non molto utile finché non si aggiungono un gruppo di macchine che si desidera gestire. Per farlo, fai semplicemente clic sul pulsante + Aggiungi mostrato nello screenshot precedente. Ti verrà presentata la possibilità di aggiungere un nuovo server, un nuovo PC, un cluster di failover o persino un cluster iperconvergente. Effettua la tua selezione e inserisci le informazioni richieste. Non ho cluster nel mio laboratorio di test, non ancora, quindi aggiungerò connessioni ai server standard che ho eseguito nell'ambiente, come mostrato nella seguente schermata:



Gestione di un server con Windows Admin Center

Avviare la gestione di un server dall'interno di WAC è semplice come fare clic sul nome del server. Come puoi vedere nello screenshot seguente, ho selezionato il mio server DC1, poiché attualmente è l'unica macchina con alcuni ruoli reali installati e in esecuzione:



Da questa interfaccia, posso gestire molti aspetti diversi del sistema operativo del mio server DC1. Ci sono funzioni di controllo dell'alimentazione, la possibilità di eseguire backup sul mio server, posso persino installare certificati da qui! È possibile monitorare le prestazioni del server, visualizzare i registri degli eventi, manipolare il Windows Firewall locale e avviare una connessione PowerShell remota al server. L'obiettivo con Windows Admin Center è che sia il tuo punto di riferimento per la gestione remota dei tuoi server e direi che è sulla buona strada per raggiungere tale obiettivo.

Non ho ancora istanze di Server Core in esecuzione nel mio laboratorio, ma ti assicuro che WAC può essere utilizzato per gestire istanze Server Core così come i server che eseguono Desktop Experience. Ciò rende Windows Admin Center ancora più potente e intrigante per gli amministratori del server.

Abilitazione delle implementazioni rapide del server con Sysprep

All'inizio di questo capitolo, abbiamo illustrato il processo di installazione del sistema operativo Windows Server 2019 sul tuo nuovo server. Che si trattasse di un componente hardware fisico o di una macchina virtuale con cui stavamo lavorando, il processo di installazione era essenzialmente lo stesso. Collegare il DVD o la chiavetta USB, avviarlo e lasciare che il programma di installazione faccia il suo corso è una cosa abbastanza facile da fare, ma cosa succede se hai bisogno di costruire dieci nuovi server invece di uno solo? Questo processo inizierebbe presto a diventare noioso e sembrerebbe che tu stia sprecando molto tempo a dover fare la stessa identica cosa più e più volte. Avresti ragione, questo fa perdere molto tempo e c'è un modo più semplice e veloce per implementare nuovi server, purché li crei tutti da una piattaforma hardware relativamente simile.

Ora, prima di approfondire questa strada descrivendo il processo Sysprep, noterò anche che ci sono più tecnologie coinvolte disponibili all'interno dell'infrastruttura di Windows che consentono il sistema operativo automatizzato e le implementazioni dei server che possono rendere il processo di implementazione del nuovo server ancora più semplice di quello che sto descrivendo qui. Il problema con alcune delle tecnologie automatizzate è che l'infrastruttura richiesta per farle funzionare correttamente è più avanzata di quella a cui molte persone avranno accesso se stanno solo imparando le basi con Windows Server. In altre parole, disporre di un meccanismo di implementazione del server completamente automatizzato non è molto fattibile per piccoli ambienti o laboratori di test, che è dove molti di noi vivono mentre impariamo queste nuove tecnologie.

Quindi, in ogni caso, non ci concentreremo su un tipo di approccio automatizzato all'implementazione del server, ma piuttosto faremo qualche minuto di lavoro extra sul nostro primo server, il che si tradurrà in un risparmio di numerosi minuti di lavoro di configurazione su ogni

server che costruiamo in seguito. Il nucleo di questo processo è lo strumento Sysprep, che è integrato in tutte le versioni di Windows, quindi puoi eseguire lo stesso processo su qualsiasi macchina Windows corrente, sia che si tratti di un client o di un server.

Sysprep è uno strumento che prepara il tuo sistema per la duplicazione. Il suo nome ufficiale è lo strumento di preparazione del sistema Microsoft e, per riassumere ciò che fa in una riga, ti consente di creare un'immagine master del tuo server che puoi riutilizzare tutte le volte che vuoi per implementare server aggiuntivi. Un vantaggio chiave dell'utilizzo di Sysprep è che puoi inserire impostazioni personalizzate sul tuo server master e installare cose come gli aggiornamenti di Windows prima di Sysprep, e tutte queste impostazioni e patch esisteranno quindi all'interno della tua immagine master. L'utilizzo di Sysprep consente di risparmiare tempo poiché non è necessario eseguire il processo di installazione del sistema operativo, ma consente di risparmiare ancora più tempo senza dover attendere che gli aggiornamenti di Windows eseguano il roll down di tutte le patch correnti su ogni nuovo sistema creato.
Alcuni di voi potrebbero chiedersi perché Sysprep sia addirittura necessario.

Se volessi clonare il tuo server master, potresti semplicemente usare uno strumento di imaging del disco rigido o, se hai a che fare con macchine virtuali, potresti semplicemente copiare e incollare il file .VHDX stesso per fare una copia del tuo nuovo server , giusto? La risposta è sì, ma il grosso problema è che la nuova immagine o il nuovo disco rigido che hai appena creato sarebbe una replica esatta di quello originale. Il nome host sarebbe lo stesso e, cosa più importante, alcune informazioni di identificazione di base in Windows, come il numero di identificazione di sicurezza (SID) del sistema operativo, sarebbero esattamente le stesse. Se dovessi attivare sia il server master originale che un nuovo server basato su questa replica esatta, causeresti conflitti e collisioni sulla rete poiché questi due server combattono per il loro diritto di essere l'unico server con quel nome univoco e SID. Questo problema si esacerba negli ambienti di dominio, dove è ancora più importante che ogni sistema all'interno della rete abbia un SID / GUID univoco, il loro identificatore all'interno di Active Directory. Se crei copie esatte dei server e le hai entrambe online, diciamo solo che nessuno dei due ne sarà felice.

Sysprep risolve tutti questi problemi inerenti al processo di duplicazione del sistema randomizzando gli identificatori univoci nel sistema operativo. Per prepararci a implementare molti server utilizzando un'immagine master che creiamo con Sysprep, ecco un riepilogo di riferimento rapido dei passaggi che verranno eseguiti:

1. Installa Windows Server 2019 su un nuovo server
2. Configura personalizzazioni e aggiornamenti sul tuo nuovo server
3. Eseguire Sysprep per preparare e arrestare il server principale
4. Crea la tua immagine principale dell'unità
5. Crea nuovi server utilizzando copie dell'immagine master

E ora esaminiamo questi passaggi in modo un po 'più dettagliato.

Installazione di Windows Server 2019 su un nuovo server

Innanzitutto, proprio come hai già fatto, dobbiamo preparare il nostro primo server installando il sistema operativo Windows Server 2019. Astenersi dall'installare ruoli completi sul server, perché, a seconda del ruolo o della sua configurazione univoca, il processo Sysprep che eseguiremo a breve potrebbe causare problemi per le configurazioni dei singoli ruoli. Installa il sistema operativo e assicurati che i driver di dispositivo siano tutti squadrati e sei pronto per il passaggio successivo.

Configurazione di personalizzazioni e aggiornamenti sul tuo nuovo server

Successivamente, si desidera configurare le personalizzazioni e installare gli aggiornamenti sul nuovo server. Ogni impostazione o installazione che puoi eseguire ora che è universale per il tuo gruppo di server ti eviterà di dover fare quel passo sui tuoi server in futuro. Questa parte potrebbe creare confusione perché un minuto fa ti ho detto di non installare i ruoli sul server master. Questo perché l'installazione di un ruolo apporta numerose modifiche al sistema operativo e alcuni dei ruoli che è possibile installare si bloccano su un particolare nome host in esecuzione sul sistema. Se dovessi fare qualcosa di simile a un server principale, quel ruolo verrebbe probabilmente interrotto quando attivato su un nuovo server. Le personalizzazioni che puoi mettere in atto sul server master sono cose come il collegamento di file e cartelle che potresti desiderare su tutti i tuoi server, come una cartella Strumenti di amministrazione o qualcosa del genere. È inoltre possibile avviare o arrestare servizi che si desidera o meno eseguire su ciascuno dei server e modificare le impostazioni nel registro se questo fa parte del normale processo di preparazione o rafforzamento del server. Qualunque siano le modifiche o le personalizzazioni che imposti, non è una cattiva idea eseguire una serie completa di test sul primo nuovo server che crei da questa immagine master, solo per assicurarti che tutte le modifiche siano state apportate tramite il processo Sysprep.

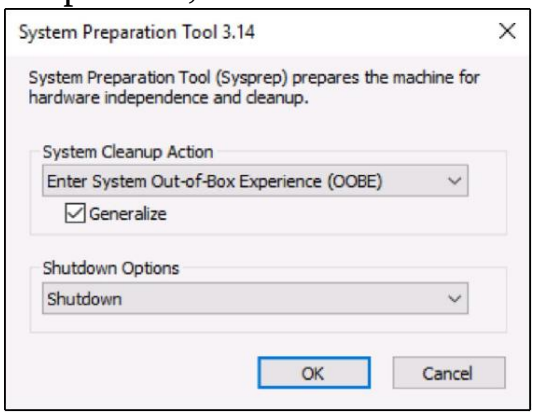
Ora è anche il momento di consentire l'installazione degli aggiornamenti di Windows e di inserire le patch su questo nuovo server che desideri siano installate su tutti i tuoi nuovi server in futuro. Non c'è niente di più frustrante che installare un nuovo sistema operativo in 5 minuti, solo per dover aspettare 4 ore per installare tutti gli aggiornamenti e le patch correnti prima di poter utilizzare il nuovo server. Includendo tutti questi aggiornamenti e patch nell'immagine master, risparmierai tutto il tempo di download e installazione per ogni nuovo server che avvii.

Continua a risparmiare tempo e fatica creando nuove copie delle tue immagini master ogni pochi mesi. In questo modo le patch più recenti sono sempre incluse nella tua immagine master e continua a farti risparmiare sempre più tempo per tutta la vita di Windows Server 2019.

Esecuzione di Sysprep per preparare e arrestare il server principale

Ora che il nostro server principale è stato preparato come vogliamo, è il momento di eseguire lo strumento Sysprep stesso. Per farlo, apri un prompt dei comandi amministrativo e vai a C: \ Windows \ System32 \ Sysprep. Ora puoi utilizzare l'utilità Sysprep.exe all'interno di quella cartella per avviare Sysprep stesso.

Come con molti eseguibili che esegui da un prompt dei comandi, ci sono una varietà di opzioni opzionali che puoi taggare alla fine del tuo comando per fargli eseguire attività specifiche. Dalla finestra del prompt dei comandi, se esegui semplicemente il comando sysprep.exe, vedrai un'interfaccia grafica per Sysprep, dove puoi scegliere tra le opzioni disponibili, come mostrato nello screenshot seguente:



Poiché utilizzo sempre lo stesso set di opzioni per Sysprep, trovo più facile includere semplicemente tutti i miei interruttori opzionali direttamente dall'input della riga di comando, quindi bypassando del tutto la schermata grafica. Di seguito sono riportate alcune informazioni sulle diverse opzioni disponibili per l'utilizzo con sysprep.exe:

- / quiet: indica a Sysprep di essere eseguito senza messaggi di stato sullo schermo.
- / generalize: questo specifica che Sysprep rimuove tutte le informazioni di sistema univoche (SID) dall'installazione di Windows, rendendo l'immagine finale utilizzabile su pi ù macchine nella rete, perch é ogni nuova uscita dall'immagine ne ricever à una nuova, SID unico.
- / audit: questo riavvia la macchina in una modalit à di controllo speciale, in cui hai la possibilit à di aggiungere driver aggiuntivi in Windows prima che venga acquisita l'immagine finale.
- / oobe: indica alla macchina di avviare la procedura guidata di mini-configurazione all'avvio successivo di Windows.
- / reboot: viene riavviato al termine di Sysprep.

- / shutdown: questo arresta il sistema (non un riavvio) al termine di Sysprep. Questo è importante ed è quello che utilizzo di solito.
- / quit: questo chiude Sysprep al termine.
- / unattend: c' è uno speciale answerfile che puoi creare, quando specificato, verrà utilizzato insieme al processo Sysprep per configurare ulteriormente i nuovi server non appena saranno online. Ad esempio, è possibile specificare in questo file di risposte che un particolare programma di installazione o file batch deve essere avviato al primo avvio di Windows dopo Sysprep. Ciò può essere utile per qualsiasi tipo di attività di pulizia che potresti voler eseguire, ad esempio, se sul tuo sistema era presente un file batch che hai utilizzato per eliminare i file di registro dopo il primo avvio di nuovi server.

I due che sono più importanti per i nostri scopi di voler creare un file di immagine principale che possiamo usare per implementazioni rapide del server in futuro sono lo switch / generalize e il
/ interruttore di spegnimento. Generalizzare è molto importante perch é sostituisce tutto ci ò che è unico le informazioni di identificazione, le informazioni SID, nelle nuove copie di Windows disponibili online. Ciò consente ai tuoi nuovi server di coesistere sulla rete con il tuo server originale e con altri nuovi server che porti in linea. Anche l'opzione di arresto è molto importante, perché vogliamo che questo server master diventi sysprep e quindi immediatamente arrestato in modo da poter creare la nostra immagine master da esso.

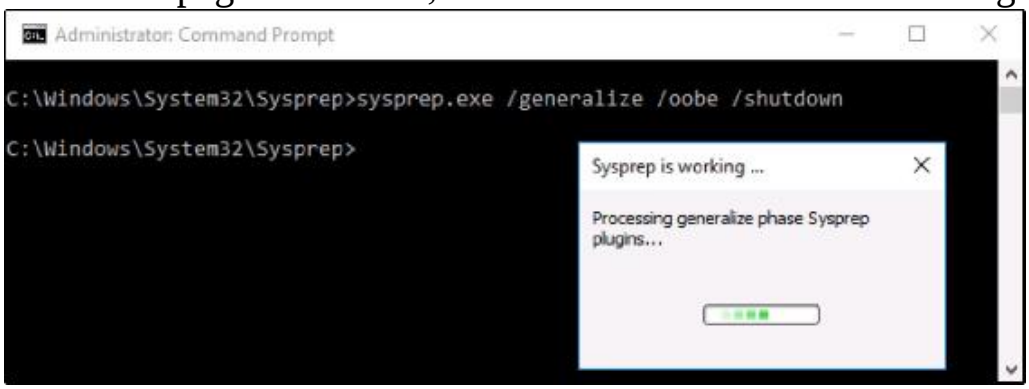
Assicurati che il tuo server NON si avvii di nuovo in Windows fino a dopo aver creato la tua immagine master o aver preso la tua copia master del file
.VHDX file. Il primola volta che Windows si avvia, inietterà le nuove informazioni SID e vuoi che ciò accada solo sui nuovi server che hai creato in base alla tua nuova immagine.

Quindi, piuttosto che semplicemente lanciarti tutti gli interruttori e lasciarti decidere, diamo un'occhiata a quelli che uso tipicamente. Farò uso di / generalize in modo da rendere unici i miei nuovi server, e mi piace anche usare / oobe in modo che la mini-configurazione guidata si avvii durante il primo avvio di Windows su uno qualsiasi dei miei nuovi sistemi. Quindi, ovviamente userò anche

/ shutdown, perch é ho bisogno che questo server sia offline immediatamente dopo Sysprep in modo da poter prendere una copia del disco rigido da utilizzare come immagine principale. Quindi, il mio comando sysprep completamente curato è mostrato nel codice seguente:

sysprep.exe / generalize / oobe / shutdown

Dopo aver avviato questo comando, vedrai Sysprep muoversi attraverso alcuni processi all'interno di Windows e, dopo un paio di minuti, il tuo server si spegnerà da solo, come mostrato nello screenshot seguente:



Ora sei pronto per creare la tua immagine master da questo disco rigido.

Creazione della tua immagine principale dell'unità

Il nostro server principale è ora spento e siamo pronti per creare la nostra immagine principale da questo server. Se si tratta di un server fisico, è possibile utilizzare qualsiasi utilità di imaging del disco rigido per creare un file immagine dall'unità. Un'utilità di imaging come quelle dell'azienda Acronis creerà un singolo file dall'unità. Questo file contiene un'immagine dell'intero disco che è possibile utilizzare per eseguire il ripristino su nuovi dischi rigidi in nuovi server in futuro. D'altra parte, la maggior parte di voi probabilmente ha a che fare con server virtuali più spesso nella vita lavorativa quotidiana e preparare nuovi server nel mondo virtuale è ancora più semplice. Una volta che il nostro server principale è stato preparato e spento, è sufficiente creare una copia del file .VHDX. Accedi al tuo server Hyper-V, copia e incolla il file del disco rigido e il gioco è fatto. Questo nuovo file può essere rinominato WS2019_Master_withUpdates.VHDX, o come vuoi che venga chiamato, per aiutarti a tenere traccia dello stato corrente su questo file immagine. Salva questo file immagine o una copia del .VHDX da qualche parte al sicuro sulla tua rete, dove sarai in grado di prenderne rapidamente copie

ogni volta che avrai la necessità di avviare un nuovo Windows Server 2019.

Creazione di nuovi server utilizzando copie dell'immagine master

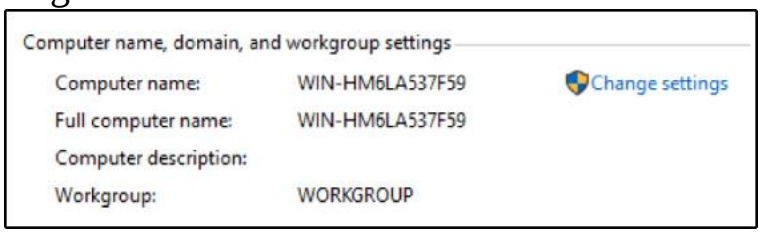
Ora arriviamo alla parte facile. Quando si desidera creare nuovi server in futuro, è sufficiente copiare e incollare il file master in una nuova posizione per il nuovo server, rinominare il file di unità in modo che sia qualcosa di appropriato per il server che si sta creando e avviare la nuova macchina virtuale da esso. Qui è dove puoi vedere il vero vantaggio del tempo risparmiato da Sysprep, poiché ora puoi avviare molti nuovi server tutti contemporaneamente, facendo una rapida copia e incolla del file dell'immagine principale e avviando tutti i tuoi nuovi server da questi nuovi file. Non è necessario installare Windows o estrarre quel DVD di installazione polveroso!

Quando i nuovi server si accendono per la prima volta e si avviano in Windows, eseguiranno l'esperienza di installazione guidata di mini-configurazione. Inoltre, in background, il sistema operativo si fornisce un nuovo nome host casuale e univoco e informazioni SID in modo che tu possa essere sicuro di non avere conflitti sulla tua rete con questi nuovi server.

I nuovi server creati da un file immagine sysprepped ricevono sempre un nuovo nome host all'avvio. Questo spesso confonde gli amministratori che potrebbero aver chiamato il loro server principale qualcosa comeMAESTRO. Dopo aver avviato i tuoi nuovi server, puoi aspettarti di vedere nomi casuali sui tuoi nuovi server e dovrai rinominarli in base ai loro nuovi compiti nella vita.

Ad esempio, prima di eseguire Sysprep e creare la mia immagine master, il server su cui stavo lavorando si chiamava DC1 perché inizialmente avevo intenzione di usarlo come controller di dominio nella mia rete. Tuttavia, poiché non avevo installato il ruolo o configurato nulla relativo al dominio su di esso, questo server era un candidato perfetto per visualizzare il processo Sysprep e quindi l'ho usato nel nostro testo oggi. L'ho preparato con il sysprema, l'ho spento, ho fatto una copia del suo file VHDX (per essere il mio file di immagine principale), quindi ho avviato il backup di DC1. Ora puoi vedere all'interno delle proprietà di sistema che sono tornato ad avere un nome host randomizzato, quindi se voglio ancora usare questo server come DC1, dovrò rinominarlo di nuovo ora che ha

terminato l'avvio tramite mini-configurazione, come mostrato nella seguente schermata:



Si spera che questo processo sia un'informazione utile che può farti risparmiare tempo durante la creazione di nuovi server nei tuoi ambienti. Esci e provalo la prossima volta che hai un nuovo server da costruire! Puoi trarre ulteriore vantaggio dallo strumento Sysprep conservando molti file di immagine principale diversi. Forse hai una manciata di diversi tipi di server che prepari regolarmente, non c'è nulla che ti impedisca di creare un numero di server principali diversi e di creare più immagini principali da questi server.

Sommario

Chiunque sia interessato a essere un amministratore di Windows Server deve essere a proprio agio con l'installazione e la gestione dei propri server e la copertura di questi argomenti costituisce un'importante linea di base per andare avanti. È abbastanza comune nel mondo IT di oggi che le nuove versioni del sistema operativo vengano testate a fondo, sia perché le risorse hardware del server sono così facilmente disponibili attraverso le tecnologie di virtualizzazione, sia perché la maggior parte dei sistemi aziendali è ora progettata per il 100% di uptime. Questo tipo di affidabilità richiede test molto approfonditi di qualsiasi modifica alla piattaforma e, per eseguire tale test del sistema operativo Windows Server 2019 nel tuo ambiente, dovrai sprecare un bel po 'di tempo girando numerose volte attraverso i processi di installazione di base.

Anni fa, veniva regolarmente profuso un po 'di impegno per capire quali ruoli e servizi potessero coesistere, perché il numero di server a nostra disposizione era limitato. Con la nuova virtualizzazione e il cambio di paradigma del cloud, molte aziende hanno un numero virtualmente illimitato di server che possono essere eseguiti, e questo significa che stiamo eseguendo quantità molto maggiori di server per eseguire gli stessi lavori e funzioni. La gestione e l'amministrazione di questi server diventano quindi un fardello per l'IT e l'adozione degli strumenti e delle idee di amministrazione centralizzata disponibili in Windows Server 2019 ti farà risparmiare molto tempo e fatica nel tuo carico di lavoro quotidiano. Nel prossimo capitolo esamineremo i servizi di infrastruttura di base.

Domande

1. Qual è il nome del nuovo strumento di gestione dei server centralizzato basato sul Web di Microsoft (precedentemente noto come Project Honolulu)?
2. Vero o falso: Windows Server 2019 deve essere installato sull'hardware del server con montaggio su rack.
3. Vero o falso: scegliendo l'opzione di installazione predefinita per Windows Server 2019, ti ritroverai con un'interfaccia utente simile a Windows 10.
4. Che cos'è il cmdlet di PowerShell che visualizza i ruoli e le funzionalità attualmente installati in Windows Server 2019?
5. Vero o falso: è possibile utilizzare Server Manager per gestire più server diversi contemporaneamente?
6. Qual è il nome del set di strumenti che può essere installato su un computer Windows 10, per eseguire Server Manager su quella workstation client?
7. Quali sono i browser Web supportati che possono essere utilizzati per interagire con Windows Admin Center?

Servizi di infrastruttura di base

Ognuno di voi che leggerà questo libro avrà un set di competenze acquisito e un livello di esperienza diversi con l'ambiente Windows Server. Come ho accennato in precedenza, essere in grado di far eseguire ai server il sistema operativo è fantastico e un primo passo molto importante per fare un lavoro reale nel tuo ambiente. Ma finché non si conosce e si comprende quali sono gli scopi dietro i ruoli principali disponibili per l'esecuzione su Windows Server 2019, l'unica cosa che fa il nuovo server è consumare elettricità.

Un server è destinato a fornire dati. I tipi di dati che servono e lo scopo dipendono interamente dai ruoli che determini che il server deve ... beh ... servire.
In modo appropriato, è necessario installare i ruoli all'interno di Windows Server 2019 per fargli fare qualcosa. Sappiamo già come installare i ruoli sul nostro server, ma non abbiamo parlato di nessuno degli scopi alla base di questi ruoli. In questo capitolo, daremo uno sguardo ai ruoli

infrastrutturali principali disponibili in Windows Server. Ciò implica la discussione dello scopo generale del ruolo, nonché l'inserimento di alcune attività particolari che si occupano di quei ruoli che sarai responsabile di svolgere nelle tue attività quotidiane come amministratore del server. In questo capitolo impareremo quanto segue:

- Cos'è un controller di dominio?
- Utilizzo di Servizi di dominio Active Directory per organizzare la rete La potenza dei Criteri di gruppo
- **Domain Name System** (DNS) DHCP contro indirizzamento statico Backup e ripristino
- Scorciatoie MMC e MSC

Cos'è un controller di dominio?

Se abbiamo intenzione di discutere i servizi di infrastruttura di base di cui hai bisogno per mettere insieme la tua rete guidata da Microsoft, non c'è posto migliore per iniziare del ruolo di controller di dominio. Un controller di dominio, comunemente indicato come DC, è il punto di contatto centrale ed è una sorta di hub centrale, a cui si accede prima di quasi tutte le comunicazioni di rete che avvengono. Il modo più semplice per descriverlo è come un contenitore di archiviazione per tutte le identificazioni che avvengono sulla rete. I nomi utente, le password, gli account computer, i gruppi di computer, i server, i gruppi e le raccolte di server, i criteri di sicurezza, i servizi di replica file e molte altre cose sono archiviati e gestiti dai controller di dominio. Se non hai intenzione di avere un controller di dominio come uno dei primi server nella tua rete incentrata su Microsoft, potresti anche non iniziare a costruire quella rete. I controller di dominio sono essenziali per il modo in cui i nostri computer e dispositivi comunicano tra loro e con l'infrastruttura dei server all'interno delle nostre aziende.

Servizi di dominio Active Directory

Se hai smesso di leggere a questo punto per installare il ruolo di controller di dominio sul tuo server, bentornato perché non esiste un ruolo chiamato controller di dominio. Il ruolo che fornisce tutte queste funzionalità è denominato Servizi di dominio Active Directory o Servizi di dominio Active Directory. Questo è il ruolo che devi installare su un server. Installando quel ruolo, avrai trasformato il tuo server in un controller di dominio. Lo scopo dell'esecuzione di un controller di dominio è davvero quello di creare una directory, o database, di oggetti nella rete. Questo database è noto come Active Directory ed è una piattaforma all'interno della quale si crea una struttura gerarchica per archiviare oggetti, come nomi utente, password e account computer.

Dopo aver creato un dominio in cui è possibile memorizzare questi account e dispositivi, è quindi possibile creare account utente e password

che i dipendenti utilizzeranno per l'autenticazione. È quindi possibile unire anche gli altri server e computer a questo dominio in modo che possano accettare e beneficiare di tali credenziali utente. Avere e partecipare a un dominio è la salsa segreta che ti consente di passare da un computer all'altro all'interno della tua azienda e accedere a ciascuno di essi con il tuo nome utente e password, anche se non hai mai effettuato l'accesso a quel computer prima. Ancora più potente è il fatto che consente alle applicazioni con capacità di directory di autenticarsi direttamente in Active Directory quando necessitano di informazioni di autenticazione. Ad esempio, quando, come utente di dominio, accedo al mio computer al lavoro con il mio nome utente e la mia password,

Una volta che conferma che sono veramente quello che dico di essere, restituisce un token di autenticazione al mio computer e sono in grado di accedere. Quindi, una volta che sono sul desktop e apro un'applicazione, diciamo che apro il mio Outlook per accedere alla mia posta elettronica: quel programma di posta elettronica è progettato per raggiungere il mio server di posta, chiamato Exchange Server, e autenticarsi per assicurarsi che venga visualizzata la mia casella di posta e non quella di qualcun altro. Ciò significa che devo reinserire il mio nome utente e la password per Outlook o per qualsiasi altra applicazione che apro dal mio computer? Di solito no. E il motivo per cui non devo reinserire le mie credenziali più e più volte è perché il mio nome utente, il mio computer e i server delle applicazioni fanno tutti parte del dominio. Quando questo è vero, ed è per la maggior parte delle reti, il mio token di autenticazione può essere condiviso tra i miei programmi. Così, una volta effettuato l'accesso al computer stesso, le mie applicazioni possono essere avviate e aperte e passare le mie credenziali al server delle applicazioni, senza ulteriori input da parte mia come utente. Sarebbe davvero un'esperienza frustrante se richiedessimo ai nostri utenti di inserire le password tutto il giorno, ogni giorno mentre aprono i programmi di cui hanno bisogno per svolgere il loro lavoro.

Il primo controller di dominio che configurerai nella tua rete sarà completamente scrivibile, in grado di accettare i dati dagli utenti del dominio e dai computer che lavorano all'interno della tua rete. In effetti, la maggior parte dei controller di dominio nella rete sarà probabilmente completamente funzionante. Tuttavia, vale la pena dedicare un minuto per sottolineare un controller di dominio di ambito limitato che può essere installato chiamato controller di dominio di sola lettura (RODC). Proprio come suggerisce il nome, un RODC può solo leggere i dati della directory da esso. Le scritture che potrebbero tentare di essere eseguite nel dominio dal computer di un utente, ad esempio una modifica della password o la creazione di un nuovo account utente, sono impossibili con un RODC. Al contrario, i controller di dominio di sola lettura ricevono i dati della directory da altri controller di dominio più tradizionali e quindi utilizzano

tali dati per verificare le richieste di autenticazione da parte di utenti e computer.
Molte aziende li stanno installando in filiali più piccole o siti meno sicuri, in modo che i computer locali in loco in quegli uffici più piccoli abbiano un accesso facile e veloce per leggere e autenticarsi nel dominio, senza il potenziale rischio per la sicurezza che un utente non autorizzato possa accedere a il server fisico e la manipolazione dell'intero dominio in modi negativi.

Lo stesso Active Directory è un argomento abbastanza ampio da giustificare il proprio libro, e in effetti ne sono stati scritti molti sull'argomento. Ora che abbiamo una conoscenza di base di che cos'è e perché è fondamentale averlo nel nostro ambiente Windows Server, sporciamoci le mani usando alcuni degli strumenti che vengono installati nel controller di dominio durante il processo di installazione del ruolo di Servizi di dominio Active Directory.

Utilizzo di Servizi di dominio Active Directory per organizzare la rete

Non esiste un unico strumento utilizzato per gestire tutti gli aspetti di Active Directory. Poiché si tratta di una tecnologia così ampia, la nostra configurazione della directory è distribuita su una serie di diverse console di gestione. Diamo un'occhiata a ciascuno di essi e ad un paio delle attività più comuni che eseguirai all'interno di questi strumenti. Ognuna di queste console di gestione può essere avviata da qualsiasi server del controller di dominio e, proprio come abbiamo visto in un capitolo precedente, il modo più semplice per avviare queste console è direttamente dal menu Strumenti nell'angolo in alto a destra di Server Manager.

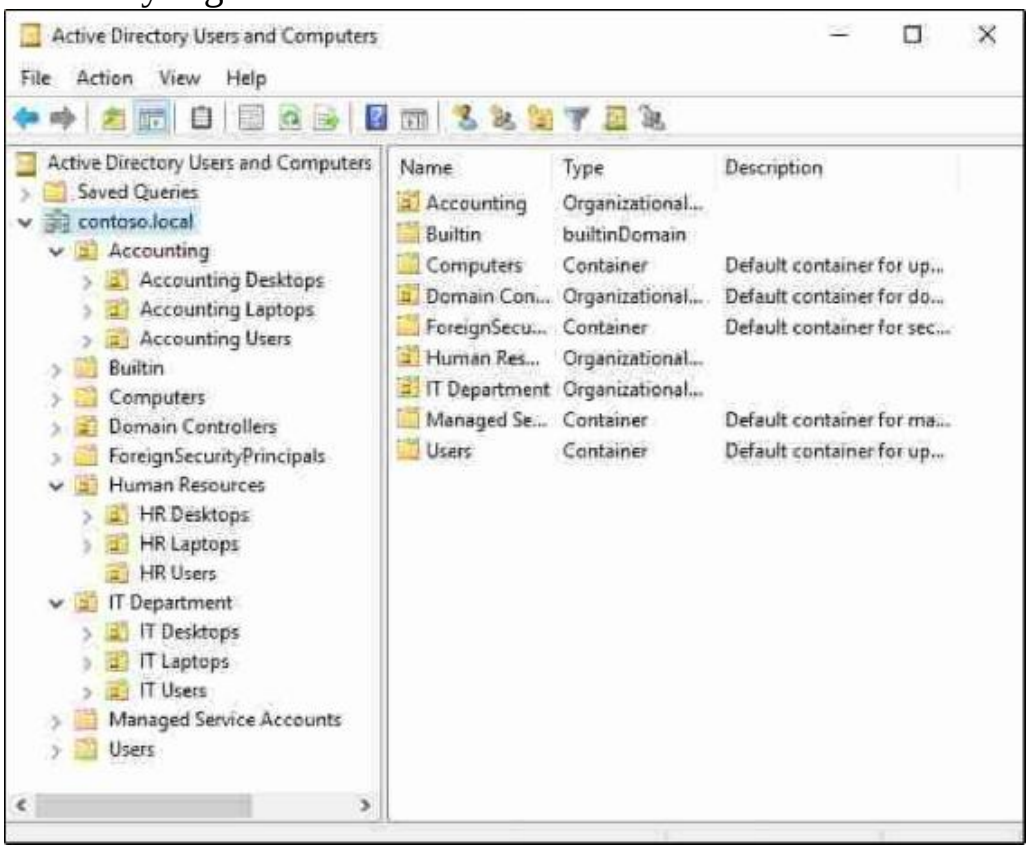
Utenti e computer di Active Directory

Inizierò con lo strumento che è l'ultimo in ordine alfabetico nell'elenco dei nostri strumenti di Active Directory, perché questo è di gran lunga quello che l'amministratore del server quotidiano utilizzerà più spesso. Utenti e computer di AD è la console da cui vengono creati e gestiti tutti gli account utente e gli account computer. Aprilo e vedrai il nome del tuo dominio elencato nella colonna di sinistra. Espandi il tuo nome di dominio e vedrai un numero di cartelle elencate qui. Se lo stai aprendo su un controller di dominio esistente in una rete ben sviluppata, potresti avere pagine e pagine di cartelle elencate qui. Se questo è un nuovo ambiente, ce ne sono solo una manciata. I pezzi più importanti da sottolineare qui sono i computer e gli utenti. Come vorrebbe il buon senso dettare,

Sebbene questa finestra assomigli un po 'a Esplora file con un albero di cartelle,
queste cartelle in realtà non sono affatto cartelle. La maggior parte delle icone delle cartelle color manila che vedi qui sono note come unità organizzative (OU). Dico la maggior parte perché ci sono alcuni

contenitori che esistono fuori dagli schemi che sono contenitori di archiviazione legittimi per contenere oggetti, ma non sono unità organizzative ufficiali. Quelli che abbiamo sottolineato in precedenza, Utenti e Computer, sono in realtà questi contenitori di archiviazione generici e non sono vere e proprie Unità organizzative. Tuttavia, tutte le nuove cartelle che crei per te stesso all'interno di AD saranno unità organizzative. La differenza è rappresentata nell'icona della cartella manila. Puoi vedere negli screenshot in arrivo che alcune delle cartelle di Manila hanno una piccola grafica in più sopra la cartella stessa. Solo le cartelle che hanno la piccola cosa gialla in più sono unità organizzative reali.

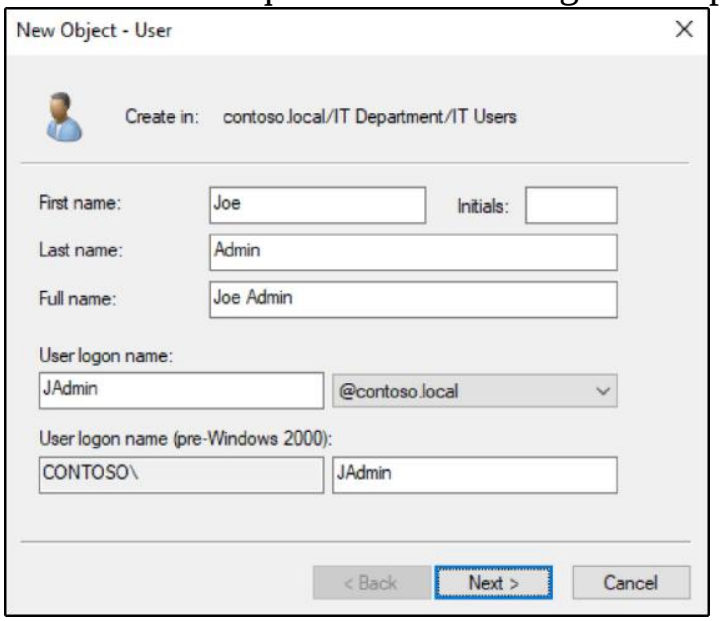
Le unità organizzative sono i contenitori strutturali che utilizziamo all'interno di Active Directory per organizzare i nostri oggetti e conservarli tutti in luoghi utili. Proprio come con le cartelle su un file server, qui puoi creare la tua gerarchia di unità organizzative, al fine di ordinare e manipolare la posizione all'interno di Active Directory di tutti i dispositivi e oggetti di rete aggiunti al dominio. Nello screenshot seguente, puoi vedere che invece di avere solo una semplice cartella Users and Computers, ho creato alcune nuove unità organizzative incluse le sottocategorie (più ufficialmente note come unità organizzative annidate) in modo che man mano che accrescerò il mio ambiente, avrò un e directory organizzata:



Profili utente

Ora che abbiamo alcune unità organizzative pronte per contenere i nostri oggetti, creiamo un nuovo utente. Supponiamo di avere un nuovo amministratore del server in arrivo e dobbiamo procurargli un accesso ad Active Directory in modo che possa iniziare il suo lavoro. Trova semplicemente l'unità organizzativa appropriata in cui risiedere il suo account, fai clic con il pulsante destro del mouse sull'unità organizzativa e vai a Nuovo | Utente. Ci viene quindi presentata una schermata di raccolta delle informazioni su tutte le cose di cui AD ha bisogno per creare questo nuovo account. La maggior parte delle informazioni qui sono autoesplicative, ma se sei nuovo in Active Directory, l'unico campo che indicherò è il nome di accesso dell'utente. Qualunque informazione venga inserita in questo campo è il nome utente ufficiale dell'utente sulla rete. Ogni volta che accedono a un computer o server, questo è il nome che inseriranno come login.

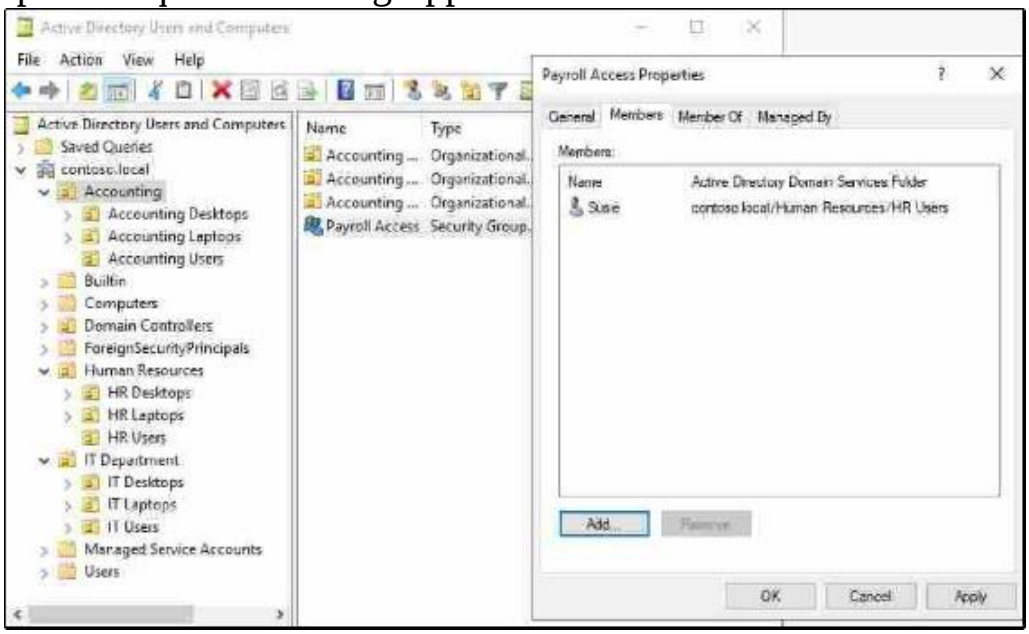
Al termine, il nostro nuovo amministratore sarà in grado di utilizzare il nuovo nome utente e password per accedere a computer e server in rete, ovviamente entro i limiti di sicurezza che abbiamo stabilito su quelle macchine. Ma questo è un altro argomento per un altro capitolo.



Gruppi di sicurezza

Un'altra utile unità di organizzazione all'interno di Active Directory è i gruppi di sicurezza. Possiamo fare un bel po 'per distinguere tra diversi tipi e tipi di utenti e account di computer utilizzando le unità organizzative, ma cosa succede quando abbiamo bisogno di una piccola contaminazione incrociata in questa struttura? Forse abbiamo un dipendente che gestisce alcune risorse umane e alcune responsabilità contabili. Forse è più probabile che abbiamo configurato le autorizzazioni per file e cartelle sui nostri file server in modo che solo le persone che fanno parte di determinati gruppi abbiano accesso per leggere e scrivere in determinate cartelle. Susie delle Risorse umane deve avere accesso alla cartella dei salari, ma Jim delle Risorse umane no. Sia Susie che Jim risiedono nella stessa unità organizzativa, quindi a quel livello avranno le stesse autorizzazioni e capacità, ma abbiamo chiaramente bisogno di un modo diverso per distinguerli in modo che solo Susie possa accedere alle informazioni sui salari. Creando gruppi di sicurezza all'interno di Active Directory, consentiamo agli utenti di aggiungere e rimuovere account utente, account computer o anche altri gruppi specifici in modo da poter definire in modo granulare l'accesso alle nostre risorse. Si creano nuovi gruppi nello stesso modo in cui si creano gli account utente, scegliendo l'unità organizzativa in cui si desidera risiedere il nuovo gruppo, quindi fare clic con il pulsante destro del mouse su tale unità organizzativa e passare a Nuovo | Gruppo. Una volta che il tuo gruppo è stato creato, fai clic destro su di esso e vai in Proprietà. È quindi possibile fare clic sulla scheda Membri; qui è dove aggiungi tutti gli utenti che vuoi far parte di questo nuovo gruppo: consentiamo agli utenti di aggiungere e rimuovere account utente specifici, account computer o anche altri gruppi in modo da poter definire in modo granulare l'accesso alle nostre risorse. Si creano nuovi gruppi nello stesso modo in cui si creano gli account utente, scegliendo l'unità organizzativa in cui si desidera risiedere il nuovo gruppo, quindi fare clic con il pulsante destro del mouse su tale unità organizzativa e passare a Nuovo | Gruppo. Una volta che il tuo gruppo è stato creato, fai clic destro su di esso e vai in Proprietà. È quindi possibile fare clic sulla scheda Membri; qui è dove aggiungi tutti gli utenti che vuoi

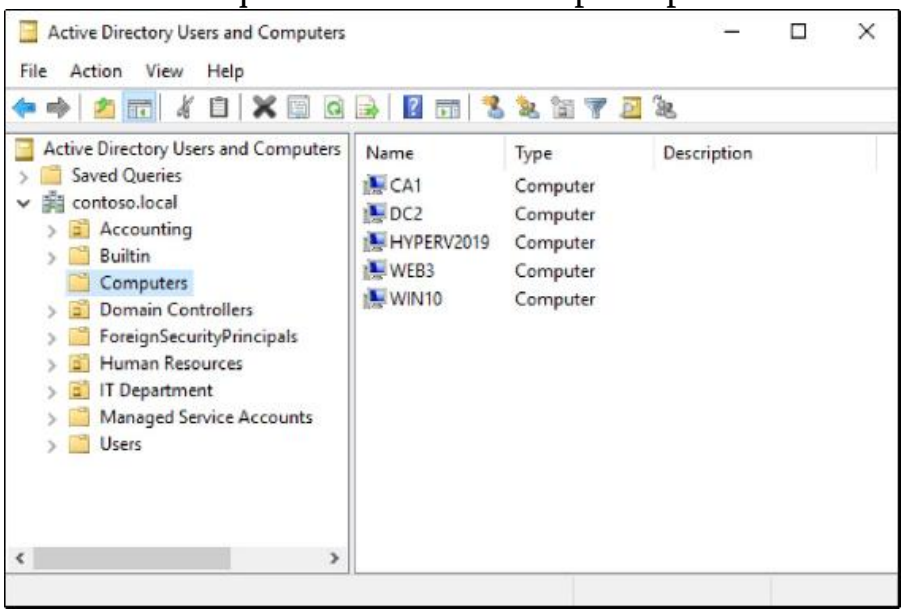
far parte di questo nuovo gruppo: consentiamo agli utenti di aggiungere e rimuovere account utente specifici, account computer o anche altri gruppi in modo da poter definire in modo granulare l'accesso alle nostre risorse. Si creano nuovi gruppi nello stesso modo in cui si creano gli account utente, scegliendo l'unità organizzativa in cui si desidera risiedere il nuovo gruppo, quindi fare clic con il pulsante destro del mouse su tale unità organizzativa e passare a Nuovo | Gruppo. Una volta che il tuo gruppo è stato creato, fai clic destro su di esso e vai in Proprietà. È quindi possibile fare clic sulla scheda Membri; qui è dove aggiungi tutti gli utenti che vuoi far parte di questo nuovo gruppo: Una volta che il tuo gruppo è stato creato, fai clic destro su di esso e vai in Proprietà. È quindi possibile fare clic sulla scheda Membri; qui è dove aggiungi tutti gli utenti che vuoi far parte di questo nuovo gruppo: Una volta che il tuo gruppo è stato creato, fai clic destro su di esso e vai in Proprietà. È quindi possibile fare clic sulla scheda Membri; qui è dove aggiungi tutti gli utenti che vuoi far parte di questo nuovo gruppo:



Prestaging degli account computer

È molto comune utilizzare Utenti e computer di Active Directory per creare nuovi account utente, perché senza la creazione manuale di un account utente quella nuova persona non sarà completamente in grado di accedere alla rete. È molto meno comune, tuttavia, pensare di aprire questo strumento quando si aggiungono nuovi computer al proprio dominio. Questo perché la maggior parte dei domini è configurata in modo che i nuovi computer possano entrare a far parte del dominio tramite azioni eseguite sul computer stesso, senza che sia stato eseguito alcun lavoro all'interno di Active Directory. In altre parole, se qualcuno conosce un nome utente e una password con diritti amministrativi all'interno del dominio, può sedersi a qualsiasi computer connesso alla rete e seguire il processo di aggiunta al dominio su quel computer locale. Si unirà con successo al dominio, e Active Directory creerà automaticamente un nuovo oggetto computer. Questi oggetti computer a generazione automatica si posizionano all'interno del contenitore Computer predefinito, quindi in molte reti, se fai clic su quella cartella Computer, vedrai un numero di macchine diverse elencate e potrebbero anche essere un mix di computer desktop e server che sono stati aggiunti di recente al dominio e non sono stati ancora spostati in un'unità organizzativa appropriata e più specifica. Nel mio ambiente di laboratorio in crescita, ho recentemente aggiunto un certo numero di macchine al dominio. L'ho fatto senza mai aprire Utenti e computer di AD e puoi vedere che i miei nuovi oggetti computer sono ancora all'interno di quel contenitore Computer predefinito: quindi in molte reti, se fai clic su quella cartella Computer, vedrai un numero di macchine diverse elencate e potrebbero anche essere un misto di computer desktop e server che sono stati aggiunti di recente al dominio e non sono stati spostati in ancora un'unità organizzativa appropriata e più specifica. Nel mio ambiente di laboratorio in crescita, ho recentemente aggiunto un certo numero di macchine al dominio. L'ho fatto senza mai aprire Utenti e computer di AD e puoi vedere che i miei nuovi oggetti computer sono ancora all'interno di quel contenitore Computer predefinito: quindi in molte reti, se fai clic su quella cartella Computer, vedrai un numero di macchine

diverse elencate e potrebbero anche essere un misto di computer desktop e server che sono stati aggiunti di recente al dominio e non sono stati spostati in ancora un'unità organizzativa appropriata e più specifica. Nel mio ambiente di laboratorio in crescita, ho recentemente aggiunto un certo numero di macchine al dominio. L'ho fatto senza mai aprire Utenti e computer di AD e puoi vedere che i miei nuovi oggetti computer sono ancora all'interno di quel contenitore Computer predefinito: Recentemente ho aggiunto un certo numero di macchine al dominio. L'ho fatto senza mai aprire Utenti e computer di AD e puoi vedere che i miei nuovi oggetti computer sono ancora all'interno di quel contenitore Computer predefinito: Recentemente ho aggiunto un certo numero di macchine al dominio. L'ho fatto senza mai aprire Utenti e computer di AD e puoi vedere che i miei nuovi oggetti computer sono ancora all'interno di quel contenitore Computer predefinito:



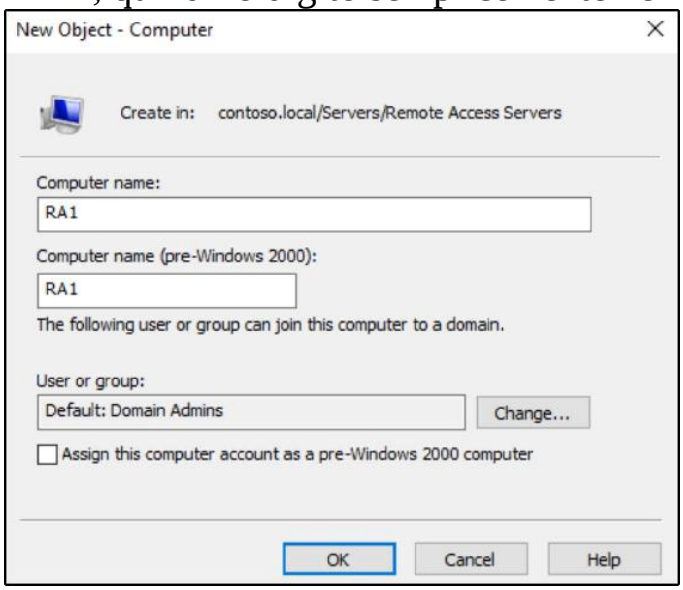
Consentire a nuovi account computer di posizionarsi all'interno del contenitore Computer predefinito in genere non è un grosso problema per i sistemi client, ma se si consente ai server di essere generati automaticamente in quella cartella, si possono causare grossi problemi. Molte aziende dispongono di criteri di sicurezza in tutta la rete e questi criteri vengono spesso creati in modo da essere applicati automaticamente a qualsiasi account di computer residente in una delle unità organizzative generalizzate. L'utilizzo dei criteri di sicurezza può essere un ottimo modo per bloccare parti delle macchine client a cui l'utente non deve accedere o utilizzare, ma se inavvertitamente le causi **confinamento** criteri da applicare ai tuoi nuovi server non appena entrano a far parte del dominio, puoi effettivamente interrompere il server prima ancora di iniziare a configurarlo. Credimi, l'ho fatto. E, sfortunatamente, i tuoi nuovi account server che vengono aggiunti ad Active Directory verranno identificati e classificati come qualsiasi workstation client aggiunta al dominio, quindi non puoi specificare un contenitore predefinito diverso per i server semplicemente perché sono un server e non una normale postazione di lavoro.

Allora, cosa si può fare per alleviare questo potenziale problema? La risposta è preinstallare gli account di dominio per i nuovi server. In linea di principio è anche possibile preinstallare tutti i nuovi account computer, ma in genere vedo questo requisito solo nelle grandi aziende. La pre-configurazione di un account computer è molto simile alla creazione di un nuovo account utente. Prima di unire il computer al dominio, creare l'oggetto per esso all'interno di Active Directory. Eseguendo la creazione dell'oggetto prima del processo di aggiunta al dominio, puoi scegliere in quale unità organizzativa risiederà il computer quando entrerà a far parte del dominio. È quindi possibile assicurarsi che si tratti di un'unità organizzativa che riceverà o meno le impostazioni e i criteri di protezione che si intende applicare su questo nuovo computer o server. Consiglio vivamente di predisporre tutti gli account computer in Active Directory per qualsiasi nuovo server che porti in linea. Se lo fai una pratica, anche se non è assolutamente necessario tutto il tempo, creerai una buona abitudine che un giorno potrebbe salvarti dal dover

ricostruire un server che hai rotto semplicemente unendolo al tuo dominio.

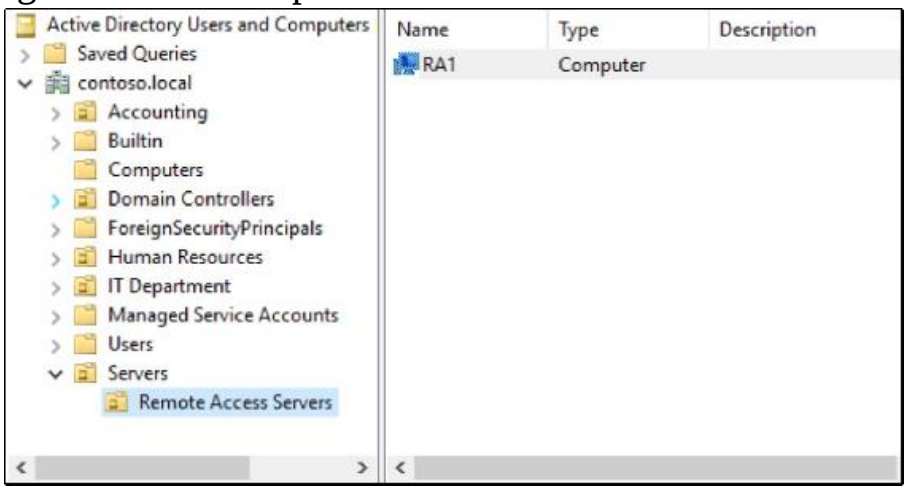
Il prestaging di un oggetto computer è estremamente veloce e semplice; facciamone uno insieme. In futuro, ho intenzione di creare un server Windows che ospita il ruolo di accesso remoto per connettere i miei utenti in roaming alla rete dalle loro case, dai bar e così via. Alcuni componenti nel ruolo di accesso remoto sono pignoli quando si tratta di criteri di sicurezza della rete, quindi preferirei assicurarmi che il mio nuovo server RA1 non riceva un intero gruppo di impostazioni di blocco non appena lo aggiungo al dominio. Ho creato un'unità organizzativa chiamata server di accesso remoto e ora pre-installerò un oggetto computer all'interno di tale unità organizzativa per il mio server RA1.

Fare clic con il pulsante destro del mouse sull'unità organizzativa dei server di accesso remoto e scegliere Nuovo | Computer. Quindi compila semplicemente il campo Nome computer con il nome del tuo server. Anche se non ho ancora creato questo server, ho intenzione di chiamarlo RA1, quindi lo digito semplicemente nel campo:



Questo è tutto! Con un paio di semplici clic del mouse e digitando il nome di un server, ora ho preinstallato (pre-creato) il mio oggetto computer per il server RA1. Se osservi attentamente lo screenshot precedente, noterai che potresti anche regolare quali utenti o gruppi sono autorizzati ad unire questo particolare computer al dominio. Se prevedi di creare un nuovo server e vuoi assicurarti di essere l'unica persona autorizzata ad aggiungerlo al dominio, questo campo può essere facilmente aggiornato per soddisfare tale requisito.

Una volta che riesco effettivamente a costruire quel server e vado avanti e passo attraverso i passaggi per aggiungerlo al mio dominio, Active Directory assocerà il mio nuovo server a questo oggetto RA1 preinstallato invece di creare un oggetto nuovo di zecca all'interno del contenitore generico dei computer :



Domini e trust di Active Directory

Questo strumento viene generalmente utilizzato solo in ambienti più grandi che hanno più di un dominio all'interno della stessa rete. Una società può utilizzare più nomi di dominio per separare risorse o servizi o per una migliore struttura organizzativa dei propri server e spazi dei nomi all'interno dell'azienda. C'è anche un altro livello nella struttura gerarchica di Active Directory di cui non abbiamo parlato e che è chiamato foresta. La foresta è fondamentalmente il livello più alto della struttura di Active Directory, con domini e sottodomini che rientrano sotto l'ombrello della foresta. Un altro modo di pensare alla foresta è come il confine della tua struttura AD. Se si dispone di più domini sotto una singola foresta, non significa necessariamente che tali domini si fidino l'uno dell'altro. Così, gli utenti di un dominio possono avere o meno le autorizzazioni per accedere alle risorse su uno degli altri domini, in base al livello di fiducia che esiste tra quei domini. Quando si dispone di un dominio e si aggiungono domini figlio sotto di esso, ci sono trust posizionati automaticamente tra quei domini, ma se è necessario unire alcuni domini

insieme in un modo diverso dalle autorizzazioni predefinite, Active Directory Domains and Trusts è lo strumento di gestione che si utilizzare per stabilire e modificare tali autorizzazioni di fiducia.

Le organizzazioni in crescita si trovano spesso nella posizione di dover gestire regolarmente i trust di dominio a seguito di acquisizioni aziendali. Se Contoso acquisisce Fabrikam ed entrambe le società hanno ambienti di dominio completamente funzionali, è spesso vantaggioso lavorare attraverso un processo di migrazione esteso per portare i dipendenti di Fabrikam ad Active Directory di Contoso, piuttosto che subire tutte le perdite associate alla semplice disattivazione della rete di Fabrikam . Quindi, per un certo periodo di tempo, vorresti eseguire entrambi i domini contemporaneamente e potresti stabilire una relazione di fiducia tra quei domini per renderlo possibile.

Se ti trovi in una posizione in cui è necessaria una migrazione del dominio di qualsiasi tipo, è disponibile uno strumento che potresti voler provare. Si chiama Active Directory Migration Tool (ADMT) e può essere molto utile in situazioni come quella descritta in precedenza. Se sei interessato a dare un'occhiata più da vicino a questo strumento, puoi scaricarlo dal seguente collegamento: https: //www.microsoft.com /en-noi/Scarica/dettagli.aspx?id =19188.

Siti e servizi di Active Directory

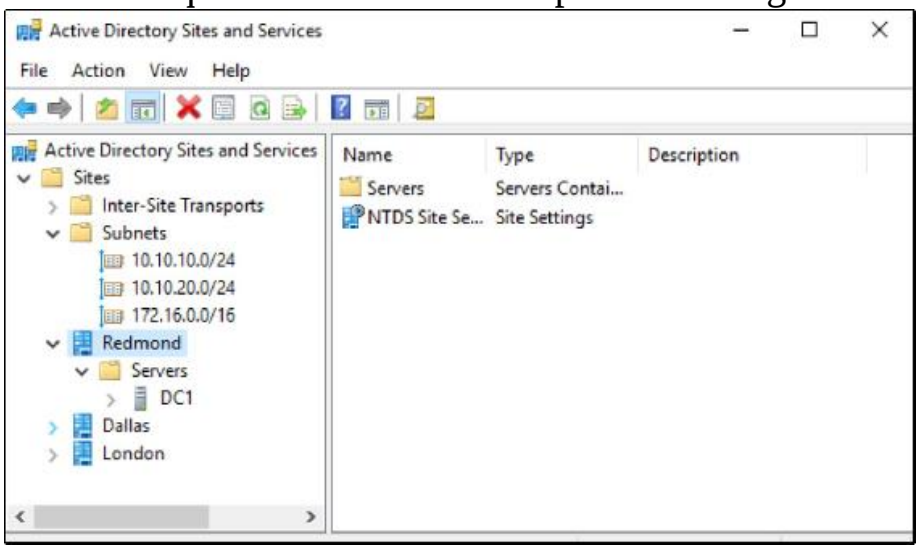
Sites and Services è un altro strumento generalmente utilizzato solo da aziende con infrastrutture Active Directory più grandi. Come nel caso di qualsiasi server, se avere un controller di dominio va bene, avere due controller di dominio è ancora meglio. Man mano che la tua azienda cresce, cresce anche la tua infrastruttura di Active Directory. Prima che tu te ne accorga, cercherai di configurare i server in una seconda posizione, poi in una terza e così via. In una rete incentrata sul dominio, avere server controller di dominio in ogni sito significativo è una pratica generale e presto potresti trovare dozzine di server controller di dominio in esecuzione nella tua rete.

Attivare nuovi controller di dominio e unirli al tuo dominio esistente in modo che inizino a servire utenti e computer è piuttosto semplice. La parte più difficile è mantenere tutto il traffico organizzato e scorrere dove vuoi. Se disponi di un centro dati principale in cui si trova la maggior parte dei tuoi server, probabilmente hai più controller di dominio in loco

in quel centro dati. In effetti, per rendere il tuo AD altamente disponibile, è essenziale che tu abbia almeno due controller di dominio. Ma facciamo finta che tu costruisca un nuovo ufficio che è abbastanza grande, dove ha senso installare anche un server DC locale in quell'ufficio, in modo che i computer in quell'ufficio non raggiungano la Wide Area Network (WAN) in ordine per autenticarsi sempre. Se dovessi avviare un server nel nuovo ufficio e trasformarlo in un controller di dominio per la tua rete, inizierebbe immediatamente a funzionare. Il problema è che i computer client non sono sempre abbastanza intelligenti da sapere con quale controller di dominio hanno bisogno di parlare. È ora possibile che i computer dell'ufficio remoto siano ancora in fase di autenticazione nei controller di dominio del datacenter principale. Ancora peggio, probabilmente hai anche computer nell'ufficio principale che ora stanno raggiungendo la WAN per autenticarsi con il nuovo controller di dominio che si trova nell'ufficio remoto, anche se ci sono controller di dominio proprio sulla rete locale con loro!

Questa è la situazione in cui i siti ei servizi di Active Directory diventano essenziali. Qui, costruisci i tuoi diversi siti fisici e assegni i controller di dominio a questi siti. Gli utenti e i computer aggiunti a un dominio all'interno di questa rete ora seguono le regole che hai messo in atto tramite Siti e servizi, in modo che possano sempre parlare e autenticarsi dai loro server controller di dominio locali. Ciò consente di risparmiare tempo, poiché le connessioni sono più veloci ed efficienti e consente inoltre di risparmiare larghezza di banda non necessaria e consumo di dati sulla WAN, che spesso consente di risparmiare denaro.

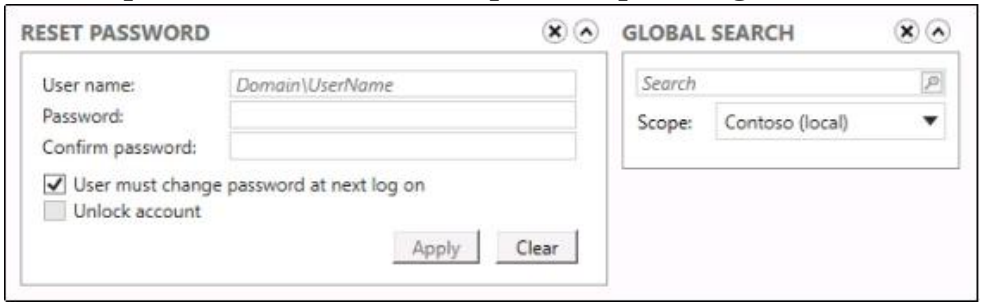
Ecco una rapida occhiata a Siti e servizi di Active Directory. Come puoi vedere, ci sono più siti elencati qui e corrispondono alle informazioni sulla subnet di rete. Questo è il modo in cui AD Sites and Services tiene traccia di quale sito è quale. Quando un computer client è online, ovviamente sa di quale sottorete fa parte, in base all'indirizzo IP che sta utilizzando. I siti e i servizi di AD quindi sanno, in base a quell'indirizzo IP, in quale sito risiede il client. L'identificazione del sito aiuta quindi Active Directory a indirizzare le richieste di autenticazione ai controller di dominio appropriati e aiuta anche cose come Criteri di gruppo (di cui parleremo circa a breve) per essere in grado di elaborare informazioni specifiche del sito. C'è una buona possibilità che un giorno dovrai utilizzare questo strumento se fai parte di un'organizzazione in crescita:



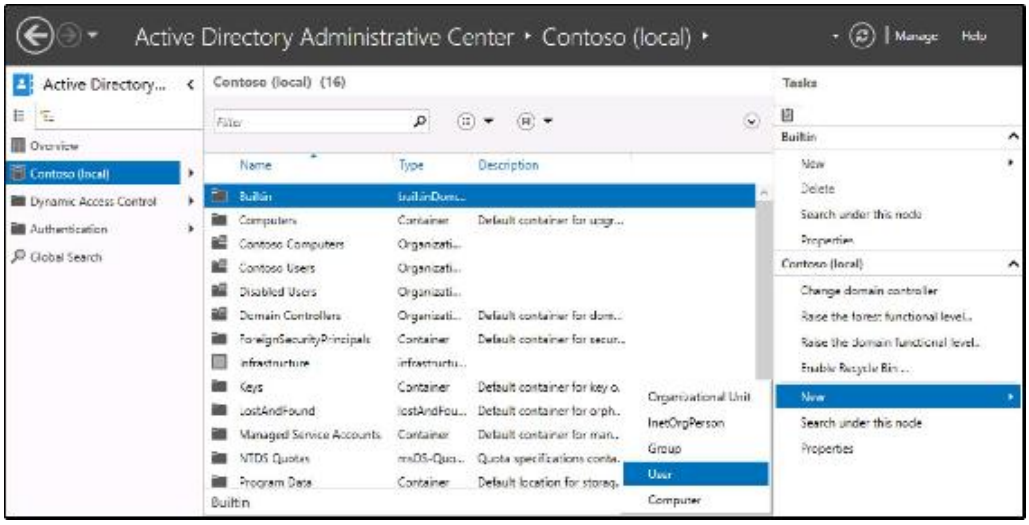
Centro di amministrazione di Active Directory

Sebbene sia fondamentale comprendere e avere familiarità con gli strumenti che abbiamo esaminato finora per gestire Active Directory, puoi dire che la loro estetica è un po 'datata. Il Centro di amministrazione di Active Directory (ADAC), d'altra parte, ha un'interfaccia molto più snella che sembra e si sente come il nuovo Server Manager con cui stiamo diventando sempre più a nostro agio. Molte delle funzioni disponibili all'interno dell'ADAC svolgono le stesse cose che possiamo fare già con gli altri strumenti, ma inserisce queste funzioni in un'interfaccia più strutturata che porta in superficie alcune delle funzioni più comunemente utilizzate e le rende più facili da correre.

Un ottimo esempio è proprio sulla pagina di destinazione di ADAC. Un'attività comune dell'helpdesk in qualsiasi rete è la reimpostazione delle password per gli account utente. Se l'utente ha dimenticato la password, l'ha modificata di recente e l'ha digitata in modo errato o se si sta reimpostando una password durante qualche altro tipo di risoluzione dei problemi, la reimpostazione di una password per un account utente in genere comporta numerosi clic del mouse all'interno di utenti e computer di AD per ottenere il lavoro fatto. Ora, c'è un collegamento rapido chiamato Reimposta password, mostrato proprio qui nella pagina principale del Centro di amministrazione di Active Directory. Utile anche la funzione di ricerca globale proprio accanto ad essa, dove puoi digitare qualsiasi cosa nel campo di ricerca e setaccia l'intera directory per i risultati relativi alla tua ricerca. Questa è un'altra attività comune in AD che in precedenza richiedeva più clic per eseguire:



Se fai clic sul nome del tuo dominio nella struttura di navigazione a sinistra, ti immergerai un po 'più a fondo nelle capacità di ADAC. Come puoi vedere, le informazioni elencate qui vengono estratte da Active Directory e sembrano le stesse informazioni che vedresti in Utenti e computer di AD. È corretto, tranne che invece di dover fare clic con il pulsante destro del mouse per ogni funzione, come le nuove creazioni o ricerche dell'utente, ora hai alcune attività rapide disponibili sulla destra che possono avviarti rapidamente nell'esecuzione di queste funzioni. Interessanti anche i collegamenti per aumentare il livello di funzionalità della foresta o del dominio in questa schermata. Per fare ciò utilizzando gli strumenti classici, vedo che la maggior parte degli amministratori lo fa avviando AD Domains and Trusts. Così, uno dei grandi vantaggi del nuovo strumento ADAC è che è in grado di fornire una finestra di gestione centralizzata dalla quale è possibile eseguire attività che normalmente avrebbero richiesto più finestre e console di gestione. Senti un tema comune in tutto Windows Server 2019 con la gestione centralizzata di tutto?



Controllo dinamico degli accessi

Oltre a insegnare nuovi trucchi ai vecchi cani, il Centro di amministrazione di Active Directory porta sul tavolo anche alcune nuove funzionalità che non sono disponibili da nessuna parte negli strumenti classici. Se guardi ancora una volta l'albero a sinistra, vedrai che la sezione successiva nell'elenco è Dynamic Access Control (DAC). Questa è una tecnologia che riguarda la sicurezza e la governance dei tuoi file, i dati aziendali che devi conservare saldamente e assicurarti che non cadano nelle mani sbagliate. DAC ti dà la possibilità di etichettare i file, classificandoli in tal modo per gruppi o usi particolari. Quindi è possibile creare criteri di controllo degli accessi che definiscono chi ha accesso a questi file particolarmente contrassegnati. Un'altra potente caratteristica del controllo dinamico degli accessi è la funzionalità di reporting. Una volta che il DAC è stato stabilito e in esecuzione nel tuo ambiente,

DAC può anche essere utilizzato per modificare le autorizzazioni degli utenti in base al tipo di dispositivo che stanno attualmente utilizzando. Se la nostra utente Susie accede con il desktop della sua azienda sulla rete, dovrebbe avere accesso a quei file sensibili delle risorse umane. D'altra parte, se porta il suo laptop personale in ufficio e lo collega alla rete, potremmo non voler consentire l'accesso a questi stessi file, anche quando forniamo le credenziali dell'utente del suo dominio, semplicemente perché non possediamo la sicurezza su quel laptop. Questi tipi di distinzioni possono essere effettuate utilizzando i criteri di controllo dinamico degli accessi.

Controller di dominio di sola lettura (RODC)

Non possiamo concludere la nostra panoramica degli strumenti e dei componenti importanti di Active Directory senza trattare i controller di dominio di sola lettura (RODC) in modo un po 'più dettagliato. In genere, quando si installano nuovi controller di dominio nella rete, si aggiunge il ruolo in modo da renderli un controller di dominio regolare, scrivibile e

completamente funzionante sulla rete in modo che possa eseguire tutti gli aspetti del ruolo di Servizi di dominio Active Directory. Ci sono alcune circostanze in cui questo non è il modo migliore per procedere, ed è per questo che il RODC è qui per aiutarti. Questo non è un ruolo separato, ma piuttosto una configurazione diversa dello stesso ruolo di Servizi di dominio Active Directory che vedrai durante la rotazione attraverso le schermate della procedura guidata durante la configurazione del tuo nuovo controller di dominio. Un RODC è un controller di dominio specializzato, in cui non è possibile scrivere nuovi dati. Contengono una cache, copia di sola lettura solo di alcune parti della directory. Puoi dire a un RODC di conservare una copia di tutte le credenziali all'interno del tuo dominio, oppure puoi anche dirgli di mantenere solo un elenco di credenziali selettive che saranno importanti per quel particolare RODC. Quali sono i motivi per utilizzare un RODC? Le filiali e le DMZ sono le più comuni che vedo.

Se hai una filiale più piccola con un numero inferiore di persone, potrebbe essere vantaggioso per loro avere un controller di dominio locale in modo che l'elaborazione dell'accesso sia veloce ed efficiente, ma poiché non hai una buona gestione della sicurezza fisica in quel piccolo ufficio, preferiresti non avere un DC in piena regola che qualcuno potrebbe raccogliere e andarsene.
Questo potrebbe essere un buon utilizzo per un RODC. Un altro è all'interno di una rete DMZ sicura. Si tratta di reti perimetrali tipicamente progettate per un accesso molto limitato, perché sono connesse a Internet pubblico. Alcuni dei tuoi server e servizi che si trovano all'interno della rete DMZ potrebbero aver bisogno dell'accesso ad Active Directory, ma non vuoi aprire un canale di comunicazione dalla DMZ a un controller di dominio completo nella tua rete. È possibile installare un RODC all'interno della DMZ, fare in modo che memorizzi nella cache le informazioni di cui ha bisogno per servire quei particolari server nella DMZ e creare un dominio o un sottodominio molto più sicuro all'interno di quella rete DMZ.

Il potere dei Criteri di gruppo

In una rete basata su server Windows e Active Directory, è quasi sempre il caso che anche il set principale di computer client sia basato sui sistemi operativi Microsoft Windows e che queste macchine siano tutte aggiunte a un dominio. L'impostazione di tutto in questo modo non solo ha senso dal punto di vista organizzativo all'interno di Active Directory, ma consente anche l'autenticazione centralizzata su dispositivi e applicazioni, come abbiamo già detto. So che in un paio di esempi che ho fornito in precedenza nel libro ho detto qualcosa del tipo, e quando un'azienda ha una politica di sicurezza in atto che ... o Assicurati che i tuoi server non ottengano quelle politiche di sicurezza esistenti perché ... Quindi quali sono queste politiche di sicurezza magiche, e come posso impostarne una?

Questo è il potere dei Criteri di gruppo. Consente di creare oggetti Criteri di gruppo (GPO) che contengono impostazioni e configurazioni che si desidera applicare ai computer o agli utenti nel dominio Active Directory. Dopo aver creato e costruito un oggetto Criteri di gruppo con una varietà di impostazioni, hai la possibilità di indirizzarlo in qualsiasi direzione tu scelga. Se si dispone di un criterio che si desidera applicare a tutti i sistemi desktop, è possibile indirizzarlo all'unità organizzativa o al gruppo di sicurezza appropriato in Active Directory che ospita tutti i computer desktop aggiunti al dominio. O forse hai creato un GPO che si applica solo ai tuoi computer Windows 7; è possibile filtrarlo in modo appropriato in modo che solo quei sistemi ricevano la politica. E la vera magia è che l'emissione di queste impostazioni avviene automaticamente, semplicemente perché i computer vengono aggiunti al tuo dominio. Non è necessario toccare affatto i sistemi client per eseguire il push delle impostazioni tramite un oggetto Criteri di gruppo. Puoi modificare o bloccare quasi tutto all'interno del sistema operativo Windows utilizzando Criteri di gruppo.

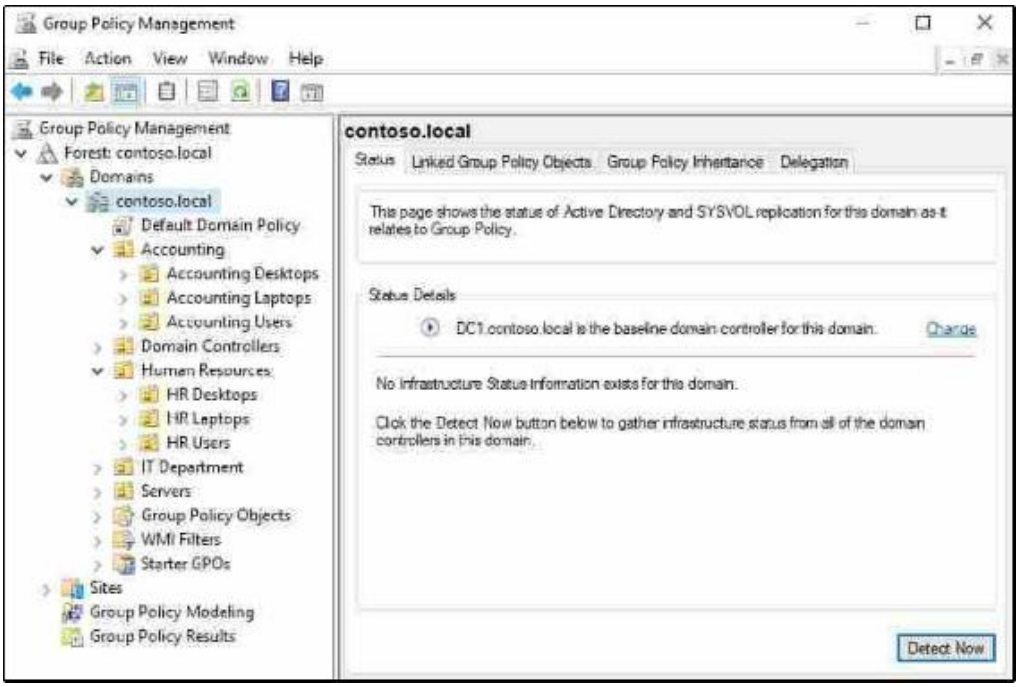
Quindi, ancora una volta, sto cercando nell'elenco dei ruoli disponibili sul mio Windows Server 2019 e non ne vedo uno chiamato Criteri di gruppo. Correggi di nuovo: non ce n'è uno! In effetti, se hai seguito la configurazione del laboratorio in questo libro, hai già Criteri di gruppo completamente funzionanti nella tua rete. Tutto ciò di cui i Criteri di gruppo hanno bisogno per funzionare fa parte di Servizi di dominio Active Directory. Quindi, se hai un controller di dominio nella tua rete, allora hai anche Criteri di gruppo sullo stesso server, perché tutte le informazioni utilizzate da Criteri di gruppo sono archiviate nella directory. Poiché l'installazione del ruolo di Servizi di dominio Active Directory è tutto ciò di cui abbiamo bisogno per utilizzare Criteri di gruppo e l'abbiamo già fatto nel nostro controller di dominio, lascia ' s entra subito e dai un'occhiata ad alcune cose che ti permetteranno di iniziare a utilizzare i Criteri di gruppo nel tuo ambiente immediatamente. Negli anni ho lavorato con molte piccole imprese che eseguivano un server Windows semplicemente perché è quello che fanno tutti, giusto? Chiunque sia il ragazzo o l'azienda IT che ha configurato questo server per loro, di certo non ha mai mostrato loro nulla sugli oggetti Criteri di gruppo, quindi hanno questo potente strumento semplicemente seduto nella cassetta degli attrezzi, inutilizzato e in attesa di essere liberato. Se non stai già utilizzando gli oggetti Criteri di gruppo, voglio che tu apra quella scatola e provi. e così hanno questo potente strumento semplicemente seduto nella cassetta degli attrezzi, inutilizzato e in attesa di essere liberato. Se non stai già utilizzando gli oggetti Criteri di gruppo, voglio che tu apra quella scatola e provi. e così hanno questo potente strumento semplicemente seduto nella cassetta degli attrezzi, inutilizzato e in attesa di essere liberato. Se non stai già utilizzando gli oggetti Criteri di gruppo, voglio che tu apra quella scatola e provi.

Il criterio di dominio predefinito

Innanzitutto, dobbiamo capire dove andiamo sul nostro controller di dominio in modo da poter creare e manipolare oggetti Criteri di gruppo. Come nel caso di qualsiasi strumento amministrativo su Windows Server

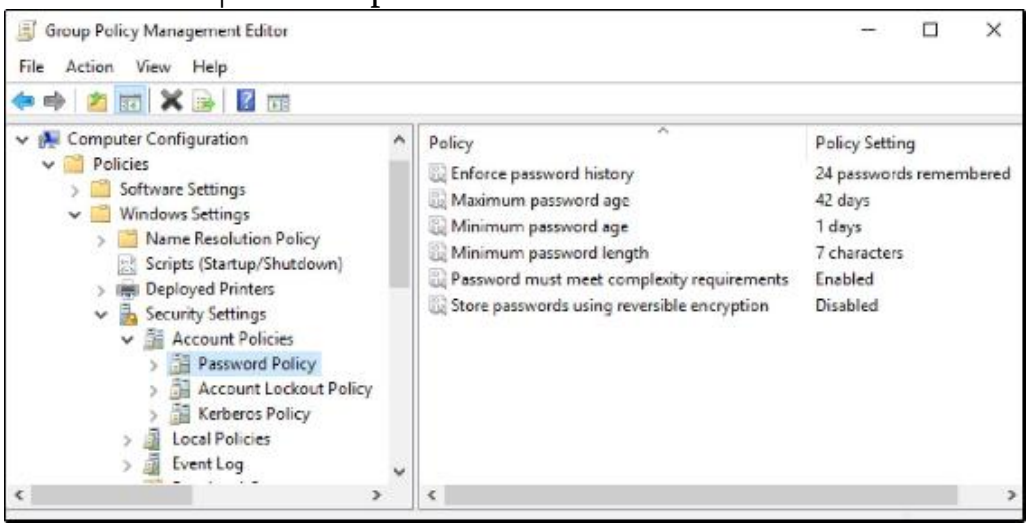
2019, Server Manager è la piattaforma centrale per l'apertura della tua console. Fare clic sul menu Strumenti da Server Manager e selezionare Gestione criteri di gruppo.

Una volta aperta la console, espandere il nome della foresta dall'albero di navigazione a sinistra, quindi espandere anche Domini e scegliere il nome del dominio. All'interno vedrai alcuni oggetti dall'aspetto familiare. Questo è un elenco delle unità organizzative che hai creato in precedenza e un paio di altre cartelle accanto alle tue unità organizzative:



Parleremo del motivo per cui l'elenco delle unità organizzative esiste qui a breve, ma, per ora, vogliamo concentrarci su un particolare oggetto Criteri di gruppo che è in genere vicino alla parte superiore di questo elenco, immediatamente sotto il nome del tuo dominio. Si chiama Default Domain Policy. Questo oggetto Criteri di gruppo viene collegato ad Active Directory per impostazione predefinita durante l'installazione e si applica a tutti gli utenti e i computer che fanno parte della directory del dominio. Poiché questo oggetto Criteri di gruppo è completamente abilitato sin dall'inizio e si applica a tutti, è un luogo comune per le aziende applicare criteri globali per le password o regole di sicurezza che devono essere applicate a tutti.

Con qualsiasi oggetto Criteri di gruppo visualizzato nella console di gestione, se fai clic con il pulsante destro del mouse su tale oggetto Criteri di gruppo e quindi scegli Modifica ... vedrai una nuova finestra aperta e questo Editor di oggetti Criteri di gruppo contiene tutti i componenti interni di quel criterio. Qui è dove si effettuano le impostazioni o le configurazioni che si desidera far parte di quel particolare oggetto Criteri di gruppo. Quindi, vai avanti e modifica il tuo criterio di dominio predefinito, quindi vai a Configurazione computer | Politiche | Impostazioni di Windows | Impostazioni di sicurezza | Politiche dell'account | Criterio password:



Qui puoi vedere un elenco delle diverse opzioni disponibili per la configurazione della politica delle password all'interno del tuo dominio. Facendo doppio clic su una qualsiasi di queste impostazioni è possibile modificarle e tale modifica inizia immediatamente ad avere effetto su tutti i computer aggiunti al dominio nella rete. Ad esempio, puoi vedere che la lunghezza minima della password predefinita è impostata su 7 caratteri. Molte aziende hanno già discusso molto sulla propria politica scritta sulla lunghezza standard delle password nella rete e, per configurare la nuova infrastruttura di directory in modo che accetti la propria decisione, è sufficiente modificare questo campo. La modifica della lunghezza minima della password a 12 caratteri qui richiederebbe immediatamente la modifica per tutti gli account utente la prossima volta che reimpostano le password.

Se guardi lungo l'albero a sinistra dell'Editor Gestione Criteri di gruppo, puoi vedere che c'è una quantità incredibilmente grande di impostazioni e configurazioni che possono essere eliminate tramite Criteri di gruppo. Sebbene il criterio di dominio predefinito sia un modo molto semplice e veloce per configurare alcune impostazioni e renderlo disponibile a tutti, procedere con cautela quando si apportano modifiche a questo criterio predefinito. Ogni volta che apporti un cambiamento di impostazione qui, ricorda che influenzerà tutti nel tuo dominio, incluso te stesso. Molte volte creerai criteri che non devono essere applicati a tutti e, in questi casi, ti consigliamo vivamente di stare lontano dal criterio di dominio predefinito e invece di impostare un nuovo oggetto Criteri di gruppo per eseguire qualsiasi attività sia quella stai cercando di mettere in atto. Infatti, alcuni amministratori consigliano di non toccare mai il criterio di dominio predefinito e di assicurarsi di utilizzare sempre un nuovo oggetto Criteri di gruppo ogni volta che si hanno nuove impostazioni da inserire. In pratica, vedo molte aziende che utilizzano il criterio di dominio predefinito integrato per i requisiti di complessità delle password, ma questo è tutto. Tutte le altre modifiche o impostazioni devono essere incluse in un nuovo oggetto Criteri di gruppo.

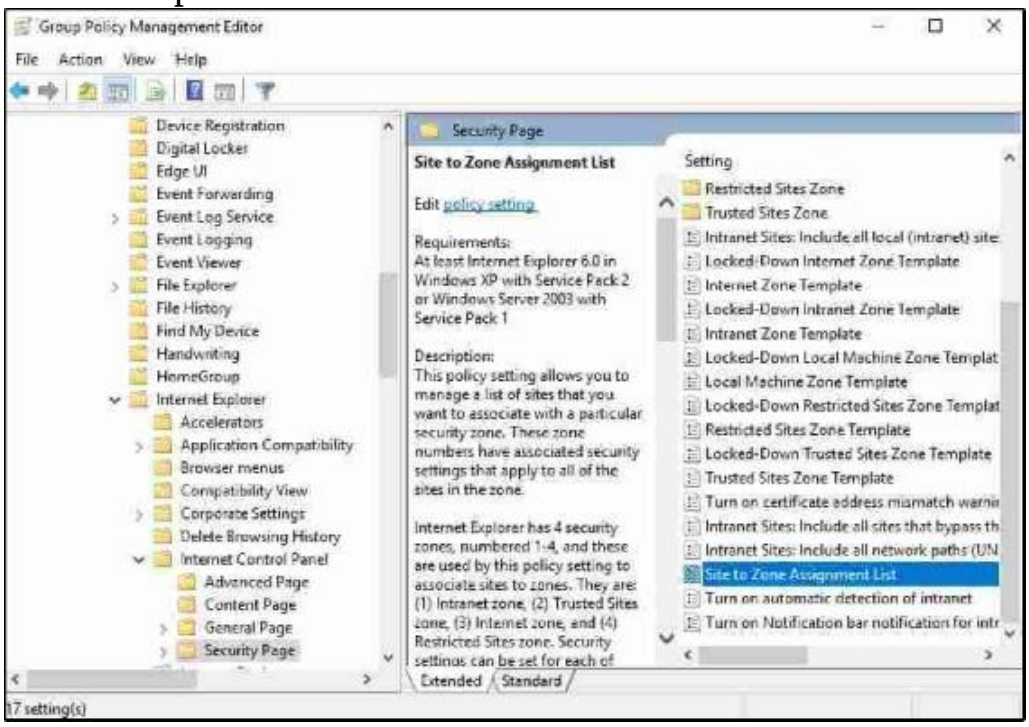
Creazione e collegamento di un nuovo GPO

Se la procedura migliore in generale è creare un nuovo oggetto Criteri di gruppo quando è necessario applicare alcune impostazioni, è meglio dedicare un minuto a coprire tale processo. Per questo esempio, creeremo un nuovo GPO che inserisce un elenco di siti attendibili in Internet Explorer sui nostri computer desktop. Se esegui un'applicazione web nella tua rete che deve eseguire controlli JavaScript o ActiveX, o qualcosa del genere, potrebbe essere necessario che il sito web faccia parte dell'elenco dei siti attendibili all'interno di Internet Explorer affinché funzioni correttamente. È possibile stampare una pagina di istruzioni per l'helpdesk su come eseguire questa operazione su ogni computer e farli passare il tempo a farlo per ogni utente che chiama

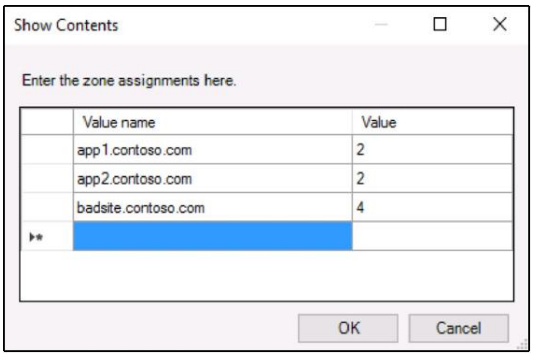
perché non può accedere all'applicazione. Oppure puoi semplicemente creare un oggetto Criteri di gruppo che apporta queste modifiche automaticamente su ogni workstation, e salva tutte quelle telefonate. Questo è solo un piccolo esempio del potere che possiede i Criteri di gruppo, ma è un buon esempio perché è qualcosa di utile ed è un'impostazione che è un po 'sepolta nelle impostazioni dell'oggetto Criteri di gruppo, in modo che tu possa avere un'idea di quanto sono profonde queste capacità.

Nella console Gestione Criteri di gruppo, fai clic con il pulsante destro del mouse sulla cartella denominata Oggetti Criteri di gruppo e scegli Nuovo. Assegna un nome al nuovo oggetto Criteri di gruppo (il mio si chiama Aggiunta di siti attendibili), quindi fai clic su OK. Il tuo nuovo oggetto Criteri di gruppo ora viene visualizzato nell'elenco degli oggetti Criteri di gruppo disponibili, ma non si applica ancora a nessuno o a nessun computer. Prima di assegnare questo nuovo oggetto Criteri di gruppo a chiunque, colleghiamo quell'elenco di siti attendibili in modo che il criterio contenga le nostre informazioni di configurazione. Abbiamo una nuova norma, ma al momento non è presente alcuna impostazione.

Fare clic con il pulsante destro del mouse sul nuovo oggetto Criteri di gruppo e scegliere **Modificare.** Ora vai a Configurazione computer | **Politiche | Modelli amministrativi | Componenti di Windows | Internet Explorer |**
Pannello di controllo Internet | Pagina di sicurezza. Vedi, te l'avevo detto che era sepolto lì!

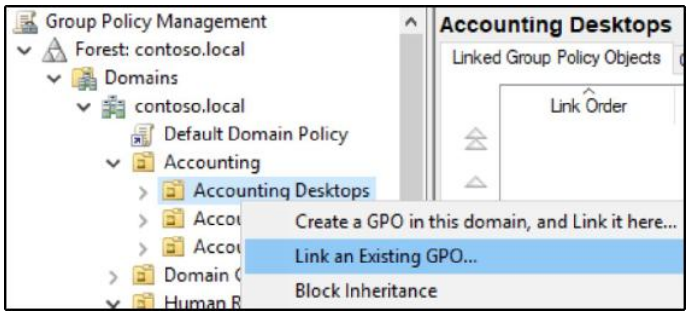


Ora, fai doppio clic su Site to Zone Assignment List e impostalo su Enabled. Ciò consente di fare clic sul pulsante Mostra ..., all'interno del quale è possibile accedere a siti Web e assegnare loro assegnazioni di zone. Ogni impostazione GPO ha un bel testo descrittivo per accompagnarla, che ti dice esattamente a cosa serve quella particolare impostazione e cosa significano le opzioni. Come puoi vedere nel testo di questo, per impostare i miei siti Web come siti affidabili, devo assegnare loro un valore di assegnazione di zona di 2. E, solo per divertimento, ho anche aggiunto in un sito che non lo faccio desidera essere accessibile ai miei utenti e gli ha assegnato un valore di zona di 4 in modo che badsite.contoso.com sia un membro della zona dei siti con restrizioni su tutti i miei computer desktop. Ecco la mia lista completa:



Abbiamo finito? Quasi. Non appena faccio clic sul pulsante OK, queste impostazioni sono ora archiviate nel mio oggetto Criteri di gruppo e sono pronte per essere distribuite, ma a questo punto non ho assegnato il mio nuovo oggetto Criteri di gruppo a nulla, quindi è solo seduto in attesa da essere usato.

Tornando alla console Gestione criteri di gruppo, trova il percorso a cui desideri collegare questo nuovo oggetto Criteri di gruppo. È possibile collegare un oggetto Criteri di gruppo all'inizio del dominio in modo simile al modo in cui funziona il criterio di dominio predefinito e verrà quindi applicato a tutto ciò che si trova al di sotto di quel collegamento. Quindi, in effetti, inizierebbe ad applicarsi a ogni macchina nella rete del tuo dominio. Per questo particolare esempio, non vogliamo che le impostazioni del sito attendibile siano così globali, quindi creeremo invece il nostro collegamento a una particolare unità organizzativa. In questo modo, questo nuovo oggetto Criteri di gruppo verrà applicato solo ai computer archiviati all'interno di tale unità organizzativa. Desidero assegnare questo oggetto Criteri di gruppo alla mia unità organizzativa desktop di contabilità che ho creato in precedenza. Quindi trovo semplicemente quell'unità organizzativa, faccio clic con il pulsante destro del mouse su di essa, quindi scelgo Collega un oggetto Criteri di gruppo esistente ...:


Group Policy Management
Forest: contoso.local
Domains
contoso.local
Default Domain Policy
Accounting
Accounting Desktops
Domain
Accounting Desktops
Linked Group Policy Objects
Link Order
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance

Ora vedo un elenco degli oggetti Criteri di gruppo disponibili per il collegamento. Scegli il nuovo GPO per l'aggiunta di siti attendibili e fai clic su OK, e il gioco è fatto! Il nuovo oggetto Criteri di gruppo è ora collegato all'unità organizzativa dei computer desktop e applicherà tali impostazioni a tutte le macchine che inserisco all'interno dell'unità organizzativa.

È possibile collegare un oggetto Criteri di gruppo a più di un'unità organizzativa. Basta seguire di nuovo la stessa procedura, questa volta scegliendo un'altra unità organizzativa in cui si desidera creare il collegamento e quell'oggetto Criteri di gruppo verrà ora applicato a entrambe le unità organizzative che hanno collegamenti attivi. È inoltre possibile rimuovere

Filtraggio di oggetti Criteri di gruppo su dispositivi particolari

Ora che hai creato un oggetto Criteri di gruppo e lo hai collegato a una particolare unità organizzativa, disponi di informazioni sufficienti per iniziare davvero a utilizzare Criteri di gruppo nel tuo ambiente. L'uso dei collegamenti per determinare quali macchine o utenti ottengono quali criteri è il metodo più comune che vedo utilizzare gli amministratori, ma ci sono molte circostanze in cui potresti voler fare un ulteriore passo avanti. E se avessi un nuovo oggetto Criteri di gruppo e lo avessi collegato a un'unità organizzativa che conteneva tutti i tuoi computer desktop, ma poi decidessi che alcune di quelle macchine avevano bisogno del criterio e altre no? Sarebbe un grattacapo dover dividere quelle macchine in due unità organizzative separate solo per lo scopo di questa politica che stai creando. È qui che entra in gioco il filtro di sicurezza GPO.

Il filtro di sicurezza è la capacità di filtrare un oggetto Criteri di gruppo fino a particolari oggetti di Active Directory. Su qualsiasi oggetto Criteri di gruppo nella directory, è possibile impostare filtri in modo che l'oggetto Criteri di gruppo si applichi solo a determinati utenti, determinati computer o anche particolari gruppi di utenti o computer. Trovo che l'uso dei gruppi sia particolarmente utile. Quindi, per il nostro esempio precedente, in cui abbiamo un criterio che deve essere applicato solo ad

alcuni computer desktop, potremmo creare un nuovo gruppo di sicurezza all'interno di Active Directory e aggiungere solo quei computer nel gruppo. Una volta che l'oggetto Criteri di gruppo è stato configurato con il gruppo elencato nella sezione dei filtri, tale criterio verrà applicato solo alle macchine che fanno parte di quel gruppo. In futuro, se avessi bisogno di rimuovere quel criterio da alcuni computer o aggiungerlo a nuovi computer, devi semplicemente aggiungere o rimuovere macchine dal gruppo stesso e non

La sezione Filtro di sicurezza viene visualizzata quando si fa clic su un oggetto Criteri di gruppo dall'interno della console Gestione criteri di gruppo. Vai avanti e apri GPMC e fai semplicemente clic una volta su uno dei tuoi oggetti Criteri di gruppo. Sul lato destro, vedi lo Scope aperto per quella policy. La sezione in alto mostra quali collegamenti sono attualmente attivi sulla politica e la metà inferiore dello schermo mostra la sezione Filtro di sicurezza. Puoi vedere qui che ho collegato il mio oggetto Criteri di gruppo all'unità organizzativa desktop di contabilità, ma ho impostato un filtro di sicurezza aggiuntivo in modo che solo le macchine che fanno parte del gruppo Contabilità - Siti attendibili riceveranno effettivamente le impostazioni dal mio oggetto Criteri di gruppo:

Un'altra caratteristica interessante che è a portata di clic è la scheda Impostazioni su questa stessa schermata. Fare clic su quella scheda e verranno visualizzate tutte le configurazioni attualmente impostate all'interno del GPO. Ciò è molto utile per controllare gli oggetti Criteri di gruppo che qualcun altro potrebbe aver creato, per vedere quali impostazioni vengono

Come accennato in precedenza, potresti prendere una qualsiasi di queste console di gestione o argomenti relativi ai servizi di infrastruttura di base all'interno di Windows Server e trasformare quell'argomento nel suo libro. In realtà ho avuto l'opportunità di fare esattamente questo con Criteri di gruppo. Se sei interessato a scoprire di più sui Criteri di gruppo e su tutti i modi in cui possono essere utilizzati per proteggere la tua infrastruttura, dai un'occhiata a Packt's Mastering Windows Group Policy (https: //www. packtpub.com /networking-e-server /mastering-finestre-gruppo-politica).

Domain Name System (DNS)

Se consideriamo i servizi di dominio Active Directory come il ruolo più comune e centrale nel far funzionare le nostre reti incentrate su Microsoft, il ruolo DNS (Domain Name System) si trova al numero due. Devo ancora incontrare un amministratore che ha scelto di distribuire un dominio senza distribuire DNS allo stesso tempo: vanno sempre di pari passo.

Il DNS è un servizio che viene in genere fornito da un server Windows, ma non deve esserlo. Sono disponibili molte piattaforme diverse, dai server Linux alle apparecchiature hardware specializzate progettate specificamente per la gestione del DNS all'interno di una rete che può essere utilizzata per questo ruolo. Per la maggior parte delle reti incentrate su Microsoft e ai fini di questo libro, supporremo che desideri utilizzare Windows Server 2019 per ospitare il ruolo

Il DNS è simile ad Active Directory in quanto è un database strutturato che viene spesso archiviato sui server del controller di dominio e distribuito automaticamente nella rete ad altri server DNS / controller di dominio. Laddove il database di un AD contiene informazioni sugli oggetti di dominio stessi, DNS è responsabile dell'archiviazione e della risoluzione di tutti i nomi sulla rete. Cosa intendo per nomi? Ogni volta che un utente o un computer tenta di contattare qualsiasi risorsa chiamando un nome, DNS è la piattaforma responsabile della trasformazione di quel nome in qualcos'altro per portare il traffico alla destinazione corretta. Vedete, il modo in cui il traffico arriva dal client al server avviene tramite la rete e in genere tramite lo stack TCP / IP, utilizzando un indirizzo IP per arrivare a destinazione. Quando apro un'applicazione sul mio computer per accedere ad alcuni dati che risiedono su un server,

Se collego 10.10.10.15 al mio applicazione configurazione, esso voluto Aperto con successo. Se io impostare centinaia di computer diversi in questo modo, tutti che puntano a indirizzi IP, funzionerebbe bene per un po '. Ma verrà il giorno in cui, per qualsiasi motivo, potrebbe essere necessario modificare l'indirizzo IP. O forse aggiungo un secondo server per condividere il carico e gestire il mio aumento del traffico utente. Cosa fare adesso? Visitare nuovamente ogni computer client e aggiornare l'indirizzo IP utilizzato? Certamente no. Questo è uno dei motivi per cui il DNS è fondamentale per il modo in cui progettiamo e gestiamo le nostre infrastrutture. Utilizzando il DNS possiamo utilizzare nomi invece di indirizzi IP. Con DNS, la mia applicazione può essere configurata per parlare con Server01 o qualunque sia il nome del mio server, e se ho bisogno di cambiare l'indirizzo IP in un secondo momento, Lo cambio semplicemente all'interno della console DNS con l'indirizzo IP aggiornato e immediatamente tutti i miei computer client inizieranno a risolvere il nome Server01 nel nuovo indirizzo IP. Oppure posso anche utilizzare un nome più generico, come intranet, e farlo risolvere su più server diversi. Ne discuteremo un po 'più a breve.

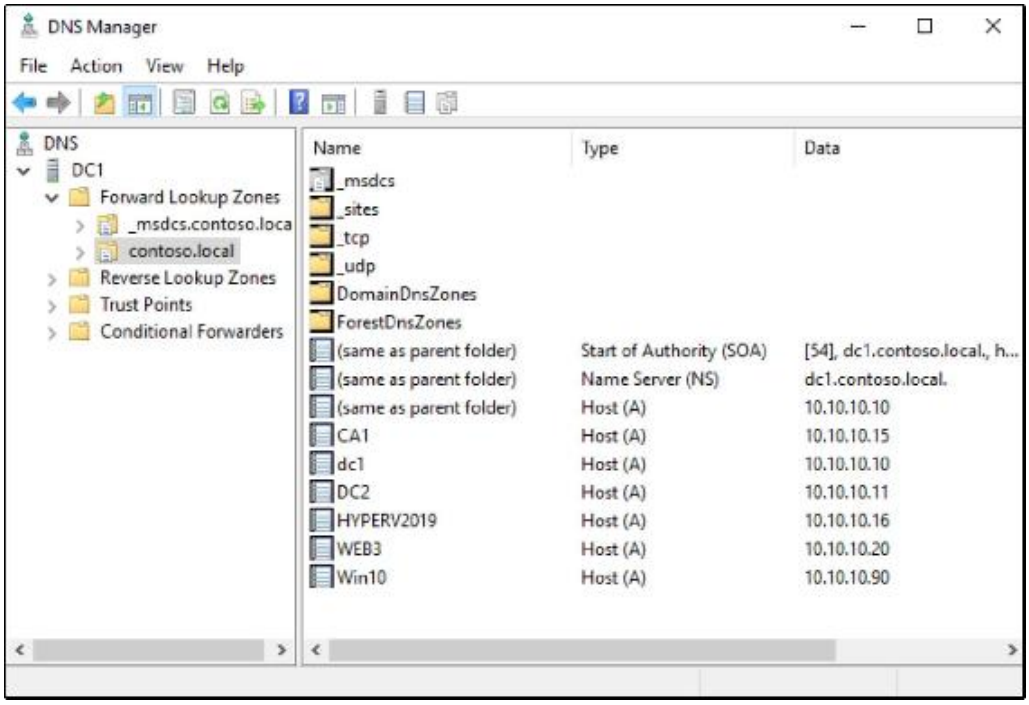
Ogni volta che un computer effettua una chiamata a un server, a un servizio o a un sito Web, utilizza il DNS per convertire quel nome in un'informazione più utile per garantire che la connessione di rete avvenga correttamente. Lo stesso vale sia all'interno che all'esterno delle reti aziendali. Sul mio portatile personale in questo momento, se apro Internet Explorer e accedo a https: //www.bing.com /, il server DNS del mio provider Internet si sta risolvendo http://www.bing.com/ ad IP indirizzo su la rete, quale è l'indirizzo quello mio il laptop comunica con e in modo che la pagina si apra correttamente. Quando lavoriamo all'interno delle nostre reti aziendali, non vogliamo fare affidamento o fidarci di un provider pubblico con le informazioni sul nome del nostro server interno, quindi costruiamo i nostri server DNS all'interno della rete. Poiché i record DNS all'interno di una rete di dominio risolvono quasi sempre i nomi in oggetti che risiedono all'interno di Active Directory, ha senso quindi che DNS e Servizi di dominio Active Directory siano strettamente integrati. Ciò suona vero nella maggior parte delle reti Microsoft, dove è una pratica

molto comune installare sia il ruolo di Servizi di dominio Active Directory, sia il ruolo DNS, sui server del controller di dominio.

Diversi tipi di record DNS

Dopo aver installato il nostro ruolo DNS su un server nella rete, possiamo iniziare a usarlo per creare record DNS, che risolvono i nomi nei loro indirizzi IP corrispondenti o altre informazioni necessarie per instradare il nostro traffico sulla rete. Supponendo che tu stia lavorando in una rete di dominio, potresti essere piacevolmente sorpreso di vedere che un certo numero di record esiste già all'interno del DNS, anche se non ne hai creato nessuno. Quando si eseguono Active Directory e DNS insieme, il processo di aggiunta al dominio eseguito con i computer e i server registra automaticamente un record DNS durante tale processo.

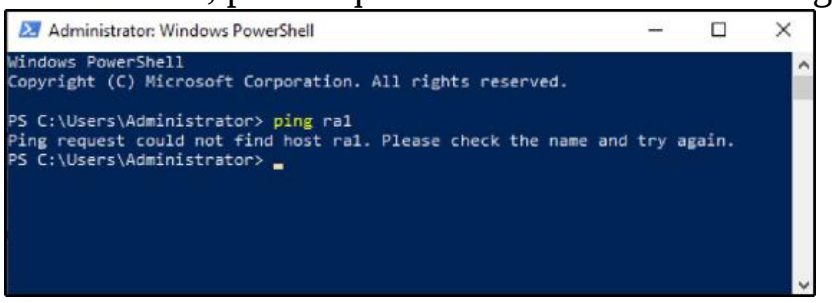
Non ho ancora creato alcun record DNS nel mio nuovo ambiente di laboratorio, comunque non intenzionalmente, eppure quando apro la console di DNS Manager dall'interno del menu Strumenti di Server Manager, posso vedere una manciata di record già esistenti. Questo perché quando ho unito ciascuna di queste macchine al dominio, ha registrato automaticamente questi record per me in modo che i nuovi server e client fossero immediatamente risolvibili all'interno del nostro dominio:



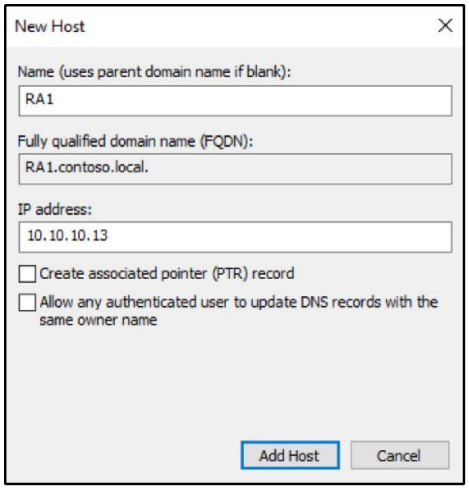
Record host (A o AAAA)

Il primo tipo di record DNS che stiamo esaminando è il tipo più comune con cui lavorerai. Un record host è quello che risolve un particolare nome in un particolare indirizzo IP. È piuttosto semplice e per la maggior parte dei dispositivi sulla rete questo sarà l'unico tipo di record che esiste per loro all'interno del DNS. Esistono due diverse classi di record host di cui dovresti essere a conoscenza, anche se probabilmente ne utilizzerai solo una per almeno qualche altro anno. I due diversi tipi di record host sono chiamati record A e record AAAA, che si pronuncia Quad A. La differenza tra i due? I record A sono per gli indirizzi IPv4 e verranno utilizzati nella maggior parte delle aziende negli anni a venire. I record AAAA hanno lo stesso identico scopo di risolvere un nome in un indirizzo IP, ma sono solo per indirizzi IPv6,

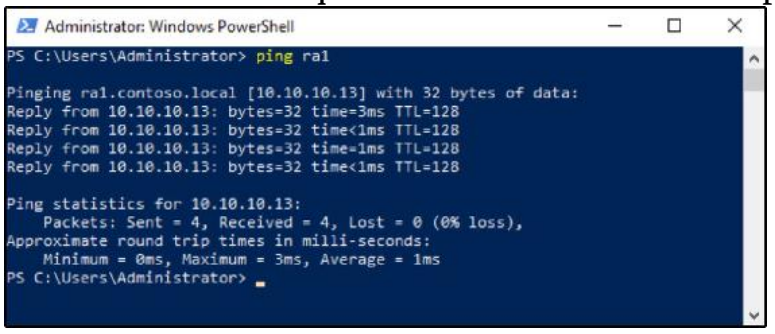
Nello screenshot precedente, puoi vedere alcuni record Host (A) che sono stati auto-creati quando quelle macchine sono entrate a far parte del nostro dominio. Ho anche un altro server in esecuzione sulla mia rete che non è ancora stato aggiunto a un dominio e quindi non si è registrato automaticamente nel DNS. Questo server si chiama RA1, ma se accedo a qualsiasi altro sistema sulla mia rete, non riesco a contattare il mio Server RA1, poiché quel nome non è ancora collegato al DNS:



Per ora, sceglierò di non unire questo server al dominio, in modo da poter creare manualmente un record DNS per esso e assicurarci di essere in grado di risolvere correttamente il nome dopo averlo fatto. Torna all'interno di DNS Manager sul mio server DNS, fai clic con il pulsante destro del mouse sul nome del tuo dominio elencato nella cartella Zone di ricerca diretta, quindi scegli Nuovo host (A o AAAA). All'interno della schermata per creare un nuovo record host, inserisci semplicemente il nome del tuo server e l'indirizzo IP che è configurato sulla sua interfaccia di rete:



Ora che abbiamo creato questo nuovo record host, dovremmo essere immediatamente in grado di iniziare a risolvere questo nome all'interno della nostra rete di dominio. Tornando alla macchina client da cui stavo provando a eseguire il ping di RA1 in precedenza, proverò di nuovo lo stesso comando e questa volta si risolverà e risponderà correttamente:

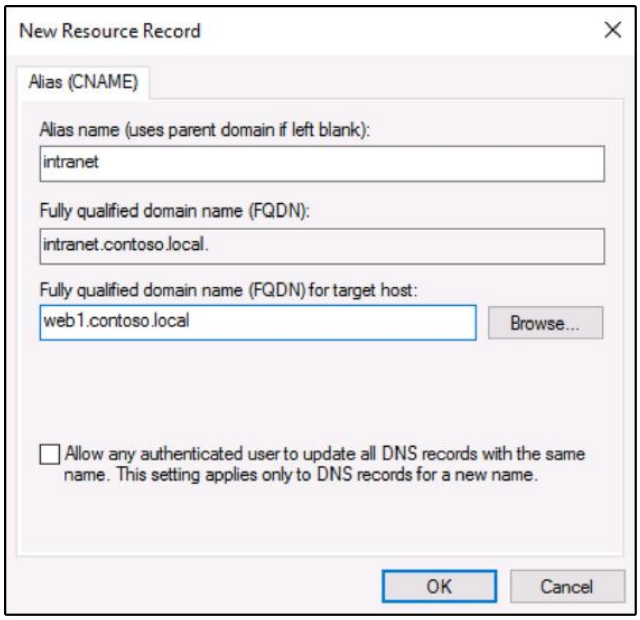


Record ALIAS - CNAME

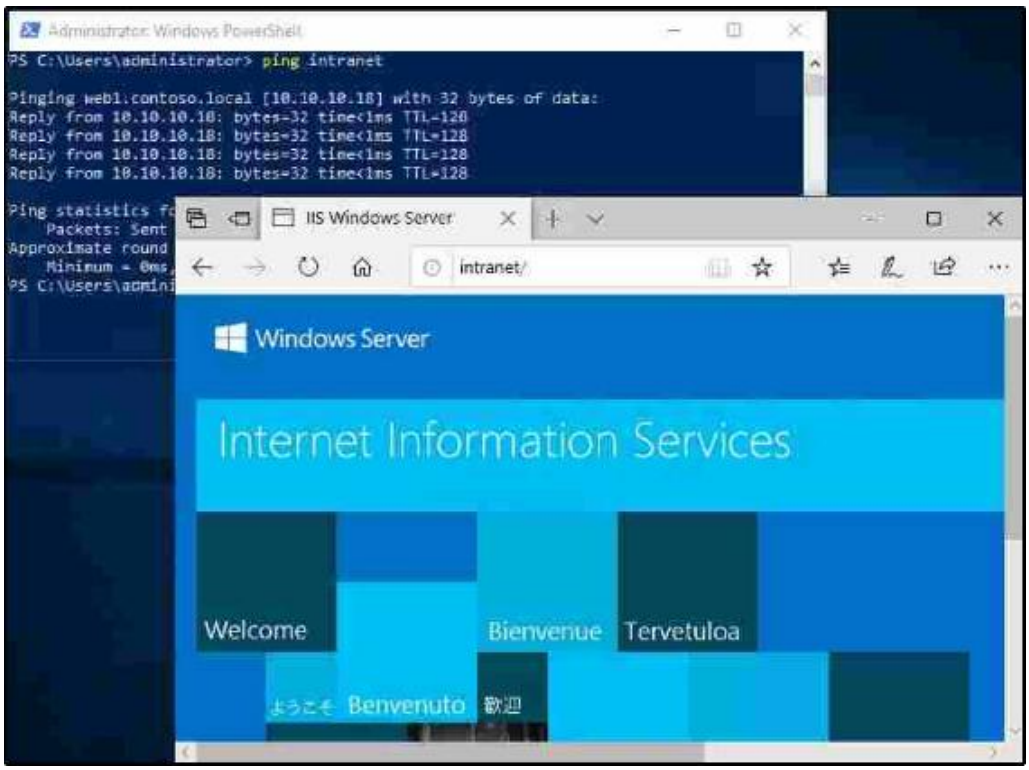
Un altro tipo utile di record DNS è CNAME, che più comunemente in questi giorni è chiamato record ALIAS. Questo è un record che puoi creare che prende un nome e lo punta a un altro nome. A prima vista sembra un po 'sciocco, perché, alla fine, dovrai ancora risolvere il tuo nome finale in un indirizzo IP per portare il traffico dove deve andare, ma gli scopi di un record ALIAS possono essere vasto. Un buon esempio per descrivere l'utilità di un record ALIAS è quando si esegue un server Web che serve siti Web all'interno della rete. Piuttosto che costringere tutti i tuoi utenti a ricordare un URL comehttp: //web1.contoso.local per accedere a un sito web, potremmo creare un ALIAS record chiamato intranet e indirizzalo a web1. In questo modo, il record intranet più generalizzato può sempre essere utilizzato dai computer client, che è un nome molto più amichevole da ricordare per gli utenti.

Oltre a creare un'esperienza utente più felice con questo nuovo record DNS, hai, allo stesso tempo, creato una flessibilità amministrativa aggiuntiva perché puoi facilmente modificare i componenti del server in esecuzione sotto quel record, senza dover regolare alcuna impostazione sul macchine client o riqualificare i dipendenti su come accedere alla pagina. Hai bisogno di sostituire un server web? Nessun problema, punta il record ALIAS su quello nuovo.
Hai bisogno di aggiungere un altro server web? Anche questo è facile, poiché possiamo creare più record ALIAS, tutti con lo stesso nome intranet, e indirizzarli ai diversi server web che sono in gioco nell'ambiente. Ciò crea una forma molto semplice di bilanciamento del carico, poiché il DNS inizierà a eseguire il round robin del traffico tra i diversi server Web, in base a quel record CNAME intranet.

In effetti, invece di continuare a parlarne, proviamolo. Ho un sito Web in esecuzione esattamente su quell'URL nel mio ambiente, ma al momento posso accedervi solo digitandohttp: //web1.contoso.local. All'interno di DNS, creerò un record ALIAS che reindirizza intranet a web1:



Ora, quando eseguo il ping di Intranet, puoi vedere che si risolve sul mio server web1. E quandoaccedendo alla pagina web, Posso semplicemente digitare la parola intranet nella barra degli indirizzi all'interno di Internet Explorer per avviare la mia pagina. Il sito Web stesso non è a conoscenza del cambio di nome in corso, quindi non ho dovuto apportare alcuna modifica al sito Web, solo all'interno del DNS:

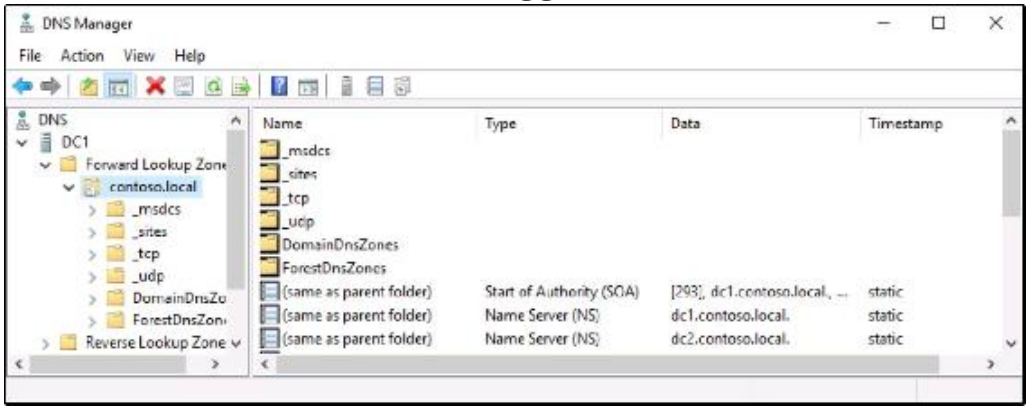


Record Mail Exchanger (MX)

Un terzo tipo di record DNS è chiamato record Mail Exchanger (MX). Nelle tue attività quotidiane, non dovresti incontrare o configurare record MX quasi quanto i record A o CNAME, ma è comunque importante comprenderli. Un record MX riguarda i servizi di posta elettronica e la consegna. Qualunque sia il nome di dominio che segue la "@" nel tuo indirizzo email, i server DNS che gestiscono quel nome di dominio devono contenere un record MX che indica al dominio dove puntare per i suoi servizi di posta. I record MX vengono utilizzati solo con DNS pubblico, per la risoluzione dei nomi su Internet. Per le aziende che ospitano la propria posta sui server Exchange locali, i server DNS pubblici conterranno un record MX che punta al proprio ambiente Exchange. Per le aziende che ospitano la propria posta elettronica in un servizio cloud,

Record Name Server (NS)

Eccone un altro con cui non devi occuparti giorno per giorno, ma dovresti comunque sapere a cosa serve. Un record NS è un identificatore all'interno di una zona DNS che gli dice quali server dei nomi (che sono i tuoi server DNS) utilizzare come autorità per quella zona. Se guardi i record NS elencati nel tuo DNS in questo momento, riconoscerai che sta chiamando i nomi dei tuoi server DNS sulla rete. Quando aggiungi un nuovo server DC / DNS al tuo dominio, un nuovo record NS per questo server verrà automaticamente aggiunto nella tua zona DNS:



Esistono molti altri possibili tipi di record che possono essere archiviati e utilizzati in un database DNS, ma in genere non sono rilevanti per l'amministratore di server comune in una tipica rete basata su Microsoft.

ipconfig / flushdns

Solo un'ultima nota per concludere questa sezione. Ho detto cose come Ora quando lo faccio ... o Immediatamente dopo questa modifica ... e se stai creando alcuni dei tuoi record, potresti aver notato che a volte ci vuole del tempo prima che i tuoi computer client li riconoscano nuovi record DNS. Questo è un comportamento normale e il tempo necessario prima che la modifica venga trasferita all'intera rete dipenderà interamente dalla dimensione della rete e dal modo in cui è configurata la replica di Active Directory. Quando crei un nuovo record DNS su un controller di dominio, il tuo nuovo record deve replicarsi su tutti gli altri controller di dominio della rete. Questo processo da solo può richiedere fino a un paio d'ore se AD non è configurato per una replica più rapida. In genere, ci vogliono solo pochi minuti.

Quindi, una volta che il nuovo record esiste su tutti i tuoi server DC, i tuoi client potrebbero impiegare ancora un po 'di tempo per utilizzare il nuovo record, perché i computer client in una rete di dominio conservano una cache di dati DNS. In questo modo, non devono contattare il server DNS per ogni singola richiesta di risoluzione del nome. Possono fare riferimento più rapidamente alla loro cache locale per vedere quali erano le informazioni dall'ultima volta che hanno effettuato il check-in con il server DNS. Se stai tentando di testare immediatamente un nuovo record DNS appena creato e non funziona, potresti provare a eseguire il comando ipconfig / flushdns sul tuo computer client. Ciò costringe il client a eseguire il dump delle proprie copie memorizzate nella cache locale dei record del resolver DNS e ad acquisire nuove informazioni aggiornate dal server DNS. Dopo aver svuotato la cache,

DHCP contro indirizzamento statico

Gli indirizzi IP sulla tua rete sono un po 'come gli indirizzi di casa sulla tua strada. Quando vuoi inviare un pacco a qualcuno, scrivi il suo indirizzo sulla parte anteriore del pacco e lo metti nella cassetta della posta. Allo stesso modo, quando il tuo computer vuole inviare dati a un server o un altro dispositivo su una rete, ognuno di questi dispositivi ha un indirizzo IP che viene utilizzato per la consegna di quei pacchetti. Sappiamo che il DNS è responsabile di indicare alle macchine quale nome risolve in quale indirizzo IP, ma come vengono messi in primo luogo quegli indirizzi IP sui server e sui computer?

L'indirizzamento statico è semplicemente il processo di configurazione manuale degli indirizzi IP sul sistema, utilizzando le proprie mani come strumento di configurazione per collegare tutte le informazioni sull'indirizzo IP alle impostazioni NIC su quel dispositivo. Sebbene questo sia un modo semplice e veloce per far fluire il traffico di rete tra pochi endpoint, assegnando a ciascuno un indirizzo IP, non è scalabile. Spesso indirizziamo staticamente i nostri server per assicurarci che quegli indirizzi IP non siano soggetti a modifiche, ma per quanto riguarda il client e il dispositivo? Anche in una piccola azienda con 10 dipendenti, ogni persona può avere un desktop e un laptop, è probabile che sulla rete ci siano anche server di stampa che necessitano di indirizzi IP e potresti avere una rete wireless in cui i dipendenti o anche gli ospiti possono connettere i telefoni e altri dispositivi per ottenere l'accesso a Internet. Assegnerai manualmente gli indirizzi IP a tutti questi dispositivi? Certamente no.

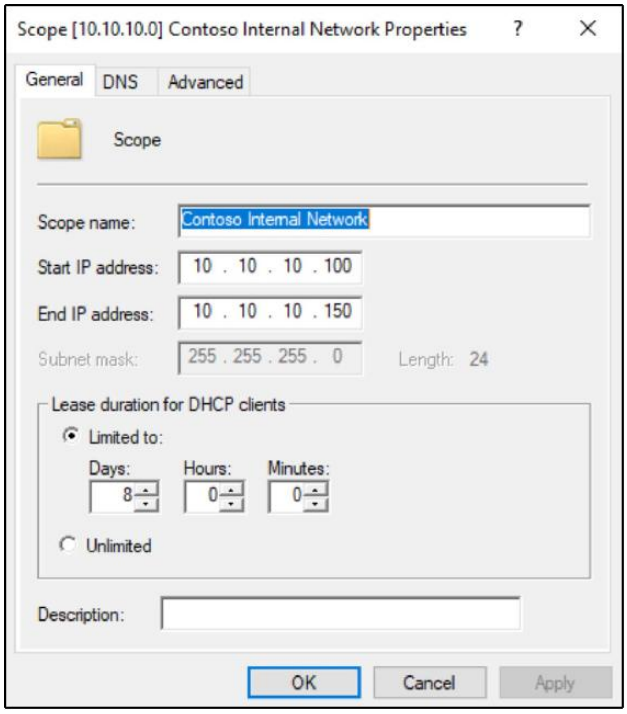
La nostra risposta a questo problema è il protocollo DHCP (Dynamic Host Configuration Protocol). Si tratta di un protocollo progettato per risolvere il nostro problema esatto fornendo la possibilità di collegare macchine e dispositivi alla rete e ottenere automaticamente informazioni sull'indirizzamento IP. Quasi tutti gli utenti su qualsiasi dispositivo in tutto il mondo utilizzano DHCP ogni giorno senza nemmeno rendersene conto. Quando colleghi il tuo laptop o smartphone a un router Wi-Fi per ottenere l'accesso a Internet, un server DHCP ti ha dato la possibilità di instradare il traffico su quella rete Wi-Fi assegnandoti informazioni di indirizzamento IP. Spesso, nel caso di un Wi-Fi pubblico, il tuo server DHCP è effettivamente in esecuzione sul router stesso, ma nelle nostre attività in cui Windows Server governa il data center, i nostri servizi DHCP sono spesso ospitati su uno o più server in rete.

L'ambito DHCP

Nel nuovo ambiente di laboratorio Windows Server 2019 che ho creato, finora ho assegnato staticamente gli indirizzi IP a tutti i server in fase di creazione. Questo sta iniziando a diventare vecchio e difficile da tenere

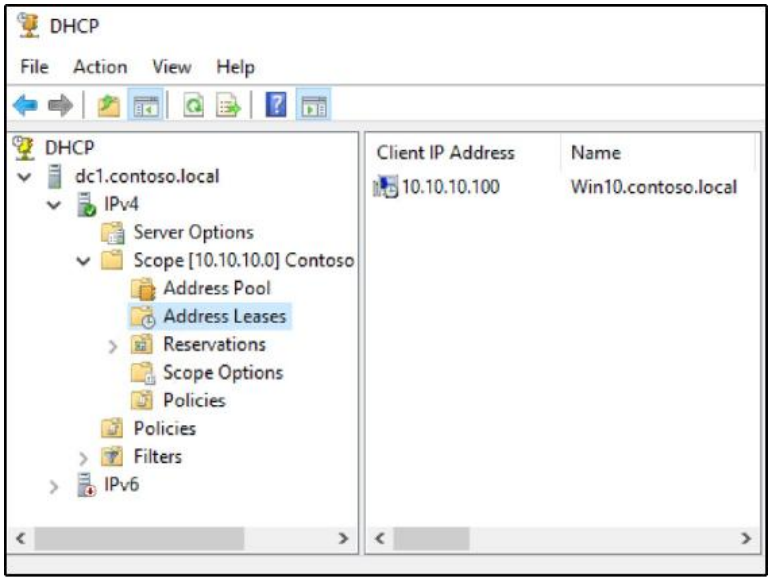
traccia. Quando è stato configurato il primo controller di dominio, ho effettivamente installato il ruolo DHCP su di esso, ma non gli ho ancora detto di iniziare a fare nulla.
Di cosa ha bisogno un server DHCP per iniziare a distribuire indirizzi IP? Deve sapere quali indirizzi IP, maschera di sottorete, gateway predefinito e indirizzi del server DNS si trovano all'interno della rete in modo da poterli impacchettare e iniziare a distribuire le informazioni ai computer che lo richiedono. Questo pacchetto di informazioni all'interno del server DHCP è chiamato ambito DHCP. Una volta definito il nostro ambito, il server DHCP inizierà a distribuire indirizzi IP da tale ambito ai nostri nuovi server e computer che non hanno già indirizzi statici definiti.

Ancora una volta, dobbiamo avviare uno strumento di gestione sul nostro Windows Server 2019 e, ancora una volta, il modo più semplice per avviarlo è utilizzare il menu Strumenti all'interno di Server Manager. Vai avanti e avvia la console DHCP. All'interno, vedrai il nome del tuo server su cui è in esecuzione il server DHCP. Espandilo e avrai opzioni sia per IPv4 che per IPv6.
Sì, questo significa che puoi utilizzare questo server DHCP per distribuire sia gli indirizzi IPv4 che gli indirizzi IPv6 per coloro che stanno testando IPv6 o hanno in programma di farlo in futuro. Per ora, ci atteniamo al buon vecchio IPv4, quindi posso fare clic con il pulsante destro del mouse su IPv4 e scegliere di creare un nuovo ambito. Verrà avviata una procedura guidata Nuovo ambito che guida l'utente attraverso le poche informazioni necessarie al server DHCP per creare un ambito pronto per iniziare a distribuire indirizzi IP all'interno della rete. Sto impostando il mio nuovo ambito per distribuire indirizzi IP dal 10.10.10.100 al 10.10.10.150:



Non appena si finisce di creare l'ambito, è immediatamente attivo e qualsiasi computer nella rete la cui scheda NIC è configurata per acquisire automaticamente un indirizzo da un server DHCP inizierà a farlo su questo nuovo server DHCP.

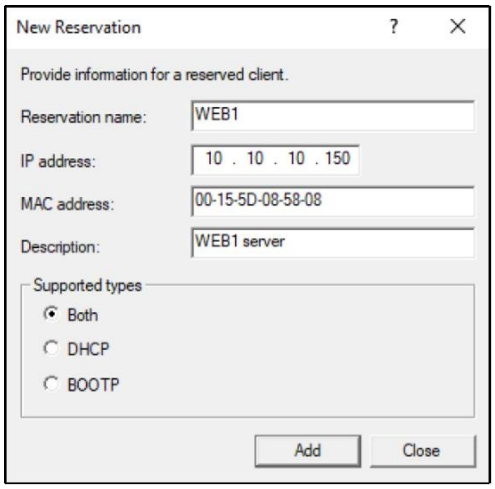
Ora che il nostro nuovo ambito è stato creato, è possibile espandere l'ambito all'interno della console DHCP e visualizzare alcune informazioni aggiuntive su questo ambito. Facendo clic sulla cartella Address Leases, è possibile vedere tutti gli indirizzi DHCP che sono stati forniti da questo server DHCP. Come puoi vedere nello screenshot seguente, ho un computer client Windows 10 sulla rete, che non ha un indirizzo statico, quindi ha acquisito un indirizzo DHCP dal mio server DHCP. È stato assegnato il primo indirizzo IP che ho definito nel mio ambito, 10.10.10.100. La prossima macchina che accede per prendere un indirizzo IP da questo server DHCP riceverà 10.10.10.101 e così via da lì:



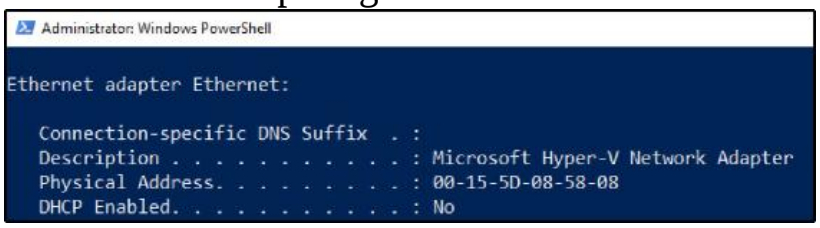
Prenotazioni DHCP

Assegnare indirizzi IP da un grande pool di quelli disponibili è ottimo, ma questi contratti di locazione di indirizzi sono soggetti a scadenza e modifica. Ciò significa che un computer che ha 10.10.10.100 oggi potrebbe ricevere 10.10.10.125 domani. In genere, questo va bene dal punto di vista del computer desktop, poiché generalmente non si preoccupano dell'indirizzo IP che hanno. I computer client di solito raggiungono l'esterno della rete, ma gli altri dispositivi raramente cercano di trovarli e contattarli. Cosa succede se hai un dispositivo più permanente nella tua rete, come un server Windows, ma non vuoi avere a che fare con l'indirizzamento statico di questo server? È qui che entrano in gioco le prenotazioni DHCP. Una prenotazione è l'atto di prendere un singolo indirizzo IP all'interno del tuo ambito DHCP e riservarlo a un particolare dispositivo. Questo dispositivo riceverà lo stesso indirizzo IP ogni volta che si connette tramite il server DHCP e questo particolare indirizzo IP non verrà distribuito a nessun altro dispositivo sulla rete. Utilizzando le prenotazioni all'interno di DHCP, è possibile consentire al server DHCP di gestire l'assegnazione di indirizzi IP anche ai server permanenti, in modo da non dover configurare manualmente le NIC di quei server, ma mantenere comunque indirizzi IP permanenti su quelle macchine.

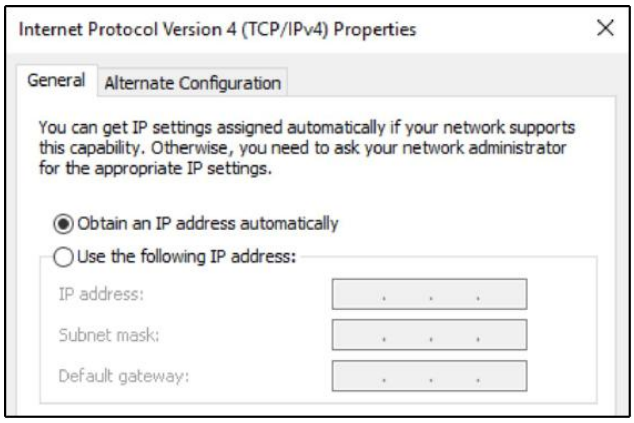
Puoi vedere la cartella chiamata Prenotazioni nella console DHCP. Al momento, non c'è nulla di elencato qui, ma facendo clic con il tasto destro su Prenotazioni e scegliendo Nuova prenotazione ... ne creeremo una per noi stessi. Lavoriamo ancora una volta con quel server web1. In questo momento, ho un indirizzo IP statico assegnato a web1, ma creerò invece una prenotazione sull'indirizzo IP 10.10.10.150:


New Reservation
?
Provide information for a reserved client.
Reservation name:
WEB1
IP address:
10 . 10 . 10 . 150
MAC address:
00-15-5D-08-58-08
Description:
WEB1 server
Supported types
Both
DHCP
BOOTP
Add
Close

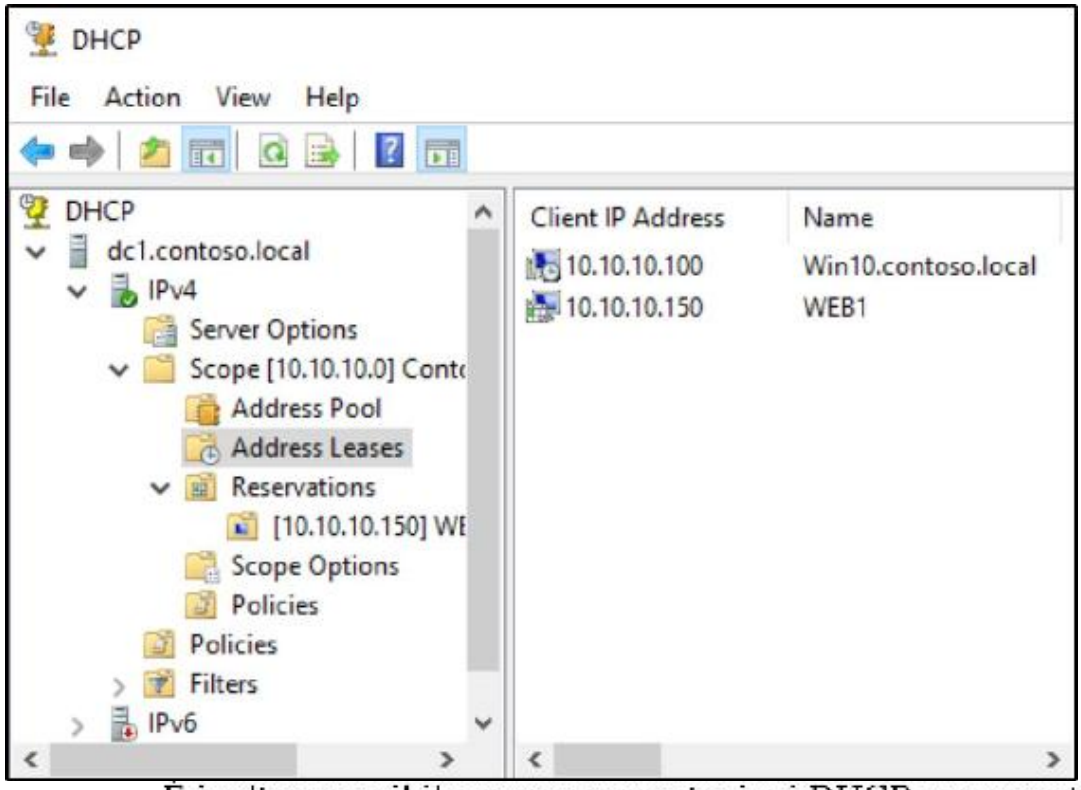
Whoa, whoa, whoa ... torna indietro con il treno. La maggior parte delle informazioni su questa schermata ha un senso - una rapida descrizione del nome del server e dell'indirizzo IP stesso - ma come sono arrivato a quell'indirizzo MAC? Un indirizzo MAC è l'indirizzo fisico di una scheda di rete sulla rete. Quando l'apparecchiatura di rete tenta di inviare informazioni a un determinato indirizzo IP o, in questo caso, quando il server DHCP deve consegnare un determinato indirizzo IP a una particolare NIC su un server, ha bisogno di un identificatore fisico per quella scheda di rete. Quindi, questo indirizzo MAC è qualcosa che è unico per la NIC sul mio server web1. Accedendo al mio server web1, posso eseguire ipconfig / all e vedere l'indirizzo MAC elencato per la mia scheda NIC proprio in quell'output, quella combinazione di lettere e numeri dall'aspetto sciocco mostrato come indirizzo fisico. È lì che ho ottenuto queste informazioni. Questo è il modo in cui DHCP decide quando richiamare le prenotazioni. Se un'interfaccia di rete richiede un indirizzo DHCP e l'indirizzo MAC di quel dispositivo è elencato qui nelle prenotazioni, il server DHCP restituirà l'indirizzo riservato al dispositivo, anziché uno dal pool generale:



Ora che la nostra prenotazione DHCP è stata creata, entrerò nelle impostazioni NIC sul mio server web1 e mi libererò di tutte le informazioni sull'indirizzamento IP statico scegliendo l'opzione Ottieni automaticamente un indirizzo IP:


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:

Dopofacendo ciò, web1 raggiungerà il server DHCP e chiederà un indirizzo, e puoi vedere che ora mi è stato assegnato l'indirizzo riservato del 10.10.10.150. Questo sarà sempre l'indirizzo IP del server web1 da questo punto in poi, a meno che non modifichi la mia prenotazione DHCP o in qualche modo modifichi l'indirizzo MAC di web1. Questo potrebbe accadere se dovessi installare una nuova NIC in web1:



È inoltre possibile creare prenotazioni DHCP per oggetti diversi dai dispositivi Windows nella rete. Poiché tutto ciò di cui hai bisogno è l'indirizzo MAC del dispositivo (e ogni dispositivo con un adattatore di rete ha un indirizzo MAC), è facile creare prenotazioni per dispositivi come server di stampa, fotocopiatrici, sistemi di allarme di sicurezza e altro ancora.

Backup e ripristino

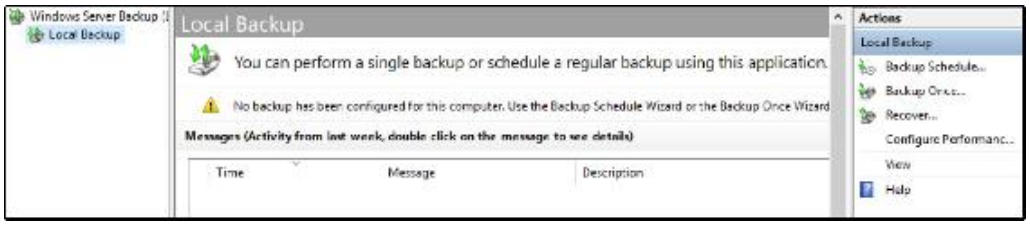
La necessità di eseguire il backup e occasionalmente di ripristinare i server è, purtroppo, ancora presente in Windows Server 2019. Sogno un giorno in cui i server siano affidabili e stabili al 100% per tutta la loro vita, non influenzati da virus e software canaglia, ma oggi non lo è quel giorno. Sebbene sul mercato siano disponibili molti strumenti di terze parti che possono migliorare e automatizzare la tua esperienza di backup durante la gestione di molti server, abbiamo queste funzionalità integrate direttamente nel nostro sistema operativo Server 2019 e dovremmo tutti avere familiarità con le modalità di utilizzo loro.

Pianifica backup regolari

L'accesso ai server e l'avvio di un'attività di backup manuale ogni giorno ovviamente non è fattibile per la maggior parte delle nostre organizzazioni, poiché il processo di esecuzione dei backup si trasformerebbe nel nostro lavoro a tempo pieno. Per fortuna, la funzionalità Windows Server Backup ci offre la possibilità di creare una pianificazione di backup. In questo modo, possiamo definire di cosa si desidera eseguire il backup, dove si desidera eseguire il backup e con quale frequenza deve essere eseguito questo backup. Quindi possiamo sederci, rilassarci e sapere che i nostri sistemi stanno eseguendo questo compito da soli.

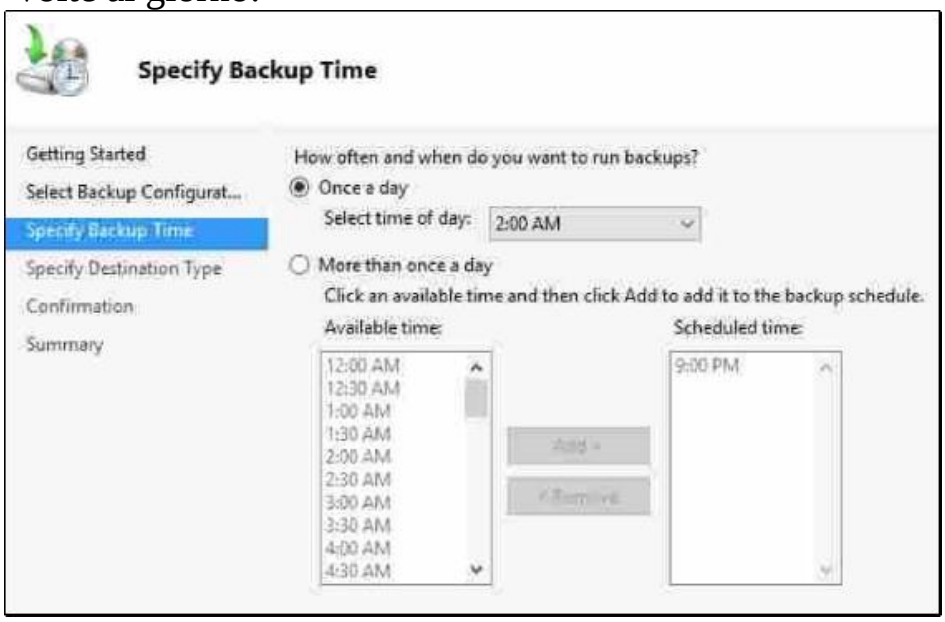
Prima di poter eseguire qualsiasi operazione con i backup, è necessario installare la funzionalità appropriata all'interno di Windows. Utilizzando il collegamento Aggiungi ruoli e funzionalità, andare avanti e installare la funzionalità denominata Windows Server Backup. Ricorda che ho detto funzionalità: non troverai Windows Server Backup nella schermata di selezione dei ruoli del server principale; è necessario andare avanti di una schermata nella procedura guidata per trovare le funzionalità. Al termine dell'installazione della funzionalità, è possibile avviare la console di Windows Server Backup disponibile nel menu Strumenti di Server Manager. Una volta dentro, fai clic su Backup locale nel riquadro della finestra a sinistra e vedrai apparire alcune azioni sul lato destro dello schermo.

Come puoi vedere, c'è un'opzione qui elencata chiamata Backup Once ... che, come suggerisce il nome, eseguirà un lavoro di backup ad hoc. Sebbene questa sia una caratteristica interessante, non è possibile che un amministratore di server acceda a tutti i propri server e lo faccia ogni giorno. Invece, facendo clic sull'azione Pianificazione backup ... verrà avviata una procedura guidata di configurazione per la creazione di un processo di backup pianificato e ricorrente:



La prima opzione che si incontra è decidere di cosa si desidera eseguire il backup. L'opzione predefinita è impostata per il server completo, che eseguirà un backup di tutto il sistema operativo. Se desideri personalizzare la quantità di dati di cui viene eseguito il backup, puoi scegliere l'opzione Personalizzata e procedere da lì. Dato che ho molto spazio su disco disponibile, mi atterrò al percorso consigliato per la creazione di backup completi del server.

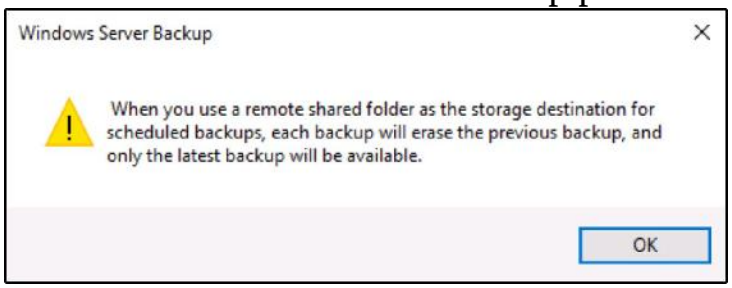
Successivamente, otteniamo il vero vantaggio dell'utilizzo del concetto di pianificazione: scegliere la frequenza di esecuzione del backup. Il modo più comune è scegliere una particolare ora del giorno e lasciare che il backup venga eseguito ogni giorno all'ora assegnata. Se hai un server i cui dati vengono aggiornati regolarmente nel corso dei giorni e desideri abbreviare la finestra di informazioni perse in caso di necessità di eseguire un ripristino, puoi anche specificare di eseguire il backup più volte al giorno:



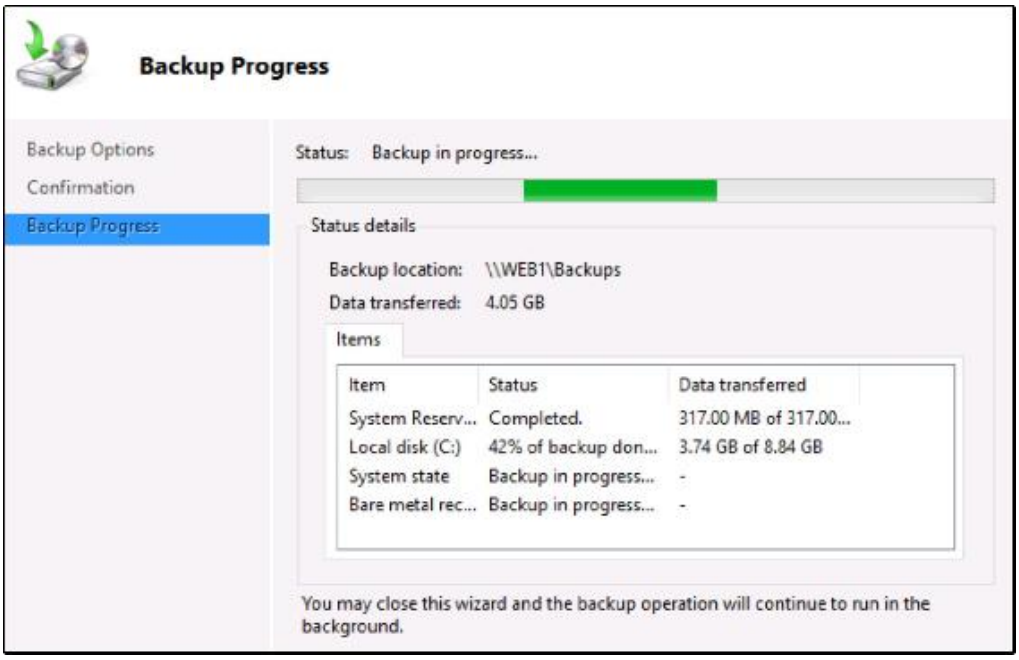
L'ultima schermata in cui dobbiamo prendere una decisione per i nostri backup pianificati è la schermata Specifica il tipo di destinazione, in cui determiniamo la posizione in cui verranno archiviati i nostri file di backup. Puoi vedere che ci sono un paio di diverse opzioni per archiviare il backup localmente sui dischi rigidi fisici dello stesso server in cui stai configurando i backup. La memorizzazione dei file di backup su un disco o volume locale, dedicato può essere vantaggiosa perché la velocità del processo di backup sarà aumentata. Per i server di cui si sta tentando di eseguire il backup nei giorni lavorativi per eseguire il backup continuo dei dati, è probabile che si desideri scegliere un'opzione di backup locale in modo che i backup vengano eseguiti rapidamente e senza intoppi. Un altro vantaggio dell'utilizzo di un disco connesso localmente per i backup è che puoi creare più punti di rollback all'interno del tuo schema di backup, mantenendo più giorni '

Tuttavia, trovo che la maggior parte degli amministratori preferisca mantenere tutti i propri file di backup in una posizione centralizzata e ciò significa scegliere la terza opzione in questa schermata, quella intitolata Backup in una cartella di rete condivisa. Scegliendo questa opzione, possiamo specificare un percorso di rete, come un file server o la mappatura di unità su un NAS, e possiamo impostare tutti i nostri diversi server per eseguire il backup in questa stessa posizione. In questo modo abbiamo una posizione centrale e standardizzata in cui sappiamo che tutti i nostri file di backup saranno archiviati nel caso in cui dovessimo estrarne uno e utilizzarlo per un ripristino.

Non posso dirti quale sia l'opzione migliore, perché dipende da come intendi utilizzare i backup nel tuo ambiente. La schermata in cui scegliamo il tipo di destinazione che vogliamo per i nostri backup include del buon testo da leggere in relazione a queste opzioni, come la nota importante che quando si utilizza una cartella di rete condivisa per i backup, è possibile archiviare un solo file di backup alla volta per il tuo server, perché il processo di creazione di un nuovo backup il giorno successivo sovrascriverà il backup precedente:



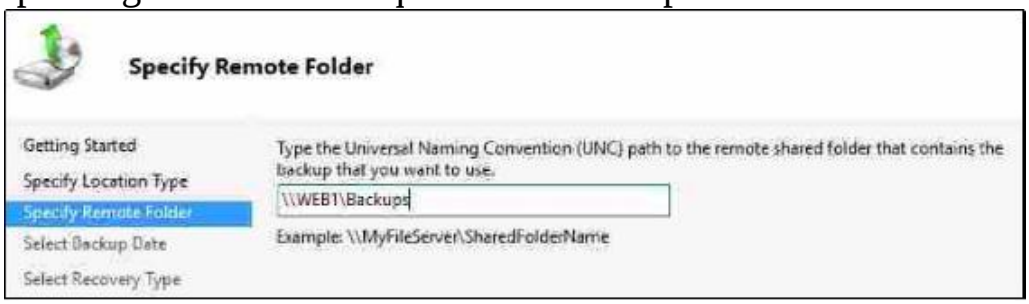
Dopo aver scelto una destinazione per i backup e specificato un percorso di condivisione di rete se questa è l'opzione scelta, la procedura guidata è terminata. I processi di backup verranno avviati automaticamente all'ora assegnata specificata durante la procedura guidata e domani vedrai un nuovo file di backup esistente per il tuo server. Se sei impaziente, come me e vuoi vedere il processo di backup in esecuzione in questo momento, puoi eseguire l'altra azione disponibile nella console di Windows Server Backup chiamata Backup Once ... per eseguire subito un backup manuale:



Ripristino da Windows

Dal momento che sei diligente e stai mantenendo buoni backup dei tuoi server, la speranza è che non dovrai mai utilizzare effettivamente quei file di backup per ripristinare un server. Ma, ahimè, verrà probabilmente il momento in cui avrai un server che va di traverso o alcuni dati vengono cancellati accidentalmente e dovrai rivisitare il processo di ripristino dei dati o di un intero server nella tua infrastruttura. Se il tuo server è ancora online e in esecuzione, il processo di ripristino è abbastanza facile da richiamare dalla stessa console di Windows Server Backup. Apri la console e scegli l'azione che dice Recupera ....

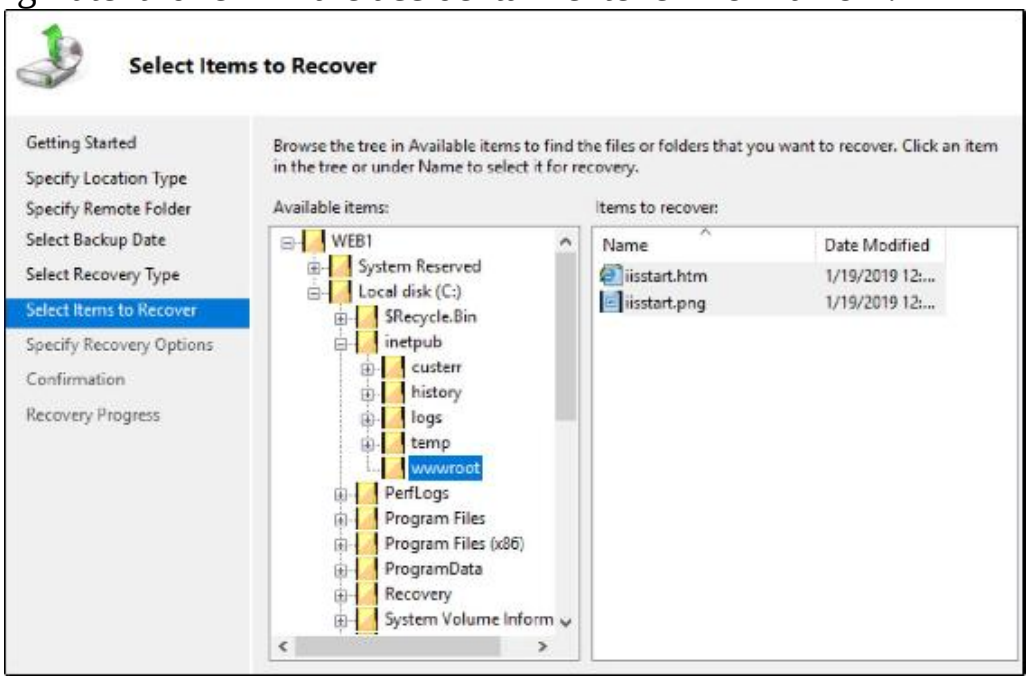
Questo richiama un'altra procedura guidata che ci guida attraverso il processo di ripristino. Innanzitutto, specifichiamo la posizione del nostro file di backup. Se si dispone di una posizione di backup dedicata sul server locale, è abbastanza semplice da trovare; altrimenti, come nel mio esempio, dove abbiamo specificato un percorso di rete, scegli Un backup archiviato in un'altra posizione, quindi scegli Cartella condivisa remota per dirgli dove trovare quel file di backup:



In base alla posizione di backup scelta, la procedura guidata identificherà ora tutte le date di rollback disponibili che sono disponibili nei file di backup. Se hai archiviato i tuoi file di backup su un disco locale in modo che siano disponibili punti di rollback per più giorni, vedrai numerose date disponibili su cui fare clic. Per me, dal momento che ho scelto di archiviare i miei backup in un percorso di rete, ciò significa che è disponibile solo un giorno di informazioni di backup e la data di ieri è l'unica che posso scegliere. Quindi sceglierò di ripristinare il backup di ieri e continuerò con la procedura guidata.

Ora che abbiamo identificato il file di backup specifico che verrà utilizzato per il ripristino, possiamo scegliere quali informazioni da quel backup verranno ripristinate. Questo è un bel pezzo della piattaforma di ripristino, perché, spesso, quando abbiamo bisogno di ripristinare dal backup, è solo per file e cartelle specifici che potrebbero essere stati eliminati o danneggiati. In tal caso, scegli l'opzione in alto, File e cartelle. In altri casi, potresti voler riportare l'intero server a una certa data e per quella funzionalità sceglieresti di ripristinare un intero volume. In questo momento, mi mancano solo alcuni file che in qualche modo sono scomparsi tra ieri e oggi, quindi sceglierò l'opzione File e cartelle predefinita.

Viene ora visualizzata la schermata Seleziona elementi da ripristinare, che esegue il polling del file di backup e mi visualizza l'intero elenco di file e cartelle all'interno del file di backup, quindi scelgo semplicemente quelli che voglio ripristinare. Questo tipo di ripristino può essere fondamentale per la gestione quotidiana di un file server, in cui il potenziale è alto per gli utenti di eliminare accidentalmente le informazioni:



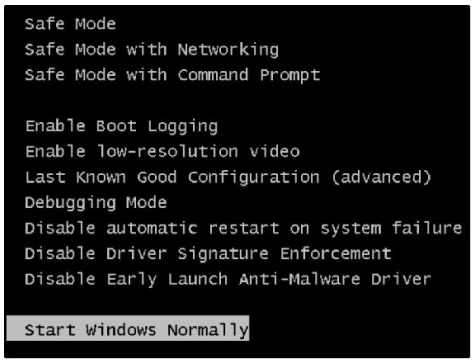
Non resta che specificare dove si desidera ripristinare i file recuperati. Puoi scegliere di riportare i file recuperati nella loro posizione originale oppure, se stai eseguendo questo processo di ripristino su una macchina diversa, puoi scegliere di ripristinare i file in una nuova posizione da cui puoi recuperarli e posizionarli manualmente ovunque abbiano bisogno di risiedere.

Ripristino dal disco di installazione

Il ripristino dalla console all'interno di Windows è una bella esperienza guidata dalla procedura guidata, ma cosa succede nel caso in cui il tuo server si sia bloccato? Se non riesci ad accedere a Windows sul tuo server, non puoi eseguire la console di Windows Server Backup per avviare il processo di ripristino. In questo caso, possiamo ancora utilizzare il nostro file di backup che è stato creato, ma dobbiamo usarlo in combinazione con un disco di installazione di Windows Server 2019, da cui possiamo richiamare il processo di ripristino.

È importante notare che questo processo di ripristino non può accedere alle posizioni sulla rete e il file di backup dovrà essere archiviato su un disco collegato al server. È possibile utilizzare un'unità USB a tale scopo durante il processo di ripristino, se non è stato originariamente impostato il processo di backup per l'archiviazione su un disco esistente collegato localmente.

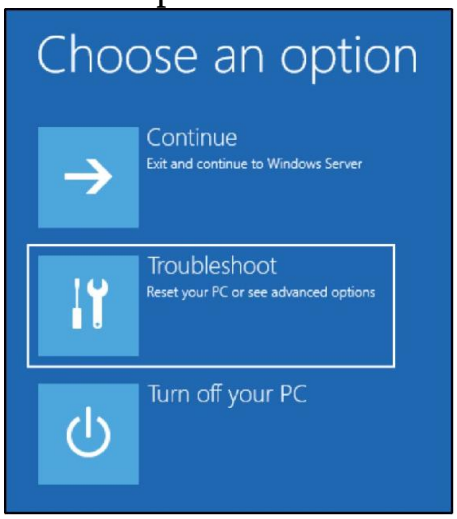
Per rendere le cose interessanti, manderò in crash il mio server. Questo è il server di cui abbiamo eseguito il backup pochi minuti fa. Ho cancellato accidentalmente alcuni file molto importanti nella mia directory C: \ Windows. Ops! Ora questo è tutto ciò che vedo quando provo ad avviare il mio server:



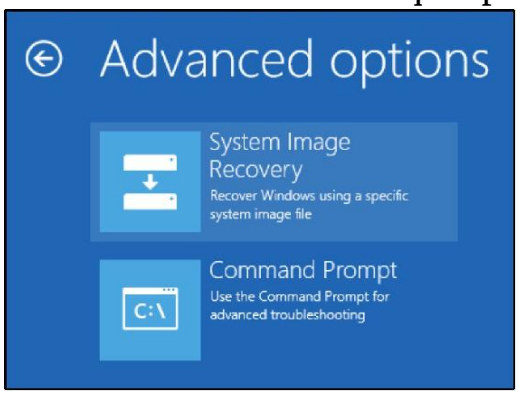
Non è uno schermo molto amichevole per vedere la prima cosa al mattino! Dal momento che mi sembra di essere bloccato qui e non riesco ad avviare Windows, le mie possibilità di eseguire la procedura guidata di ripristino sono nulle. Cosa fare? Avviare il DVD di installazione di Windows Server 2019? No, non voglio installare nuovamente Windows, poiché tutti i miei programmi e dati potrebbero essere sovrascritti in quello scenario.

Piuttosto, una volta entrato nelle schermate del programma di installazione, noterai che c'è un'opzione nell'angolo per riparare il tuo computer. Scegli questa opzione per aprire le opzioni di ripristino disponibili sul DVD di installazione.

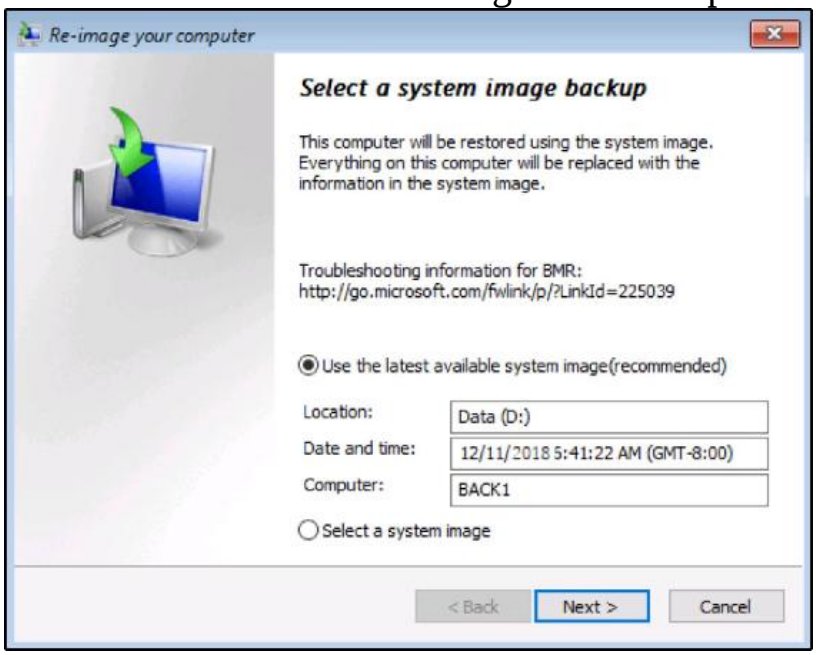
Ora vedi lo schermo adattarsi a una nuova tonalità blu, indicando che abbiamo inserito una parte speciale del disco di installazione. Se facciamo clic sul pulsante Risoluzione dei problemi, possiamo vedere tutte le opzioni che abbiamo a disposizione:



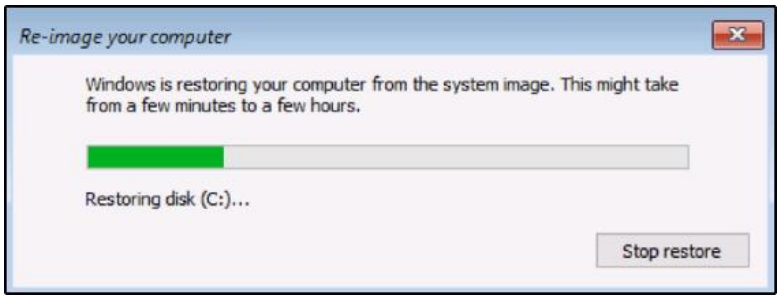
Se pensi di poter risolvere qualunque sia il problema dal prompt dei comandi, scegli quell'opzione e prova a risolverlo da solo. Per il nostro esempio, sono abbastanza sicuro di aver ospitato in modo significativo il sistema operativo, quindi eseguirò un ripristino completo dell'immagine di sistema e farò clic su quel pulsante:



Finché si dispone di un disco rigido collegato che contiene un file di backup di Windows Server, la procedura guidata si avvia e inserisce le informazioni sul backup. Poiché inizialmente avevo scelto di archiviare il mio file di backup in un percorso di rete, ho copiato i file di backup su un disco e l'ho collegato come secondo disco al mio server. La procedura guidata riconosce automaticamente il file di backup e lo visualizza nella schermata Seleziona un'immagine di backup del sistema:



Ora, facendo semplicemente clic su Avanti alcune volte per procedere con la procedura guidata, la mia immagine di backup viene ripristinata sul mio server:

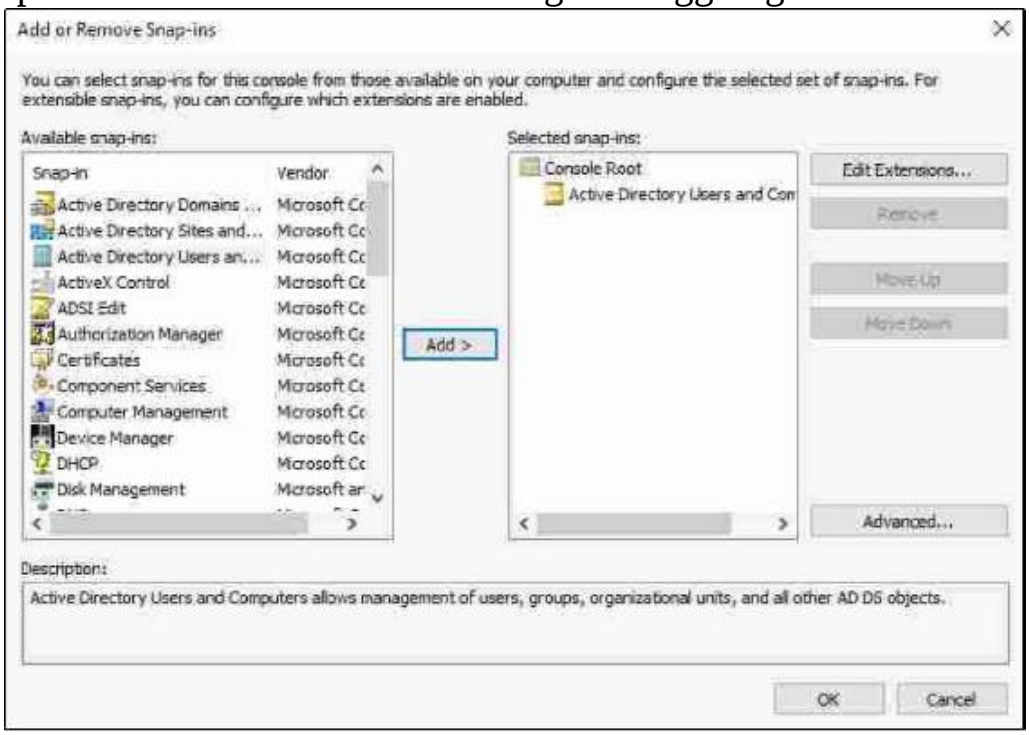


Una volta completato il processo di ripristino, il sistema si riavvia e si riavvia automaticamente in Windows, dove è completamente funzionante fino al punto di ripristino. Il mio server di prova non ha molto in esecuzione su di esso, quindi il tempo necessario per il ripristino è stato piuttosto minimo e una scatola di produzione potrebbe richiedere un po 'più di tempo, ma direi che 20 minuti dall'espansione del server all'essere completamente recuperato è un periodo di tempo davvero impressionante!

Mantenere file di backup buoni e recenti è fondamentale per la sostenibilità della tua attività. Ho lavorato su parecchi sistemi in cui gli amministratori hanno eseguito alcuni backup manuali dopo aver configurato inizialmente i loro server, ma non hanno mai impostato una pianificazione regolare. Anche se i dati sul server non cambiano mai, se fai parte di un dominio, non vorrai mai farlo. Nel caso in cui un server si guasti e sia necessario ripristinarlo, il ripristino di un backup vecchio di pochi giorni generalmente si ripristina bene. Ma se ripristini un'immagine che ha 6 mesi, Windows stesso tornerà online senza problemi e tutti i tuoi dati esisteranno, ma in quel lasso di tempo il tuo account del computer per quel server sarebbe sicuramente caduto fuori sincronizzazione con il dominio, causando errori di autenticazione nei confronti dei controller di dominio. In alcuni casi, potresti anche dover fare cose sciocche come scollegare e ricollegare il server al dominio dopo il ripristino dell'immagine per ripristinare le comunicazioni con il dominio. Se avessi mantenuto backup regolari da cui eseguire il ripristino, non avresti dovuto affrontare questi problemi.

Scorciatoie MMC e MSC

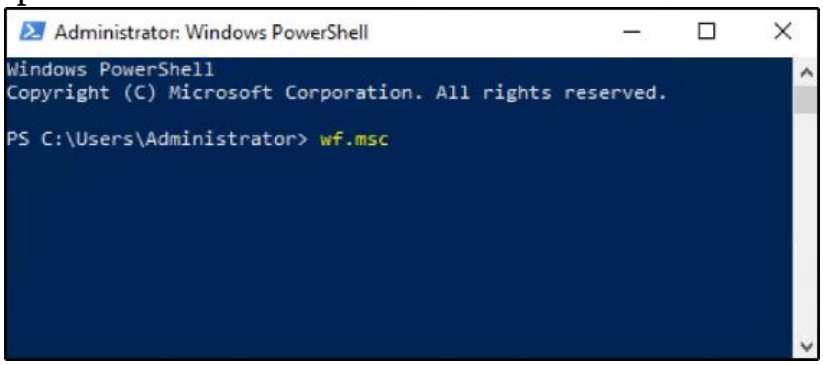
Probabilmente avrai notato che molte delle console di gestione che utilizziamo per configurare i componenti all'interno di Windows Server 2019 sono piuttosto simili. Quello che succede sotto il cofano con un certo numero di queste console è che stai effettivamente guardando una funzione snap-in, un insieme specifico di strumenti che vengono inseriti in uno strumento di console generico chiamato Microsoft Management Console, più comunemente denominato MMC. Infatti, piuttosto che aprire tutte queste funzioni di gestione dall'interno di Server Manager, per molte di esse, potresti semplicemente digitare MMC navigando su Start | Esegui o nel prompt dei comandi e richiama la console MMC generica. Da qui, puoi fare clic sul menu File e scegliere Aggiungi o Rimuovi snap-in:



Scegli lo snap-in di gestione in cui desideri lavorare e aggiungilo alla console. Ci sono un gran numero di funzioni di gestione a cui è possibile accedere tramite la console MMC standard, e anche alcune funzioni particolari in cui MMC è il metodo preferito, o forse l'unico, per interagire con alcuni componenti di Windows. Ad esempio, più avanti nel nostro libro esamineremo gli archivi di certificati all'interno di Windows Server 2019 e utilizzeremo MMC per alcune di queste interazioni.

Un altro modo interessante per aprire molte delle console di gestione è utilizzare il nome diretto dello strumento MSC. Un file MSC è semplicemente una configurazione salvata di una sessione della console MMC. Ci sono molte scorciatoie MSC memorizzate in Windows Server 2019 fuori dalla scatola. Se una determinata console di gestione offre la possibilità di essere avviata da un MSC, tutto ciò che devi fare è digitare il nome dell'MSC accedendo a Start | Esegui o nel prompt dei comandi o in una finestra di PowerShell e si avvierà immediatamente in quella particolare console di gestione senza bisogno di agganciare nulla e senza dover aprire alcun Server Manager. Poiché tendo a preferire l'uso di una tastiera al mouse, ho sempre una finestra di PowerShell o un prompt dei comandi aperti su ogni sistema con cui lavoro, e posso usare molto rapidamente quella finestra per aprire una qualsiasi delle mie console amministrative MSC. Facciamo un esempio, in modo che tu sappia esattamente come utilizzare questa funzionalità, quindi fornirò un elenco degli MSC comuni che trovo utili su base giornaliera.

Apri una finestra di PowerShell con privilegi elevati, digita WF.MSC e premi Invio:



Si aprirà la finestra Windows Defender Firewall con sicurezza avanzata, pronta ad accettare l'input da parte tua. Non abbiamo dovuto sfogliare il Pannello di controllo o aprire il normale Windows Firewall e quindi fare clic sul collegamento Impostazioni avanzate, che sono i modi comuni per accedere a questa console utilizzando un mouse. Conoscendo il nostro nome di scorciatoia MSC, siamo stati in grado di prendere una strada diretta per aprire la console WFAS completa, che è dove vado spesso per controllare particolari regole o stato del firewall:

Ora che hai visto come funziona un comando MSC, e di nuovo ci sono molti posti diversi in cui puoi digitare il nome di un MSC e invocarlo, voglio lasciarti con un elenco di console MSC comuni che puoi usare per accedi rapidamente a molte console amministrative sui tuoi server:

- DSA.MSC : Utenti e computer di Active Directory DSSITE.MSC : Siti e servizi di Active Directory DNSMGMT.MSC : DNS Manager
- GPEDIT.MSC : Editor Criteri di gruppo locali
- GPMC.MSC : Console di gestione dei criteri di gruppo CERTSRV.MSC : Gestione delle autorità di certificazione CERTTMPL.MSC : Gestione dei modelli di

certificato CERTLM.MSC : Archivio certificati computer locale

- CERTMGR.MSC : Archivio certificati utente corrente COMPMGMT.MSC : Gestione informatica DEVMGMT.MSC : Gestore dispositivi DHCPMGMT.MSC : Gestore DHCP
- DISKMGMT.MSC : Gestione disco EVENTVWR.MSC : Visualizzatore eventi PERFMON.MSC : Monitoraggio delle prestazioni SECPOL.MSC : Console dei criteri di sicurezza locale FSMGMT.MSC : Cartelle condivise
- WF.MSC: Windows Defender Firewall con sicurezza avanzata

Sommario

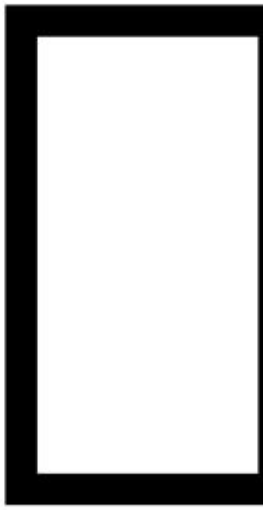
In questo capitolo, abbiamo discusso alcuni dei ruoli e dei componenti all'interno di Windows Server 2019 che dovrai utilizzare e con cui avrai familiarità, se vuoi eseguire un'infrastruttura realmente incentrata su Microsoft. Active Directory, DNS e DHCP sono i servizi principali principali che sono alla base e supportano l'intera infrastruttura. Una conoscenza di base di queste tecnologie è essenziale per qualsiasi amministratore di Windows Server e una conoscenza approfondita del modo in cui questi strumenti lavorano insieme ti aprirà molte porte man mano che avanzi nella tua carriera IT. Quasi tutti gli altri ruoli e funzionalità disponibili in Windows Server sono supportati o dipendono da questi servizi principali. Spero che tu ti senta a tuo agio nel navigare al loro interno dopo aver seguito gli esempi in questo capitolo.

Ora continuiamo il nostro viaggio attraverso Windows Server 2019 con il capitolo successivo mentre ci immergiamo in uno degli argomenti più spaventosi, comunque per molti amministratori, i certificati! Nel prossimo capitolo esamineremo i certificati in Windows Server 2019.

Domande

1. All'interno di Active Directory, un contenitore (cartella) che contiene computer e account utente è chiamato ...?
2. Qual è il termine per creare un account computer all'interno di Active Directory prima che il computer venga aggiunto al tuo dominio?
3. Quale strumento di gestione viene utilizzato per specificare che determinate posizioni fisiche nella rete sono associate a particolari sottoreti IP?

4. Qual è il nome di un controller di dominio speciale che non può accettare nuove informazioni, ma solo sincronizzarsi da un controller di dominio esistente?
5. Quale oggetto Criteri di gruppo contiene le impostazioni di complessità della password in una nuova installazione di Criteri di gruppo?
6. Che tipo di record DNS risolve un nome in un indirizzo IPv6?
7. Qual è il collegamento MSC per l'apertura di utenti e computer di Active Directory?



Certificati in Windows Server 2019

"Uffa, dobbiamo usare i certificati per far funzionare questo."

- Citazione di un amministratore anonimo che ha appena scoperto il loro ultimo acquisto di tecnologia richiede l'uso di certificati nella propria organizzazione

Se questo suona familiare, non scartare ancora quel nuovo progetto! Per qualche ragione, l'uso dei certificati sembra un compito arduo per molti di noi, anche per coloro che lavorano nel settore IT da molti anni. Penso che ciò sia probabilmente dovuto al fatto che ci sono molte diverse opzioni disponibili su un server dei certificati, ma non c'è molto buon senso o facilità d'uso incorporata nella console di gestione per la gestione dei

certificati. Ciò, combinato con una generale mancanza di requisiti per i certificati sui server per così tanti anni, significa che, anche se questa tecnologia esiste da molto tempo, molti amministratori di server non hanno avuto l'opportunità di scavare e distribuire i certificati da soli. Distribuisco regolarmente un paio di tecnologie che richiedono un ampio uso di certificati in un'organizzazione, spesso ho bisogno di trasmetterli a ogni workstation o utente nella rete, e sento questo tipo di preoccupazioni tutto il tempo. Il rilascio di un certificato a un singolo server Web critico per l'azienda sembra abbastanza scoraggiante se non si ha alcuna esperienza con il processo, per non parlare del rilascio di centinaia o migliaia di certificati contemporaneamente. Un altro scenario comune è quello in cui un'azienda ha determinato che i certificati fossero nel proprio interesse ma non disponeva delle risorse del personale per difendersi da sé, quindi ha assunto una terza parte per implementare i certificati all'interno della rete.
Mentre questo fa funzionare i certificati, spesso lascia una lacuna di conoscenza che non viene mai colmata, quindi potresti avere un server dei certificati attivo e funzionante, ma non sentirti affatto a tuo agio nel modificarlo o utilizzarlo.

Il termine generico per un ambiente certificato è noto come infrastruttura a chiave pubblica (PKI). Lo chiamo specificamente perché probabilmente vedrai PKI elencato nella documentazione o nei requisiti ad un certo punto, se non l'hai già fatto. La vostra PKI è fornita dai server nella vostra rete e la configurazione di quei server per emettere certificati per voi è lo scopo di questo capitolo. I server che decidi di essere i tuoi server di certificazione sono noti come server di autorità di certificazione (CA) e li chiameremo server CA in questo libro.

Per farti lavorare con i certificati nella tua rete, ecco gli argomenti che tratteremo in questo capitolo:

- Tipi di certificati comuni
  Pianificazione dell'infrastruttura PKI
- Creazione di un nuovo modello di certificato Emissione dei nuovi certificati Creazione di un criterio di registrazione automatica
- Ottenere un certificato SSL di un'autorità pubblica Esportazione e importazione di certificati

Tipi di certificati comuni

Esistono diversi tipi di certificati che potresti dover pubblicare. Come vedrai, quando hai bisogno di un certificato che ha un elenco di requisiti particolari, puoi creare un modello di certificato secondo le specifiche che preferisci. Quindi, in un certo senso, non esistono affatto tipi di certificato, ma solo modelli di certificato che si ambiscono a contenere tutte le informazioni necessarie affinché quel certificato possa svolgere il proprio lavoro. Sebbene questo sia vero tecnicamente, è generalmente più facile segmentare i certificati in gruppi diversi, rendendoli più distinguibili per il lavoro particolare che si intendono eseguire.

Certificati utente

Come suggerisce il nome, un certificato utente viene utilizzato per scopi specifici per il nome utente stesso. Una delle piattaforme che sta guidando una maggiore adozione dei certificati è il processo di autenticazione di rete. Le aziende che stanno cercando un'autenticazione più forte nei loro ambienti spesso guardano ai certificati come parte di quel processo di autenticazione. Le smart card sono uno dei meccanismi specifici che possono essere utilizzati per questo scopo, in particolare, una sorta di scheda fisica da collegare a un computer in modo che l'utente possa accedere a quel computer.

Le smart card possono anche essere archiviate virtualmente, in un posto speciale sulle macchine più recenti chiamato TPM. Ma questa è una discussione per un giorno diverso. Il motivo per cui citiamo le smart card qui è perché, spesso la funzionalità principale dell'autenticazione della smart card è fornita da un certificato utente che è stato memorizzato su quella smart card. Se ti trovi nel bel mezzo di un progetto per distribuire smart card, probabilmente ti ritroverai ad aver bisogno di una PKI.

Un altro popolare modulo di autenticazione forte è la password monouso (OTP). Ciò richiede all'utente di inserire un PIN generato in modo casuale oltre ai normali criteri di accesso e, in alcuni casi, quando l'utente inserisce il PIN, gli viene rilasciato un certificato utente temporaneo da utilizzare come parte della catena di autenticazione. Ulteriori luoghi in cui si trovano comunemente i certificati utente includono quando le aziende utilizzano tecnologie di crittografia dei file, come EFS (abbreviazione di Encrypting File System), o quando si creano sistemi di rete privata virtuale (VPN) per consentire agli utenti remoti di ricollegare i loro laptop al rete aziendale.
Molte aziende non vogliono fare affidamento esclusivamente su un nome utente e una password per l'autenticazione VPN, quindi l'emissione di certificati utente e la richiesta che siano presenti per costruire quel tunnel VPN è comune.

Certificati di computer

Spesso indicati come certificati di computer o certificati di macchine, questi ragazzi vengono rilasciati ai computer per aiutare con l'interazione tra la rete e l'account del computer stesso. Le tecnologie, come SCCM, che interagiscono e gestiscono i sistemi informatici indipendentemente dagli utenti che hanno effettuato l'accesso a tali computer, fanno uso di certificati di computer. Questi tipi di certificati vengono utilizzati anche per l'elaborazione della crittografia tra i sistemi sulla rete, ad esempio, se si è interessati a utilizzare IPsec per crittografare le comunicazioni tra i client e un file server altamente protetto. Il rilascio di certificati di computer o macchine agli endpoint all'interno di questa catena di

comunicazione sarebbe essenziale per far funzionare correttamente. Spesso mi ritrovo a rilasciare certificati di computer ai computer di un'azienda per autenticare i tunnel DirectAccess, un'altra forma di accesso remoto automatizzato. Ci sono molti diversi motivi e tecnologie a cui potresti essere interessato, che richiederebbero l'emissione di certificati alle workstation client nel tuo ambiente.

Certificati SSL

Se ti trovi nel mezzo della strada del certificato, dove non hai davvero gestito un server CA ma a un certo punto hai emesso e installato una sorta di certificato, è probabile che il certificato con cui hai lavorato fosse un certificato SSL. Questo è di gran lunga il tipo di certificato più comune utilizzato nell'odierna infrastruttura tecnologica e la tua azienda è più che probabile che utilizzi certificati SSL, anche se non ne sei a conoscenza e non hai un singolo server CA in esecuzione all'interno della tua rete.

I certificati SSL sono più comunemente usati per proteggere il traffico del sito web. Ogni volta che visiti un sito web e vedi HTTPS nella barra degli indirizzi, il tuo browser utilizza un flusso di pacchetti SSL per inviare informazioni avanti e indietro tra il tuo computer e il server web con cui stai parlando. Il server web ha un certificato SSL e il tuo browser ha controllato quel certificato prima di consentirti di accedere alla pagina web, per assicurarti che il certificato sia valido e che il sito web sia davvero quello che dice di essere. Vedi, se non usassimo i certificati SSL sui siti web, chiunque potrebbe impersonare il nostro sito e avere accesso alle informazioni che vengono trasmesse al sito web.

Forniamo un rapido esempio. Supponiamo che uno dei tuoi utenti si trovi in un bar, utilizzando il Wi-Fi pubblico. Un utente malintenzionato ha individuato un modo per manipolare il DNS su quella rete Wi-Fi, quindi quando l'utente tenta di visitare mail.contoso.com per accedere a Outlook Web Access della propria azienda per controllare la posta elettronica, l'hacker ha dirottato il traffico e l'utente è ora seduto su un sito Web che assomiglia al portale aziendale, ma in realtà è un sito Web ospitato dall'aggressore. L'utente digita il nome utente e la password e l'attaccante bingo ora ha le credenziali di quell'utente e può utilizzarle per accedere alla tua rete reale. Cosa impedisce che ciò accada ogni giorno nel mondo reale? Certificati SSL. Quando imponi che i tuoi siti web rivolti all'esterno, come quella pagina di accesso all'email, siano siti HTTPS, richiede che i browser client controllino il certificato SSL presentato con il sito web. Quel certificato SSL contiene informazioni che solo tu come azienda possiedi, non può essere impersonato. In questo modo, quando il

tuo utente accede alla tua pagina di login reale, il browser controlla il certificato SSL, lo trova corretto e continua semplicemente per il suo modo felice. L'utente non sa nemmeno di essere protetto, ad eccezione del piccolo lucchetto vicino alla barra degli indirizzi del browser. D'altra parte, se il loro traffico viene intercettato e reindirizzato a un sito Web fasullo, il controllo del certificato SSL fallirà (perché l'aggressore non avrebbe un certificato SSL valido per il nome del sito Web della tua azienda) e l'utente verrà fermato nel proprio tracce, almeno per leggere una pagina di avviso del certificato prima di poter procedere. A questo punto,

I certificati SSL utilizzati dai siti Web su Internet sono quasi sempre forniti, non dal server CA interno, ma da un'autorità di certificazione pubblica. Probabilmente hai sentito parlare di molti di loro, come Verisign, Entrust, DigiCert e GoDaddy. Le aziende generalmente acquistano certificati SSL da queste autorità pubbliche perché tali autorità sono considerate attendibili per impostazione predefinita sui nuovi computer che gli utenti potrebbero acquistare sul campo. Quando si acquista un nuovo computer, anche direttamente da un negozio al dettaglio, se si dovesse aprire il negozio locale di certificati che esiste fuori dagli schemi su quel sistema, si troverà un elenco di autorità radice attendibili. Quando visiti un sito web protetto da un certificato SSL emesso da una di queste autorità pubbliche, quel certificato, e quindi il sito web, viene automaticamente considerato attendibile da questo computer.

Quando un'azienda acquisisce un certificato SSL da una di queste autorità pubbliche, c'è un processo di verifica approfondito che l'autorità intraprende per assicurarsi che la persona che richiede il certificato (tu) sia davvero qualcuno con la società appropriata e autorizzata per emettere questi certificati. Questa è la base della sicurezza nell'utilizzo dei certificati SSL di una CA pubblica. Tutti i nuovi computer sanno per impostazione predefinita di considerare attendibili i certificati emessi da queste autorità e non è necessario intraprendere alcuna azione speciale per far funzionare i siti Web su Internet. D'altra parte, è possibile emettere certificati SSL da un server CA che hai costruito tu stesso e che hai in esecuzione all'interno della tua rete, ma richiede un paio di cose che lo rendono difficile, perché il tuo server CA ovviamente non è considerato affidabile da tutti i computer ovunque, né dovrebbe essere. In primo luogo, se si desidera emettere il proprio certificato SSL da utilizzare su un sito Web pubblico, è necessario esternalizzare su Internet almeno una parte della PKI interna, nota come CRL (Certificate Revocation List). Ogni volta che prendi un componente interno alla tua rete e lo pubblicizzi su Internet, stai introducendo un rischio per la sicurezza, quindi a meno che non sia assolutamente necessario farlo, in genere non è raccomandato. Il secondo motivo per cui è difficile utilizzare i propri certificati SSL su siti Web pubblici è che solo i computer aggiunti al dominio della propria

azienda sapranno come fidarsi di questo certificato SSL. Quindi, se un utente porta a casa il proprio laptop aziendale e lo utilizza per accedere alla propria pagina di accesso e-mail, probabilmente funzionerà bene. Ma se un utente tenta di accedere alla stessa pagina di accesso e-mail dal proprio computer di casa, che non fa parte del tuo dominio o della tua rete, riceveranno un messaggio di avviso del certificato e dovranno adottare misure speciali per ottenere l'accesso al sito web. Che dolore per gli utenti. Non dovresti mai incoraggiare gli utenti ad accettare il rischio e procedere attraverso un messaggio di avviso del certificato: questa è una ricetta per il disastro, anche se il certificato su cui stanno facendo clic è uno emesso dalla tua CA. È una questione di principio non accettare mai questo rischio.

Questi problemi possono essere alleviati acquistando un certificato SSL da una di quelle autorità di certificazione pubbliche, quindi l'acquisto di questi tipi di certificati è il modo normale e consigliato per utilizzare SSL sui siti Web pubblicamente accessibili. I siti web che sono completamente all'interno della rete sono una storia diversa, poiché non si trovano ad affrontare Internet e la loro impronta di sicurezza è molto più piccola. È possibile utilizzare il server CA interno per emettere certificati SSL ai siti Web interni e non è necessario sostenere i costi associati all'acquisto di certificati per tutti questi siti Web.

Esistono diversi livelli di certificati SSL che è possibile acquistare da una CA pubblica, le cui informazioni sono elencate sui siti Web dell'autorità. In sostanza, l'idea è che più paghi, più è sicuro il tuo certificato. Questi livelli sono correlati al modo in cui l'autorità convalida rispetto al richiedente del certificato, poiché è proprio qui che entra in gioco la sicurezza con i certificati SSL. L'autorità garantisce che quando si accede alla pagina protetta dal loro certificato, il certificato è stato rilasciato alla società reale che possiede quella pagina web.

Oltre al livello di convalida, che puoi scegliere quando acquisti un certificato, c'è anche un'altra opzione su cui devi decidere, e questa è molto più importante per l'aspetto tecnico del modo in cui funzionano i certificati. Quando si acquista un certificato sono disponibili diverse convenzioni di denominazione e non esiste una risposta migliore per quale scegliere. Ogni situazione che richiede un certificato sarà unica e dovrà essere valutata individualmente per decidere quale schema di denominazione funziona meglio. Copriamo rapidamente tre possibilità per una convenzione di denominazione del certificato SSL.

Certificati con un solo nome

Questo è il percorso più economico e più comune da intraprendere quando si acquista un certificato per un singolo sito web. Un certificato con un solo nome protegge e contiene informazioni su un singolo nome DNS. Quando si configura un nuovo sito Web su portal.contoso.com e si desidera che questo sito Web protegga parte del traffico utilizzando

HTTPS, è necessario installare un certificato SSL sul sito Web. Quando si invia la richiesta all'autorità di certificazione per questo nuovo certificato, si immette il nome specifico di portal.contoso.com nel campo Nome comune del modulo di richiesta. Questo singolo nome DNS è l'unico nome che può essere protetto e convalidato da questo certificato.

Certificati del nome alternativo del soggetto

Nome alternativo del soggetto I certificati (SAN) generalmente costano un po 'di più dei certificati con nome singolo, perché hanno più capacità. Quando richiedi un certificato SAN, hai la possibilità di definire più nomi DNS che il certificato può proteggere. Una volta emesso, il certificato SAN conterrà un nome DNS primario, che tipicamente è il nome principale del sito web, e, all'interno delle proprietà del certificato, troverai elencati i nomi DNS aggiuntivi che hai specificato durante la tua richiesta. Questo singolo certificato può essere installato su un server Web e utilizzato per convalidare il traffico per uno qualsiasi dei nomi DNS contenuti nel certificato. Un esempio di caso d'uso di un certificato SAN è quando si configura un server Lync (Skype for Business). Lync utilizza molti nomi DNS diversi, ma tutti i nomi che si trovano nello stesso dominio DNS. Questa è una nota importante per quanto riguarda i certificati SAN: i tuoi nomi devono far parte dello stesso dominio o sottodominio. Di seguito è riportato un elenco di esempio dei nomi che potremmo includere in un singolo certificato SAN ai fini di Lync:

- Lync.contoso.com (quello principale)
- Lyncdiscover.contoso.com
- Meet.contoso.com
- Dialin.contoso.com
- Admin.contoso.com

Questi diversi siti Web / servizi utilizzati da Lync vengono quindi implementati su uno o più server ed è possibile utilizzare lo stesso certificato SAN su tutti questi server per convalidare il traffico diretto verso uno di quei nomi DNS.

Certificati con caratteri jolly

Ultimo ma certamente non meno importante è il certificato jolly. Questo è il modello di lusso, quello che ha il maggior numero di funzionalità, offre

la massima flessibilità e allo stesso tempo offre il percorso più semplice per l'implementazione su molti server. Il nome su un certificato con caratteri jolly inizia con una stella (*). Questa stella significa che qualsiasi, come in qualsiasi cosa che precede il nome di dominio DNS, è coperto da questo certificato. Se sei il proprietario di contoso.com e prevedi di gestire molti record DNS pubblici che passeranno a molti siti Web e server Web diversi, potresti acquistare un singolo certificato con caratteri jolly con il nome * .contoso.com e potrebbe coprire tutto il tuo certificato esigenze.

In genere, i caratteri jolly possono essere installati su tutti i server Web di cui hai bisogno, senza alcun limite al numero di diversi nomi DNS che può convalidare. Ho riscontrato un'eccezione una volta, quando l'accordo di un particolare cliente con la propria autorità di certificazione specificava che dovevano segnalare e pagare per ogni istanza del loro certificato jolly che era in uso. Quindi fai attenzione a quegli accordi quando li fai con la tua CA. La maggior parte delle volte, un carattere jolly è pensato per essere gratuito per tutti all'interno dell'azienda in modo da poter distribuire molti siti e servizi su molti server e utilizzare il certificato con caratteri jolly ovunque.

Lo svantaggio di un certificato con caratteri jolly è che costa di più, molto di più. Ma se hai bisogno di certificati di grandi dimensioni o grandi progetti di crescita, renderà la tua amministrazione dei certificati molto più semplice, veloce ed economica a lungo termine.

Pianificazione della PKI

Dal momento che tutta la nostra discussione in questo libro ruota attorno a Windows Server 2019, ciò significa che il tuo server CA può e deve essere uno fornito da questo ultimo e migliore dei sistemi operativi. Come con la maggior parte delle funzionalità in Server 2019, la creazione di un server autorità di certificazione nella rete è semplice come installare un ruolo Windows. Quando si aggiunge il ruolo a un nuovo server, è il primo ruolo nell'elenco di Servizi certificati Active Directory (AD CS). Durante l'installazione di questo ruolo, ti verranno presentate un paio di opzioni importanti e devi comprenderne il significato prima di creare un solido ambiente PKI.

Il nome host del server e lo stato del dominio non possono essere modificati dopo aver implementato il ruolo CA Assicurati di aver impostato il nome host finale e di aver aggiunto questo server al dominio (se applicabile), prima di installare il ruolo di Servizi certificati Active Directory. Non

Servizi di ruolo

La prima decisione che devi prendere quando installi il ruolo di Servizi certificati Active Directory è quali servizi di ruolo desideri installare, come puoi vedere nello screenshot seguente:

Fare clic su ciascuna opzione ti darà una descrizione delle sue capacità, quindi puoi probabilmente determinare quali parti del ruolo ti servono sfogliando questa schermata. Ecco anche un breve riassunto di queste opzioni. Nota che li sto elencando fuori ordine, a causa del modo in cui li vedo normalmente configurati nel campo:

- **Autorità di certificazione**: Questo è il motore di certificazione principale che deve essere installato affinché questo server diventi ufficialmente una CA.
- **Registrazione Web dell'autorità di certificazione**: Spesso viene installato anche questo, soprattutto in ambienti sufficientemente piccoli da poter eseguire un singolo server CA per l'intero ambiente. La parte di registrazione Web installerà le funzionalità IIS (server Web) su questo server e avvierà un piccolo sito Web utilizzato per la richiesta di certificati. Ne discuteremo ulteriormente quando esamineremo l'emissione di certificati da questa interfaccia web, più avanti nel capitolo.
- **Servizio Web di registrazione dei certificati e Servizio Web dei criteri di registrazione dei certificati**: La maggior parte delle volte, ci occupiamo solo di emettere certificati ai nostri sistemi di proprietà dell'azienda, collegati a un dominio. In questi casi, queste due selezioni non sono necessarie. Se si prevede di emettere certificati a computer non appartenenti a un dominio da questo server CA, si desidera selezionare queste opzioni.

- **Servizio di registrazione dei dispositivi di rete**: Come suggerisce il nome, questa parte del ruolo CA fornisce la capacità di emettere certificati a router e altri tipi di dispositivi di rete.
- **Risponditore in linea**: Questa è una funzione speciale riservata agli ambienti più grandi. All'interno di ogni certificato è presente una specifica per un elenco di revoche di certificati (CRL). Quando un computer client utilizza un certificato, raggiunge e controlla questo CRL per assicurarsi che il suo certificato non sia stato revocato. Il CRL è un pezzo importante del puzzle di sicurezza del certificato; in un ambiente con migliaia di client, il CRL potrebbe essere molto, molto impegnato a rispondere a tutte queste richieste. È possibile distribuire server CA aggiuntivi che eseguono Risponditore in linea per facilitare il carico.

Ai fini del nostro laboratorio e per coprire le capacità richieste dalla maggior parte delle piccole e medie imprese là fuori, selezionerò le due opzioni mostrate in precedenza
screenshot: Autorità di certificazione e registrazione Web dell'autorità di certificazione.

Enterprise contro Standalone

Dopo l'installazione del ruolo di Servizi certificati Active Directory, Server Manager notificherà che i servizi di certificazione richiedono una configurazione aggiuntiva, come è comune con molte installazioni di ruoli. Quando configuri il tuo ruolo CA per la prima volta, ti verrà presentata una vasta scelta. Desideri che questo server CA sia una CA aziendale o una CA autonoma?

Cominciamo con la CA aziendale. Come ti dirà la procedura guidata, un server CA aziendale deve essere un membro del tuo dominio e questi server di certificazione in genere rimangono in linea in modo che possano emettere certificati ai computer e agli utenti che ne hanno bisogno. Apetta un minuto! Perché nel mondo dovremmo voler disattivare comunque un server dei certificati? Ne parleremo tra un minuto, ma se intendi utilizzare

questa CA per emettere certificati, deve ovviamente rimanere attiva. La maggior parte dei server CA all'interno di un ambiente di dominio saranno CA aziendali. Quando si crea una CA aziendale, i modelli e alcune informazioni specifiche del certificato sono in grado di archiviarsi all'interno di Active Directory, il che rende l'integrazione tra i certificati e il dominio più stretta e vantaggiosa. Se questa è la tua prima interazione con il ruolo CA,

Come puoi correttamente dedurre dal testo precedente, ciò significa che una CA autonoma è meno comune da vedere in natura. Gli utenti autonomi possono essere membri del dominio oppure possono rimanere fuori da quella parte della rete e risiedere in un gruppo di lavoro locale. Se avessi un requisito di sicurezza che imponeva che il tuo server dei certificati non potesse essere aggiunto a un dominio, questo potrebbe essere un motivo per cui dovresti utilizzare una CA autonoma. Un altro motivo potrebbe essere dovuto al fatto che Active Directory semplicemente non esiste nell'ambiente scelto. Ai miei occhi, sarebbe estremamente raro trovare una rete in cui qualcuno stesse cercando di utilizzare Windows Server 2019 come autorità di certificazione e allo stesso tempo non stesse eseguendo Active Directory Domain Services, ma sono sicuro che da qualche parte c'è un caso d'angolo che sta facendo esattamente questo. In tal caso, dovresti anche scegliere standalone. Un terzo esempio in cui sceglieresti standalone è l'evento a cui abbiamo già accennato, in cui potresti avere un motivo per spegnere il tuo server. Quando si esegue questo scenario, viene in genere indicato come avere una radice offline. Non abbiamo ancora parlato di CA radice, ma lo faremo tra un minuto. Quando si esegue una root offline, si crea il livello superiore della gerarchia PKI come CA root autonoma, quindi si creano CA subordinate al di sotto di essa. Le tue CA subordinate sono quelle che svolgono il lavoro più impegnativo emettendo certificati, il che significa che la radice può essere chiusa in sicurezza poiché non ha compiti in corso. Perché dovresti farlo? Bene, la maggior parte delle aziende non lo fa, ma ho lavorato con alcune che hanno politiche di sicurezza di livello molto alto, ed è per questo che potresti visitare questo argomento. Se tutta una società ' s I server CA sono collegati insieme come CA aziendali e tutte le loro informazioni vengono archiviate all'interno di Active Directory, una compromissione di una delle CA emittenti subordinate potrebbe significare un disastro per l'intera PKI. È possibile che l'unico modo per porre rimedio a un attacco sia eliminare l'intero ambiente PKI, tutti i server CA e ricostruirli. Se dovessi farlo, significherebbe non solo ricostruire i tuoi server, ma anche riemettere copie nuove di zecca di tutti i tuoi certificati a ogni utente e dispositivo che li possiede.

D'altra parte, se avessi eseguito una CA radice autonoma che era offline, non sarebbe stata interessata dall'attacco. In questo caso, potresti abbattere i server dei certificati interessati, ma il tuo server principale principale sarebbe stato nascosto in modo sicuro. Potresti quindi riportare questa radice online, ricostruire nuovi subordinati da essa e avere un percorso più semplice per essere operativi al 100% perché le tue chiavi radice archiviate all'interno della CA non dovrebbero essere riemesse, come non lo sarebbero mai state. compromesso nell'attacco.

Come ho detto, non lo vedo molto spesso sul campo, ma è una possibilità. Se sei interessato a saperne di più sulle CA root offline e sul loro utilizzo, ti consiglio vivamente di consultare l'articolo di TechNet all'indirizzo http://social.technet.microsoft.com/wiki/contents/articles/2900.offline-root-certification-authority-ca.aspx. Se stai pensando di andare avanti con una CA root offline solo perché sembra più sicura, ma non hai un motivo specifico per farlo, ti consiglio di cambiare marcia e andare avanti con una CA root aziendale online. Sebbene ci siano alcuni vantaggi di sicurezza per la radice offline, la maggior parte delle aziende non ritiene che questi vantaggi valgano il fastidio aggiuntivo che accompagna l'utilizzo di una CA radice offline. Ci sono sicuramente dei compromessi sull'usabilità quando si va in quella direzione.

Nella maggior parte dei casi, ti consigliamo di selezionare Enterprise CA e procedere da lì.

Root vs Subordinato (emissione)

Questa è la seconda grande scelta che devi fare quando costruisci una nuova CA. Il tuo nuovo server sarà una CA radice o una CA subordinata? In alcuni casi, anche in molta documentazione Microsoft, una CA subordinata è più spesso chiamata CA emittente. In genere, in una PKI multilivello, le CA subordinate / emittenti sono quelle che effettuano l'emissione di certificati agli utenti e ai dispositivi nella rete.

La differenza è solo una questione di come vuoi che sia la tua gerarchia CA. In un albero PKI, c'è un unico certificato di alto livello, autofirmato a se stesso dalla CA radice, a cui tutto concatena. Una CA subordinata, d'altra parte, è quella che risiede sotto una CA radice nell'albero e le è stato emesso un proprio certificato dalla radice sopra di essa.

Se si prevede di eseguire solo un singolo server CA, deve essere una radice. Se stai creando un approccio a più livelli per l'emissione di certificati, la prima CA nel tuo ambiente deve essere una radice e puoi far scorrere i subordinati al di sotto di essa. È consentito avere più radici, e quindi più alberi, all'interno di una rete. Quindi la tua particolare PKI

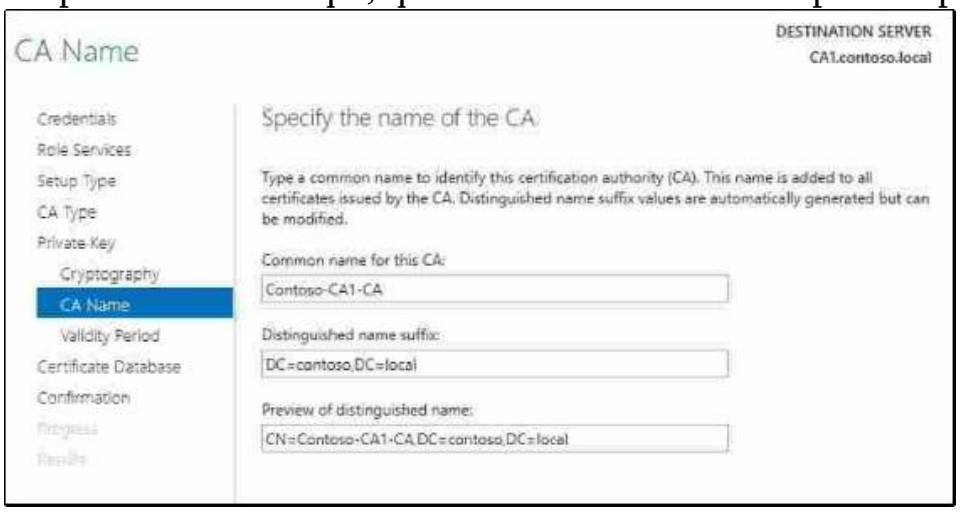
può essere strutturata come meglio credi. Nelle aziende più piccole, è molto comune vedere un solo server CA, una radice aziendale. Per motivi di semplicità nell'amministrazione, questi clienti sono disposti a correre il rischio che, se succede qualcosa a quel server, non sarà un grosso problema crearne uno nuovo e riemettere i certificati.

Per reti più grandi, è più comune vedere una singola radice con un paio di subordinati sotto di essa. In genere, in questo caso, il root è responsabile solo di essere il top dog e le CA subordinate sono quelle che fanno il vero lavoro, ovvero l'emissione di certificati ai client.

Assegnare un nome al server CA.

A questo punto, ora che hai installato il ruolo, il nome host del server stesso è scolpito nella pietra. Lo sapevi già. Ma mentre avanzi nelle procedure guidate per configurare la tua CA per la prima volta, ti imbatterai in una schermata chiamata Specifica il nome della CA. Eh? Pensavo lo avessimo già fatto quando abbiamo impostato il nome host?

No, abbiamo il nostro nome host finale e il nome del server è collegato ad Active Directory quando il mio server viene aggiunto al dominio, ma il "Nome CA" effettivo è qualcos'altro. Questo è il nome che verrà identificato all'interno delle proprietà di ogni certificato emesso da questa CA. Questo è anche un nome che verrà configurato in vari punti all'interno di Active Directory, poiché sto creando una CA aziendale. La procedura guidata identifica automaticamente un possibile nome da utilizzare, che molti amministratori prendono e utilizzano semplicemente. Se vuoi configurare il tuo nome, è qui che dovresti farlo. Una volta impostato il nome qui, questo è il nome della CA per sempre:



Posso installare il ruolo CA su un controller di dominio?

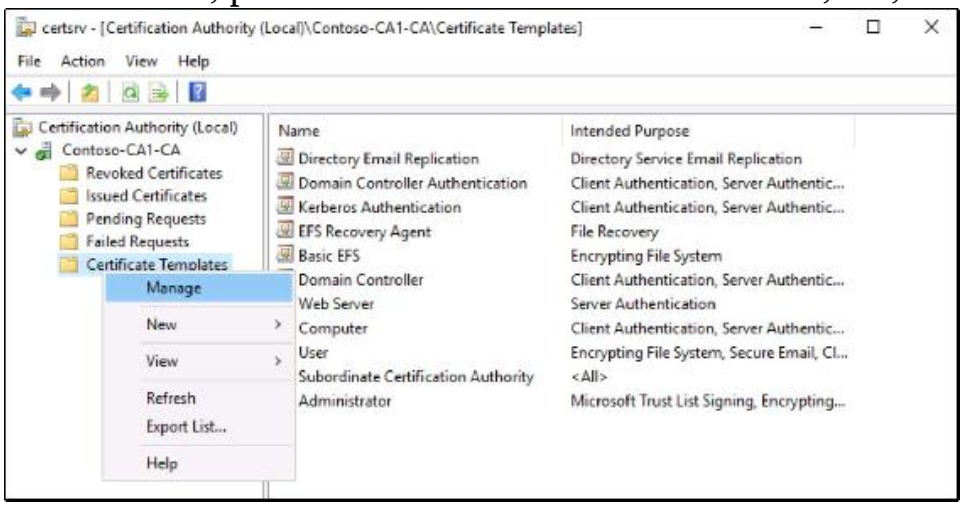
Poiché il ruolo è ufficialmente chiamato ruolo Servizi certificati Active Directory, significa che dovrei installare questo ruolo su uno dei miei server controller di dominio? No!
Sfortunatamente, ho incontrato molte piccole e medie imprese che hanno fatto esattamente questo e fortunatamente non hanno troppi problemi. Quindi tecnicamente funziona. Tuttavia, non è un percorso di installazione consigliato da Microsoft e dovresti creare le tue CA sui propri server; cerca di non ospitarli insieme ad altri ruoli quando possibile.

Creazione di un nuovo modello di certificato

Basta parlare, è ora di portare a termine un po 'di lavoro. Ora che il nostro ruolo CA è stato installato, facciamogli fare qualcosa! Lo scopo di un server dei certificati è emettere certificati, giusto? Quindi, lo faremo? Non così in fretta. Quando si emette un certificato da un server CA a un dispositivo o utente, non si sceglie quale certificato si desidera distribuire; piuttosto si sta scegliendo quale modello di certificato si desidera utilizzare per distribuire un certificato basato sulle impostazioni configurate all'interno di quel modello. I modelli di certificato sono una sorta di ricette per cucinare. Sul server CA, si creano i modelli e si includono tutti gli ingredienti o le impostazioni particolari che si desidera incorporare nel certificato finale. Quindi, quando gli utenti o i computer vengono a richiedere un certificato dal server CA, stanno in qualche modo creando un certificato nel loro sistema dicendo alla CA quale modello di ricetta seguire durante la creazione di quel certificato.
Certificati relativi al cibo?
Forse è una forzatura, ma si sta facendo piuttosto tardi la notte e questa è la prima cosa che mi è venuta in mente.

Quando esegui i passaggi per configurare il tuo primo server CA, viene fornito con alcuni modelli di certificato predefiniti direttamente nella console. In effetti, uno di quei modelli, chiamato Computer, è tipicamente preconfigurato al punto in cui, se un computer client dovesse raggiungere e richiedere un certificato computer dalla tua nuova CA, sarebbe in grado di emetterne uno con successo. Tuttavia, dov'è il divertimento nell'usare modelli e certificati predefiniti? Preferisco costruire il mio modello in modo da poter specificare le configurazioni e le impostazioni particolari all'interno di quel modello. In questo modo, so esattamente quali impostazioni sono contenute nei miei certificati che verranno infine rilasciati ai miei computer nella rete.

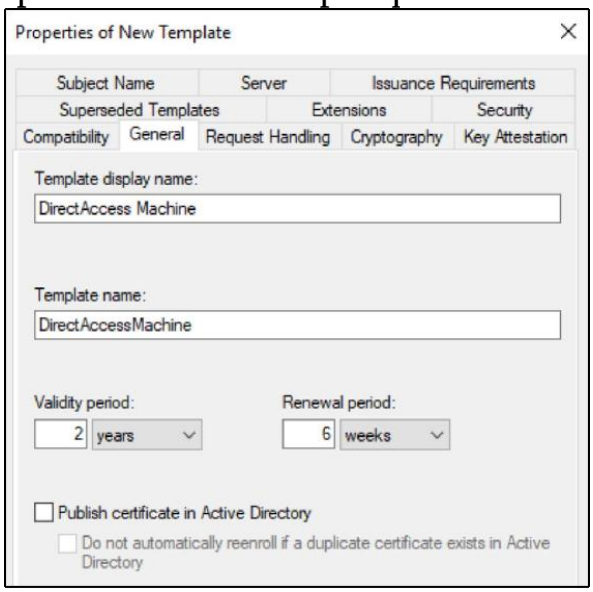
Ancora una volta, dobbiamo avviare la console di amministrazione appropriata per svolgere il nostro lavoro. All'interno del menu Strumenti di Server Manager, fare clic su Autorità di certificazione. Una volta dentro, puoi espandere il nome della tua autorità di certificazione e vedere alcune cartelle, inclusa una in basso chiamata Modelli di certificato. Se fai clic su questa cartella, vedrai un elenco dei modelli attualmente incorporati nel nostro server CA. Dal momento che non vogliamo utilizzare uno di questi modelli preesistenti, è logico che proviamo a fare clic con il pulsante destro del mouse qui e creare un nuovo modello, ma questo non è in realtà il posto corretto per creare un nuovo modello. Il motivo per cui i nuovi modelli di certificato non vengono creati direttamente da questa schermata deve essere superiore al mio grado di retribuzione, perché sembra sciocco che non lo sia, ma,



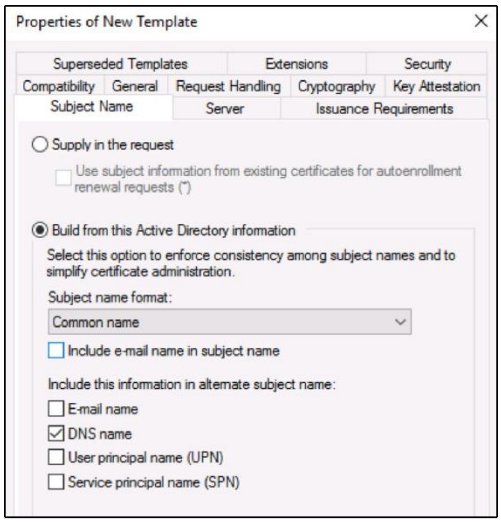
Ora viene visualizzato un elenco molto più completo di modelli, inclusi alcuni di essi che non è stato possibile visualizzare nella prima schermata. Per creare un nuovo modello, quello che vogliamo fare è trovare un modello preesistente che funzioni in modo simile allo scopo che vogliamo che il nostro nuovo modello di certificato serva. I modelli di computer stanno diventando comunemente rilasciati in molte organizzazioni a causa del numero sempre maggiore di tecnologie che richiedono l'esistenza di questi certificati, tuttavia, come abbiamo detto, non vogliamo utilizzare quel modello integrato, che si chiama semplicemente Computer, perché vogliamo il nostro modello per avere un nome più specifico e forse vogliamo che il periodo di validità del

certificato sia più lungo delle impostazioni predefinite. Fare clic con il pulsante destro del mouse sul modello Computer integrato e fare clic su Duplica modello. Si apre la schermata Proprietà per il nostro nuovo modello,

In un capitolo successivo, discuteremo di DirectAccess, la tecnologia di accesso remoto che verrà utilizzata nel nostro ambiente. Una buona implementazione di DirectAccess include i certificati del computer che vengono rilasciati a tutte le workstation client mobili, quindi pianificheremo di utilizzare questo nuovo modello per tali scopi. La scheda Generale è anche il luogo in cui possiamo definire il nostro periodo di validità per questo certificato, che imposteremo a 2 anni:

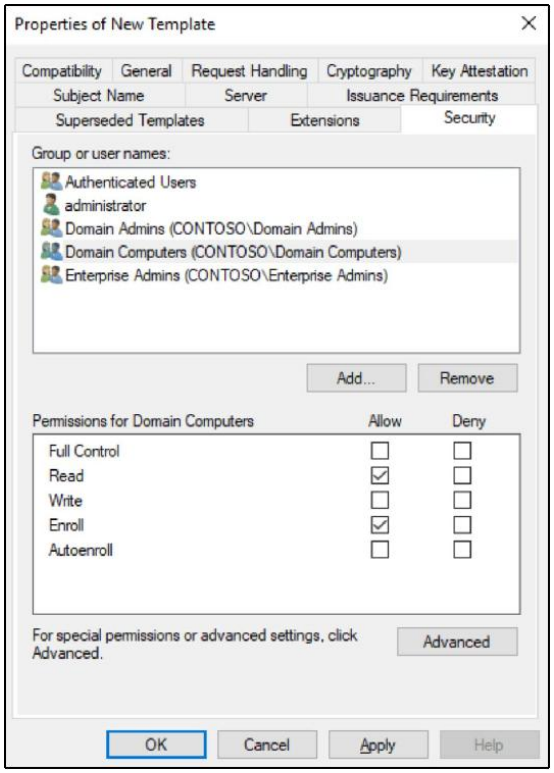


Se i certificati che si desidera emettere richiedono ulteriori modifiche alle impostazioni, è possibile scorrere le schede disponibili all'interno delle proprietà e apportare le modifiche necessarie. Per il nostro esempio, un'altra impostazione che cambierò è all'interno della scheda Nome soggetto. Desidero che i miei nuovi certificati abbiano un nome soggetto che corrisponda al nome comune del computer in cui vengono emessi, quindi ho scelto Nome comune dall'elenco a discesa:



Abbiamo un'altra scheda da visitare e questa è qualcosa che dovresti controllare su ogni modello di certificato che crei: la scheda Sicurezza. Vogliamo controllare qui per assicurarci che le autorizzazioni di sicurezza per questo modello siano impostate in modo da consentire il rilascio del certificato agli utenti o ai computer desiderati, e allo stesso tempo assicurarci che le impostazioni di sicurezza del modello non lo siano troppo sciolto, creando una situazione in cui qualcuno che non ne ha bisogno potrebbe essere in grado di ottenere un certificato. Per il nostro esempio, ho intenzione di emettere questi certificati DirectAccess a tutti i computer nel dominio, perché il tipo di certificato del computer che ho creato potrebbe essere utilizzato anche per le autenticazioni IPsec generali, che un giorno potrei configurare.

Quindi, mi sto solo assicurando che i computer del dominio siano elencati nella scheda Sicurezza e che siano impostati per le autorizzazioni di lettura e registrazione, in modo che qualsiasi computer che fa parte del mio dominio avrà la possibilità di richiedere un nuovo certificato in base a il mio nuovo modello:



Poiché questo è tutto ciò di cui ho bisogno nel mio nuovo certificato, faccio semplicemente clic su OK e il mio nuovo modello di certificato è ora incluso nell'elenco dei modelli sul mio server CA.

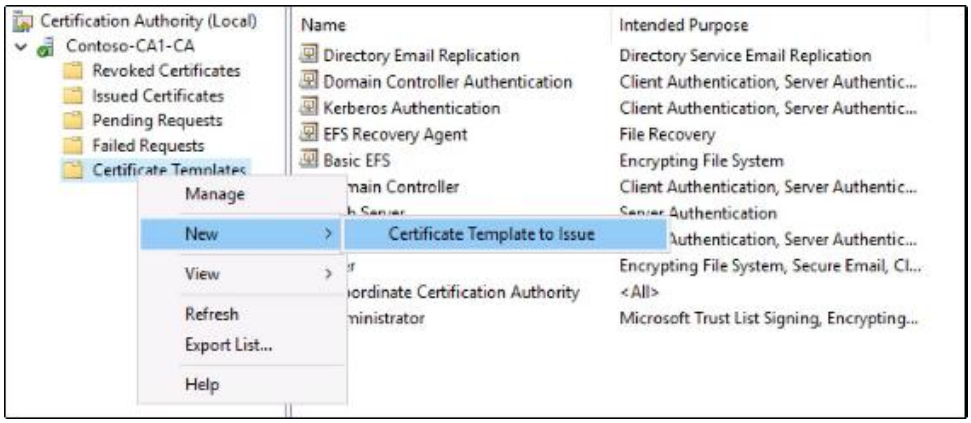
Emissione dei nuovi certificati

Segue la parte che fa inciampare molte persone al primo tentativo. Ora hai un modello nuovo di zecca da emettere e abbiamo verificato che le autorizzazioni all'interno di quel modello di certificato siano configurate in modo appropriato in modo che qualsiasi computer che è un membro del nostro dominio possa richiedere uno di questi certificati, giusto? Quindi il nostro passaggio logico successivo sarebbe saltare su un computer client e richiedere un certificato, ma prima è necessario eseguire un'altra attività per renderlo possibile.

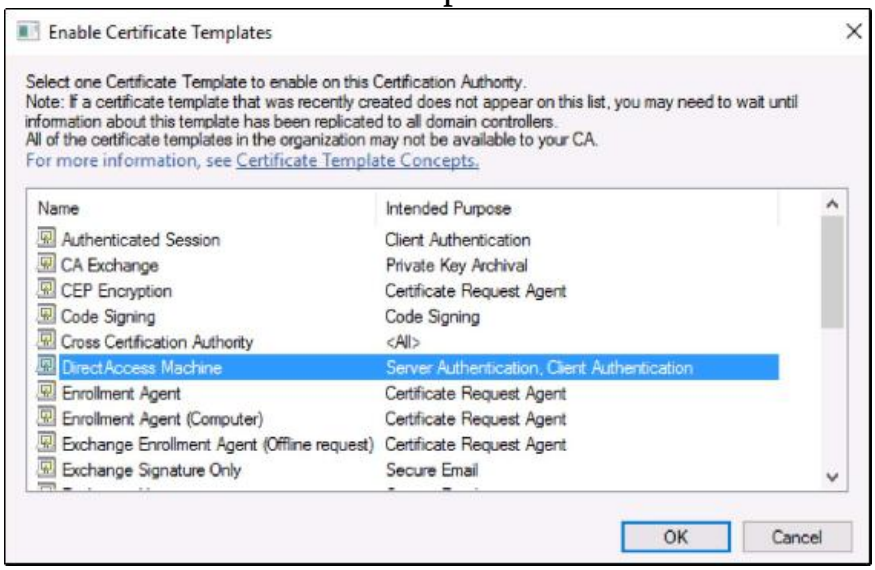
Anche se il nuovo modello è stato creato, non è stato ancora pubblicato. Quindi, al momento, il server CA non offrirà il nostro nuovo modello come opzione ai client, anche se le autorizzazioni di sicurezza sono configurate per farlo. Il processo per pubblicare un modello di certificato è molto veloce, solo un paio di clic del mouse, ma a meno che tu non sappia della necessità di farlo, può essere un'esperienza molto frustrante perché nulla nell'interfaccia ti dà un suggerimento su questo requisito.

Pubblicazione del modello

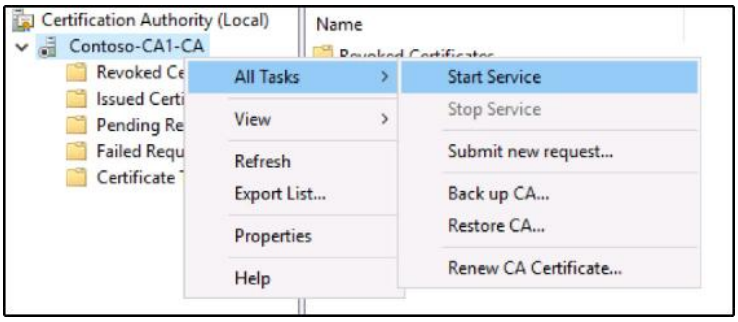
Se la tua Console dei modelli di certificato è ancora aperta (quella in cui stavamo gestendo i nostri modelli), chiudila in modo da tornare alla console di gestione dell'autorità di certificazione principale. Ricordi come abbiamo notato che l'elenco dei modelli di certificato disponibili che viene visualizzato qui è molto più breve? Questo perché solo questi modelli di certificato sono attualmente pubblicati e disponibili per essere emessi. Per aggiungere ulteriori modelli all'elenco pubblicato, incluso il nostro nuovo, è sufficiente fare clic con il pulsante destro del mouse sulla cartella Modelli di certificato e quindi passare a Nuovo | Modello di certificato da emettere:


Certification Authority (Local)
Contoso-CA1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Manage
New
Certificate Template to Issue
View
Refresh
Export List...
Help
Name
Intended Purpose
Directory Email Replication
Directory Service Email Replication
Domain Controller Authentication
Client Authentication, Server Authentic...
Kerberos Authentication
Client Authentication, Server Authentic...
EFS Recovery Agent
File Recovery
Basic EFS
Encrypting File System
Client Authentication, Server Authentic...
Encrypting File System, Secure Email, Cl...
<All>
Microsoft Trust List Signing, Encrypting...

Ora ci viene presentato un elenco dei modelli disponibili che non sono ancora stati rilasciati. Tutto quello che devi fare è scegliere il tuo nuovo modello dall'elenco e fare clic su OK. Il nuovo modello è ora incluso nell'elenco dei modelli di certificato pubblicati e siamo pronti per richiederne uno da un computer client:

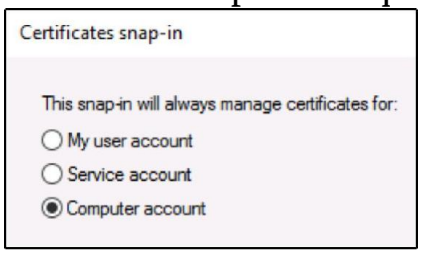


Se esamini questo elenco e non vedi il modello appena creato, potresti dover fare un passaggio aggiuntivo. A volte la semplice attesa risolverà questo comportamento, perché a volte il motivo per cui il nuovo modello non viene visualizzato nell'elenco è perché si attende che i controller di dominio finiscano la replica. Altre volte, scoprirai che, anche dopo aver atteso un po ', il tuo nuovo modello non è ancora in questo elenco. In tal caso, probabilmente è sufficiente riavviare il servizio dell'autorità di certificazione per forzarlo a inserire le nuove informazioni sul modello. Per riavviare il servizio CA, fai clic con il pulsante destro del mouse sul nome della CA nella parte superiore della console di gestione dell'autorità di certificazione e vai a Tutte le attività | Interrompi servizio. L'interruzione di quel servizio richiede in genere solo uno o due secondi, | Avvia servizio. Ora prova a pubblicare di nuovo il tuo nuovo modello e dovresti vederlo nell'elenco:



Richiesta di un certificato da MMC

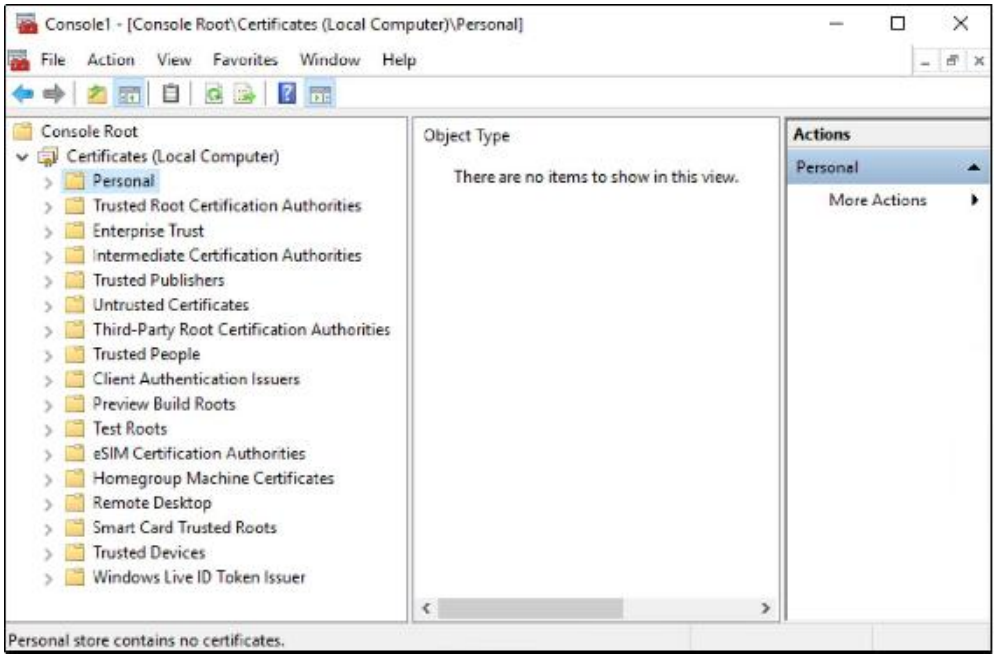
Il nostro nuovo modello di certificato è stato creato e lo abbiamo pubblicato con successo nella console CA, rendendolo così ufficialmente pronto per l'emissione. È ora di provarlo. Vai avanti e accedi a un normale computer client sulla tua rete per farlo. Esistono un paio di modi standard per richiedere un nuovo certificato su un computer client. Il primo è usare la buona vecchia console MMC. Sul tuo computer client, avvia MMC e aggiungi il file
snap-in per i certificati. Quando scegli Certificati dall'elenco degli snap-in disponibili e fai clic sul pulsante Aggiungi, ti vengono presentate alcune opzioni aggiuntive per l'archivio certificati che desideri aprire. Puoi scegliere tra l'apertura di certificati per l'account utente, l'account di servizio o l'account computer. Poiché stiamo tentando di emettere un certificato che verrà utilizzato dal computer stesso, desidero scegliere Account computer da questo elenco e fare clic su Fine:



Nella pagina successiva, fare nuovamente clic sul pulsante Fine per scegliere l'opzione predefinita, ovvero Computer locale. Ciò si aggancerà nell'archivio certificati basato su computer della macchina locale all'interno di MMC.

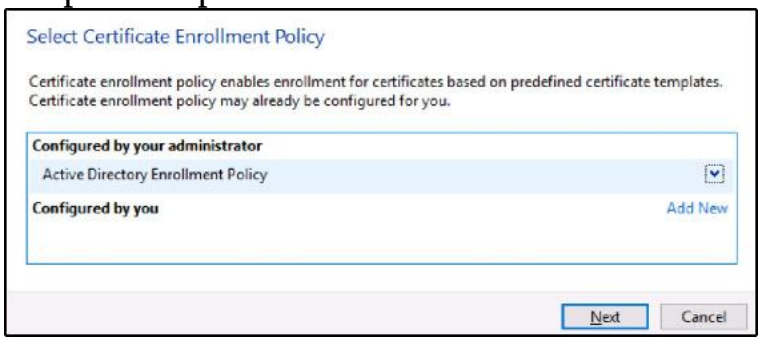
Sui sistemi operativi più recenti, come Windows 8 e 10 e con Windows Server 2012, 2012R2, 2016 e 2019, è disponibile un collegamento MSC per l'apertura direttamente nell'archivio certificati del computer locale. Basta digitareCERTLM.MSC in un prompt Esegui e MMC avvierà automaticamente e crea questo snap-in per te.

Quando si installano certificati su un computer o un server, questo è generalmente il luogo che si desidera visitare. All'interno di questo archivio certificati, la posizione specifica in cui vogliamo installare il nostro certificato è la cartella Personale. Questo è vero sia che stiate installando un certificato macchina come stiamo facendo qui, sia che stiate installando un certificato SSL su un server web. La cartella dei certificati personali del computer locale è la posizione corretta per entrambi i tipi di certificati. Se fai clic su Personale, puoi vedere che al momento non abbiamo nulla elencato lì:

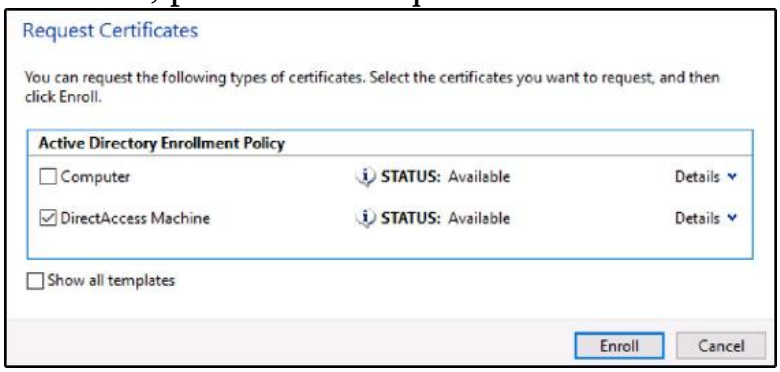


Per richiedere un nuovo certificato dal nostro server CA, è sufficiente fare clic con il pulsante destro del mouse su Personale
cartella, quindi vai a Tutte le attività | Richiedi nuovo**Certificato.** In questo modo si apre una procedura guidata; andare avanti e fare clic una volta sul pulsante Avanti.

Ora hai una schermata che sembra che qualcosa debba essere fatto, ma nella maggior parte dei casi poiché stiamo richiedendo un certificato su una delle nostre macchine aziendali collegate a un dominio, in realtà non abbiamo bisogno di fare nulla sulla schermata presentata di seguito immagine dello schermo. Basta fare clic su Avanti e la procedura guidata interrogherà Active Directory per mostrare tutti i modelli di certificato disponibili per essere emessi:

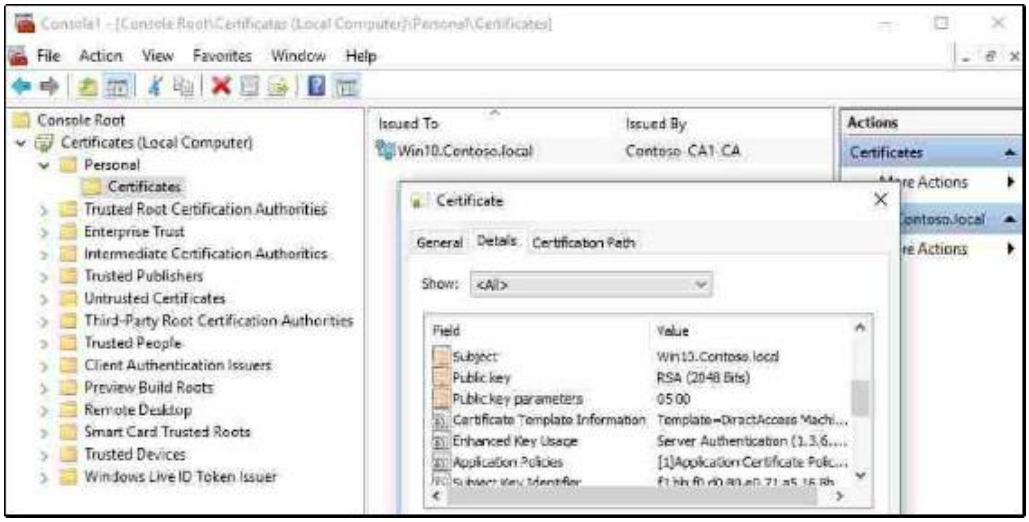


Viene visualizzata la schermata Richiedi certificati, che è l'elenco dei modelli a nostra disposizione. Questo elenco è dinamico; si basa sul computer a cui hai effettuato l'accesso e sulle autorizzazioni del tuo account utente. Ricordi quando abbiamo impostato la scheda di sicurezza del nostro nuovo modello di certificato? È lì che abbiamo definito chi e cosa potrebbe estrarre nuovi certificati in base a quel modello e, se avessi definito un gruppo più particolare rispetto ai computer di dominio, è possibile che il mio nuovo modello di macchina DirectAccess non venga visualizzato in questo elenco. Tuttavia, dal momento che ho aperto quel modello per essere distribuito a qualsiasi computer all'interno del nostro dominio, posso vederlo qui:



Se non vedi il tuo nuovo modello nell'elenco, fai clic sulla casella di controllo per Mostra tutti i modelli. Questo ti darà un elenco completo di tutti i modelli sul server CA e una descrizione su ognuno di essi sul motivo per cui non è attualmente disponibile per l'emissione

Metti un segno di spunta accanto a tutti i certificati che desideri e fai clic su Iscriviti. Ora la console gira per alcuni secondi mentre il server CA elabora la tua richiesta ed emette un nuovo certificato specifico per il tuo computer e i criteri che abbiamo inserito nel modello di certificato. Una volta terminato, puoi vedere che il nostro nuovissimo certificato della macchina è ora all'interno di Personal | Certificati nella MMC. Se fai doppio clic sul certificato, puoi controllare le sue proprietà per assicurarti che tutte le impostazioni che desideri vengano inserite in questo certificato esistono:



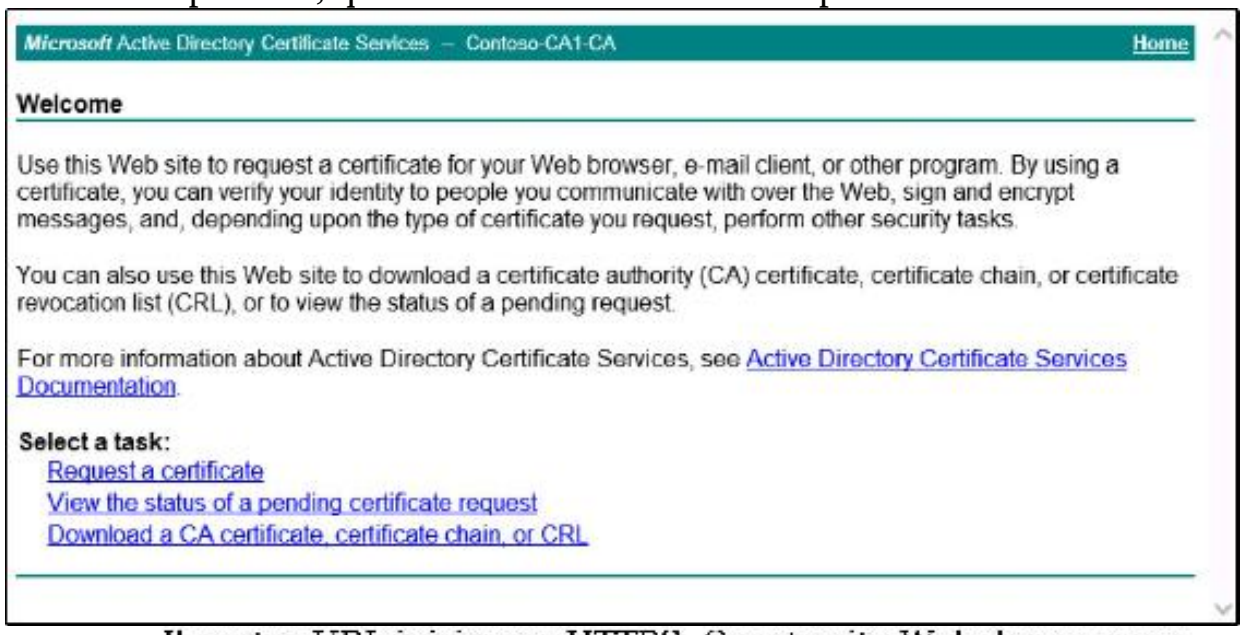
Richiesta di un certificato dall'interfaccia Web

Di solito utilizzo MMC per richiedere certificati quando possibile, ma, nella maggior parte dei casi, esiste un'altra piattaforma da cui è possibile richiedere ed emettere certificati. Dico nella maggior parte dei casi perché l'esistenza di questa opzione dipende da come è stato costruito il server CA in primo luogo. Quando ho installato il mio ruolo di Servizi certificati Active Directory, mi sono assicurato di scegliere le opzioni sia per l'autorità di certificazione che per la registrazione Web dell'autorità di certificazione. Questa seconda opzione è importante per la nostra prossima sezione di testo. Senza la parte di registrazione Web del ruolo, non avremmo un'interfaccia Web in esecuzione sul nostro server CA e questa parte non sarebbe disponibile. Se il tuo server CA non ha la registrazione Web attivata, puoi rivisitare la pagina di installazione del ruolo in Server Manager e aggiungerla al ruolo esistente:

Una volta che la registrazione Web dell'Autorità di certificazione è stata installata sulla CA, su quel server è ora in esecuzione un sito Web a cui è possibile accedere tramite un browser dall'interno della rete. Avere questo sito web è utile se hai la necessità che gli utenti siano in grado di emettere i propri certificati per qualche motivo; sarebbe molto più facile fornire loro la documentazione o addestrarli sul processo di richiesta di un certificato da un sito Web piuttosto che aspettarsi che navighino nella console MMC. Inoltre, se stai tentando di richiedere certificati da computer che non si trovano nella stessa rete del server CA, l'utilizzo di MMC può essere difficile. Ad esempio, se hai la necessità che un utente a casa possa richiedere un nuovo certificato, senza un tunnel VPN

completo, molto probabilmente la console MMC non sarà in grado di connettersi al server CA per estrarre quel certificato. Ma poiché abbiamo questo sito Web di registrazione del certificato in esecuzione, è possibile pubblicare esternamente questo sito Web come si fa con qualsiasi altro sito Web nella rete, utilizzando un proxy inverso o un firewall per mantenere il traffico sicuro e presentare agli utenti la possibilità di colpire questo sito e richiedere certificati ovunque si trovino.

Per accedere a questo sito Web, utilizziamo di nuovo il nostro normale computer client. Questa volta, invece di aprire MMC, avvierò semplicemente Internet Explorer o qualsiasi altro browser e accedo al sito Web in esecuzione su https: // <CASERVER> / certsrv. Per il mio ambiente specifico, quell'indirizzo web esatto è https: // CA1 / certsrv:

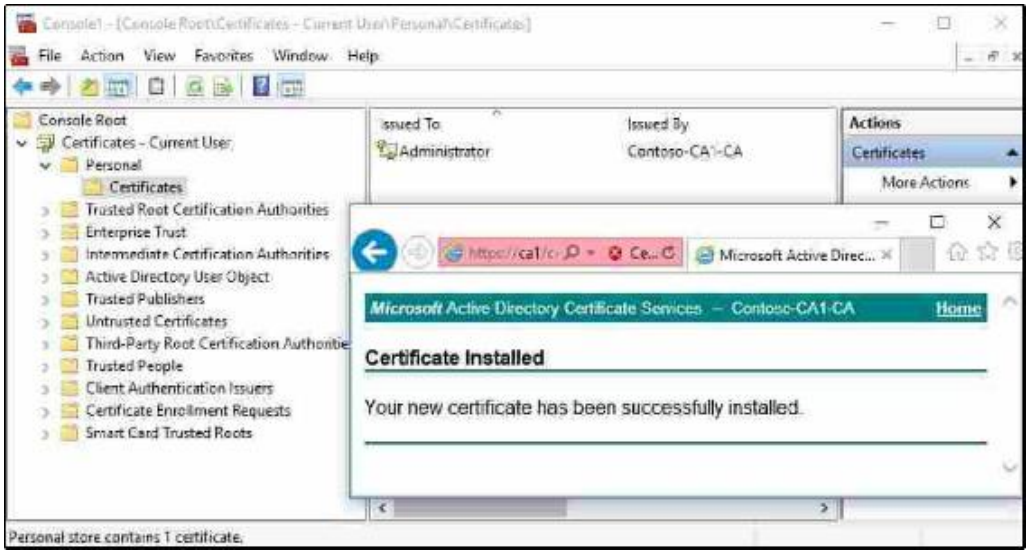


Il nostro URL inizia con HTTPS. Questo sito Web deve essere configurato per essere eseguito su HTTPS anziché su HTTP normale per consentire al sito Web di richiedere certificati. Non consente l'emissione di certificati su HTTP perché tali informazioni viaggerebbero in testo non crittografato per il client. L'abilitazione del sito Web sul server CA per HTTPS garantisce che il certificato emesso verrà crittografato durante

Facendo clic sul collegamento Richiedi un certificato si accede alla nostra procedura guidata in cui possiamo richiedere un nuovo certificato dal server CA. Quando gli utenti si dirigono autonomamente attraverso questa interfaccia web, in genere è ai fini di un certificato basato sull'utente, poiché abbiamo alcuni modi piuttosto semplici per distribuire automaticamente i certificati a livello di computer senza alcuna interazione da parte dell'utente. Ne discuteremo tra un momento. Tuttavia, per questo esempio, poiché chiediamo ai nostri utenti di accedere qui e richiedere un nuovo certificato utente, nella pagina successiva, sceglierò quel collegamento:

Se non fossi interessato a un certificato utente e volessi utilizzare l'interfaccia web per richiedere un certificato macchina, un certificato server web o qualsiasi altro tipo di certificato, potresti invece scegliere il link per la richiesta avanzata del certificato e seguire le istruzioni da fare così

Successivamente, premi il pulsante Invia e, una volta generato il certificato, vedrai un collegamento che ti consente di installare questo certificato. Fare clic su quel collegamento e il nuovo certificato che è stato appena creato per te è stato installato sul tuo computer. Puoi vedere nella seguente schermata la risposta che il sito web mi ha dato, indicando un'installazione riuscita, e puoi anche vedere che ho aperto i certificati utente correnti all'interno di MMC per vedere e convalidare che il certificato esiste davvero:

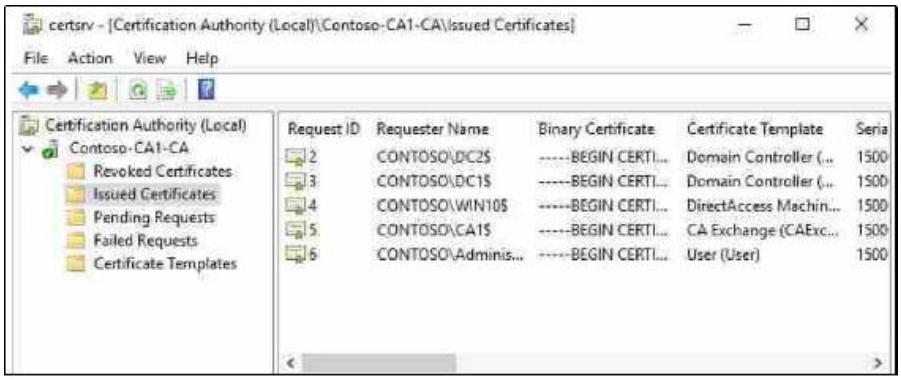


Creazione di un criterio di registrazione automatica

Il nostro server dell'autorità di certificazione è configurato e in esecuzione e possiamo emettere correttamente i certificati alle macchine client. Grande! Ora facciamo finta di avere un nuovo progetto nei nostri piatti e uno dei requisiti per questo progetto è che tutti i computer nella tua rete debbano avere una copia di questo nuovo certificato macchina che abbiamo creato. Uh oh, sembra un sacco di lavoro. Anche se il processo per richiedere uno di questi certificati è molto veloce - solo una manciata di secondi su ogni workstation - se dovessi farlo individualmente su un paio di migliaia di macchine, stai parlando di un periodo di tempo serio che deve essere speso su questo processo. Inoltre, in molti casi, i certificati che rilasci saranno validi solo per un anno. Ciò significa che devo affrontare una quantità enorme di lavoro amministrativo ogni anno per riemettere questi certificati quando scadono? Certamente no!

Scopriamo come utilizzare Criteri di gruppo per creare un oggetto Criteri di gruppo che registrerà automaticamente i nostri nuovi certificati su tutte le macchine della rete e, mentre siamo lì, configuriamolo anche in modo che quando arriva la data di scadenza di un certificato, il certificato si rinnoverà automaticamente agli intervalli appropriati.

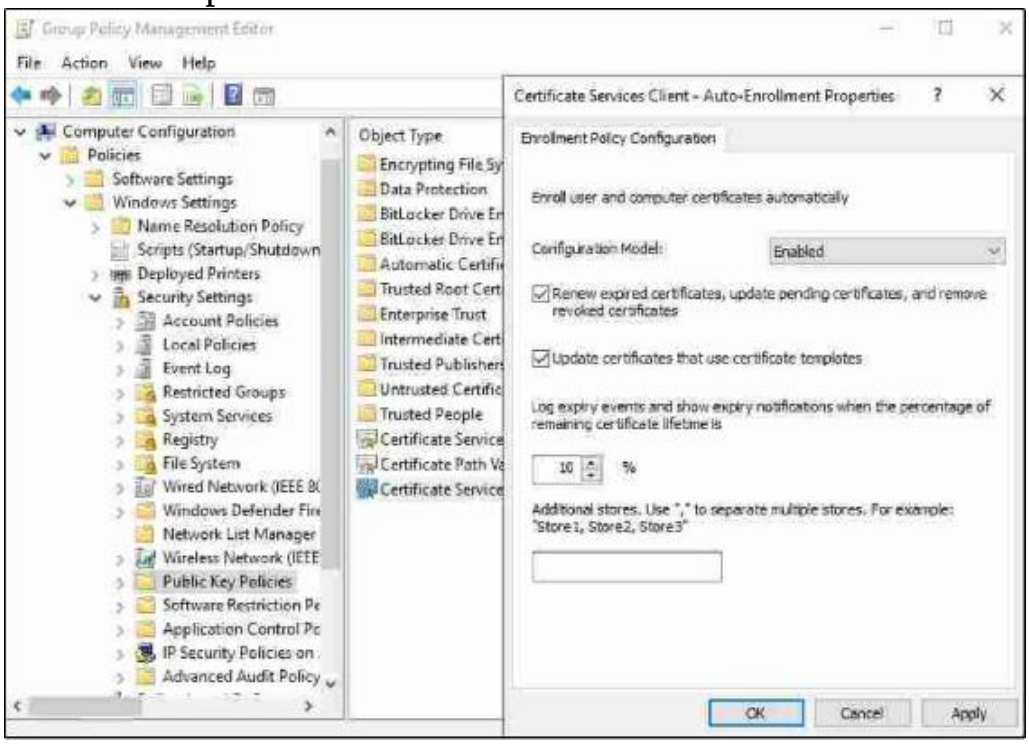
Facciamo un salto nella console di gestione dell'Autorità di certificazione sul nostro server CA e diamo un'occhiata alla cartella Certificati emessi. Voglio solo guardare qui per un minuto per vedere quanti certificati abbiamo emesso finora nella nostra rete. Sembra solo una manciata di loro, quindi si spera che una volta terminata la configurazione della nostra politica, se lo abbiamo fatto correttamente e ha effetto automaticamente, dovremmo vedere più certificati che iniziano a comparire in questo elenco:


certsrv - [Certification Authority (Local)\Contoso-CA1-CA\Issued Certificates]
File Action View Help
Certification Authority (Local)
Contoso-CA1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Request ID
Requester Name
Binary Certificate
Certificate Template
Seria
2 CONTOSO\DC2$ -----BEGIN CERTI... Domain Controller (... 1500
3 CONTOSO\DC1$ -----BEGIN CERTI... Domain Controller (... 1500
4 CONTOSO\WIN10$ -----BEGIN CERTI... DirectAccess Machin... 1500
5 CONTOSO\CA1$ -----BEGIN CERTI... CA Exchange (CAExc... 1500
6 CONTOSO\Adminis... -----BEGIN CERTI... User (User) 1500

Accedi a un server controller di dominio, quindi apri la console Gestione criteri di gruppo. Ho creato un nuovo oggetto Criteri di gruppo chiamato Abilita registrazione automatica certificato e ora lo sto modificando per trovare le impostazioni che devo configurare per fare in modo che questo oggetto Criteri di gruppo faccia il suo lavoro:

Le impostazioni all'interno di questo oggetto Criteri di gruppo che si desidera configurare si trovano in Configurazione computer | Politiche | Impostazioni di Windows | Impostazioni di sicurezza | Politiche chiave pubblica | Client di Servizi certificati - Registrazione automatica.

Fare doppio clic su questa impostazione per visualizzarne le proprietà. Tutto ciò che dobbiamo fare è modificare il modello di configurazione su Abilitato e assicurarci di selezionare la casella che dice Rinnova i certificati scaduti, aggiorna i certificati in sospeso e rimuovi i certificati revocati. Seleziona anche la casella Aggiorna certificati che utilizzano modelli di certificato. Queste impostazioni garantiranno che il rinnovo automatico avvenga automaticamente quando i certificati inizieranno a scadere nei prossimi anni:



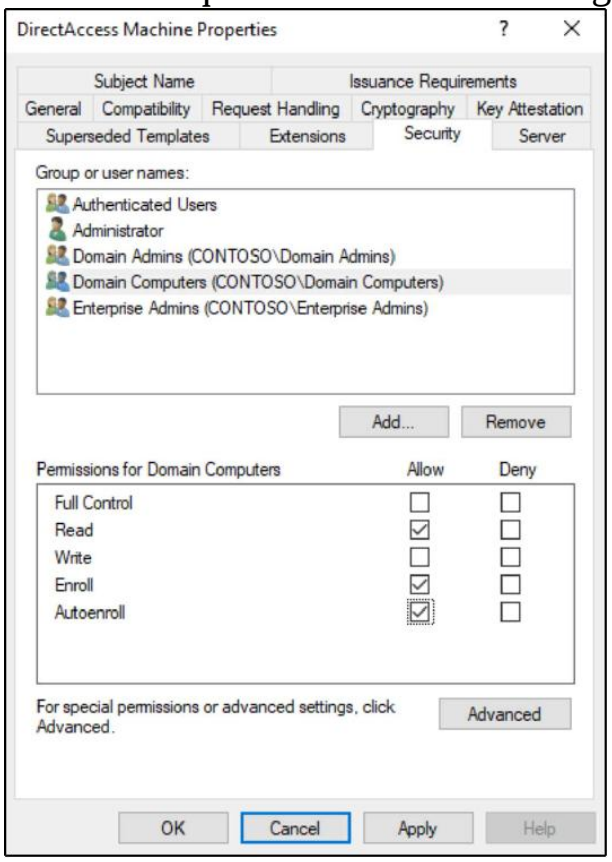
Qual è l'ultima cosa che dobbiamo fare sul nostro GPO per renderlo attivo? Crea un collegamento in modo che inizi ad applicarsi! Per il tuo ambiente, probabilmente creerai un collegamento più specifico a una particolare unità organizzativa, come abbiamo discusso nell'ultimo capitolo, ma, per il mio laboratorio, voglio che questi certificati si applichino a ogni singola macchina che fa parte del dominio, quindi Collegherò il mio nuovo oggetto Criteri di gruppo alla radice del dominio, in modo che si applichi a tutti i miei client e server.

Ora che l'oggetto Criteri di gruppo è stato creato e configurato e l'abbiamo collegato al dominio, penserei che sarebbero stati emessi alcuni nuovi certificati e ci sarebbero stati più nomi mostrati nella mia cartella Certificati emessi all'interno della mia console dell'autorità di certificazione. Ma non ci sono. Aspetta un minuto, nel nostro GPO non abbiamo specificato nulla di particolare per il mio modello di certificato DirectAccess Machine, vero? Potrebbe essere questo il problema? No, non c'era davvero un'opzione per specificare quale modello volevo impostare per la registrazione automatica.

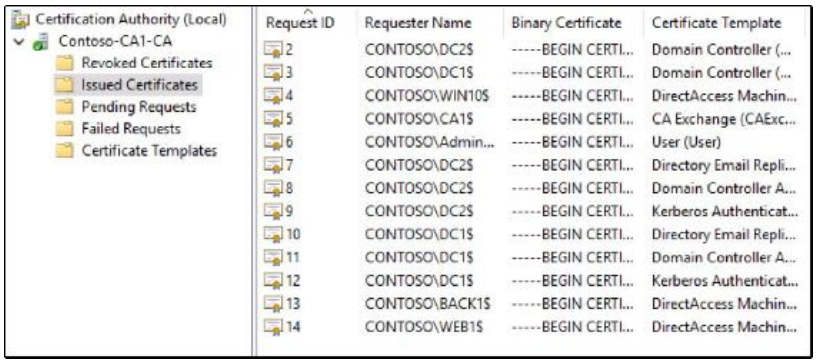
Quando si abilita la registrazione automatica in Criteri di gruppo, è sufficiente capovolgere un interruttore di attivazione / disattivazione e attivarlo per ogni modello di certificato. Quindi, ora che abbiamo una policy configurata per abilitare la registrazione automatica ed è collegata al dominio, rendendola così attiva, la registrazione automatica è stata abilitata su ogni computer che fa parte del dominio, per ogni modello di certificato pubblicato sulla nostra CA server. Eppure, nessuno di loro si sta inviando ai miei computer. Questo perché dobbiamo modificare le impostazioni di sicurezza nel nostro nuovo modello di macchina DirectAccess. Attualmente lo abbiamo configurato in modo che tutti i computer del dominio dispongano delle autorizzazioni di registrazione, ma se ricordi quella scheda di sicurezza all'interno delle proprietà del modello di certificato, c'era un identificatore di sicurezza aggiuntivo chiamato Registrazione automatica. Ogni modello di certificato ha l'identificatore dell'autorizzazione alla registrazione automatica, e non è consentito per impostazione predefinita. Ora che l'interruttore della luce è stato acceso per la registrazione automatica nel nostro dominio, dobbiamo

abilitare l'autorizzazione alla registrazione automatica su qualsiasi modello che vogliamo iniziare a distribuire da solo. Non appena abilitiamo tale autorizzazione, questi certificati inizieranno a circolare nella nostra rete.

Accedi alla sezione di gestione dei certificati del tuo server CA e apri le Proprietà del tuo nuovo modello, quindi vai alla scheda Sicurezza e consenti le autorizzazioni di registrazione automatica per il gruppo Computer di dominio. Questo dovrebbe indicare alla CA di iniziare a distribuire questi certificati di conseguenza:



E abbastanza sicuro, se lascio riposare il mio ambiente per un po ', dando ad Active Directory e ai Criteri di gruppo la possibilità di aggiornarsi su tutte le mie macchine, ora vedo che sono stati emessi più certificati dal mio server CA:



Per emettere automaticamente i certificati da qualsiasi modello che crei, pubblica semplicemente il modello e assicurati di configurare le autorizzazioni di registrazione automatica appropriate su quel modello. Una volta che l'oggetto Criteri di gruppo di registrazione automatica è stato impostato su tali client, questi raggiungeranno il server CA e gli chiederanno i certificati da qualsiasi modello per il quale dispongono delle autorizzazioni per ricevere un certificato. In futuro, quando il certificato sta per scadere e la macchina necessita di una nuova copia, il criterio di registrazione automatica ne emetterà uno nuovo prima della data di scadenza, in base ai timestamp definiti all'interno dell'oggetto Criteri di gruppo.

La registrazione automatica del certificato può sopportare quello che normalmente sarebbe un enorme onere amministrativo e trasformarlo in un processo completamente automatizzato!

Ottenere un certificato SSL di un'autorità pubblica

Ora siamo abbastanza a nostro agio con l'acquisizione di certificati dal nostro server CA all'interno della nostra rete, ma per quanto riguarda la gestione di quei certificati SSL per i nostri server Web che dovrebbero essere acquisiti da un'autorità di certificazione pubblica? Per molti di voi, questa sarà l'interazione più comune con i certificati ed è molto importante capire anche questo lato della medaglia. Quando è necessario acquisire un certificato SSL dall'autorità pubblica scelta, è necessario eseguire una procedura in tre fasi: creare una richiesta di certificato, inviare la richiesta di certificato e installare il certificato risultante. Utilizzeremo il mio server WEB1, sul quale ho un sito web in esecuzione. Attualmente il sito è in grado di gestire solo il traffico HTTP,

Per poter utilizzare HTTPS, dobbiamo installare un certificato SSL sul server WEB1. Questo server Web esegue la piattaforma dei servizi Web Microsoft, Internet Information Services (IIS). Il processo in tre fasi che eseguiamo è lo stesso se stai eseguendo un server web diverso, come Apache, ma le cose particolari che devi fare per eseguire questi tre passaggi saranno diverse, perché Apache o qualsiasi altro server web avrà un'interfaccia utente diversa da IIS. Poiché stiamo lavorando su un server Web Windows Server 2019, stiamo utilizzando IIS 10.

Coppia di chiavi pubblica / privata

Prima di passare all'esecuzione di questi tre passaggi, discutiamo del motivo per cui tutto questo è importante. Probabilmente hai sentito parlare del termine chiave privata, ma potresti non capire bene cosa significhi. Quando inviamo traffico su Internet, dai nostri computer client a un sito Web HTTPS, comprendiamo che il traffico è crittografato. Ciò significa che i pacchetti sono legati in un bel pacchetto prima di lasciare il mio laptop in modo che nessuno possa vederli mentre viaggiano, e vengono quindi scartati con successo quando quei pacchetti raggiungono il server web. Il mio laptop utilizza una chiave per crittografare il traffico e il server utilizza una chiave per decrittografare quel traffico, ma come fanno a sapere quali chiavi utilizzare? Esistono due diversi tipi di metodologia di crittografia che possono essere utilizzati qui:

- **Crittografia simmetrica**: Il metodo di crittografia più semplice, simmetrico, significa che esiste un'unica chiave e viene utilizzata da entrambe le parti. Il traffico viene impacchettato utilizzando una chiave e la stessa chiave viene utilizzata per scartare quel traffico quando raggiunge la sua destinazione. Poiché questa singola chiave è l'onnipotente Oz, non vorresti che finisse nelle mani sbagliate, il che significa che non la presenteresti su Internet. Pertanto, la crittografia simmetrica non viene generalmente utilizzata per proteggere il traffico del sito Web Internet.
- **Crittografia asimmetrica**: Questo è il nostro obiettivo con il traffico HTTPS. La crittografia asimmetrica utilizza due chiavi:

una chiave pubblica e una chiave privata. La chiave pubblica è inclusa nel tuo certificato SSL, quindi chiunque su Internet può contattare il tuo sito web e ottenere la chiave pubblica. Il tuo laptop utilizza quindi quella chiave pubblica per crittografare il traffico e lo invia al server web. Perché è sicuro se la chiave pubblica viene trasmessa all'intera Internet? Perché il traffico può essere decrittografato solo utilizzando una chiave privata corrispondente, che viene archiviata in modo sicuro sul tuo server web. È molto importante mantenere la sicurezza sulla tua chiave privata e sui tuoi server web e assicurarti che la chiave non cada nelle tasche di qualcun altro.

Creazione di una richiesta di firma del certificato

Se il primo passo per acquisire un certificato SSL dall'entità CA pubblica è stato quello di accedere al loro sito Web, acquistare un certificato e scaricarlo immediatamente, hai già perso l'imbarcazione. Quel certificato ovviamente non avrebbe modo di conoscere una chiave privata che potresti avere seduto sul tuo server web, e quindi quel certificato sarebbe effettivamente inutile se installato ovunque.

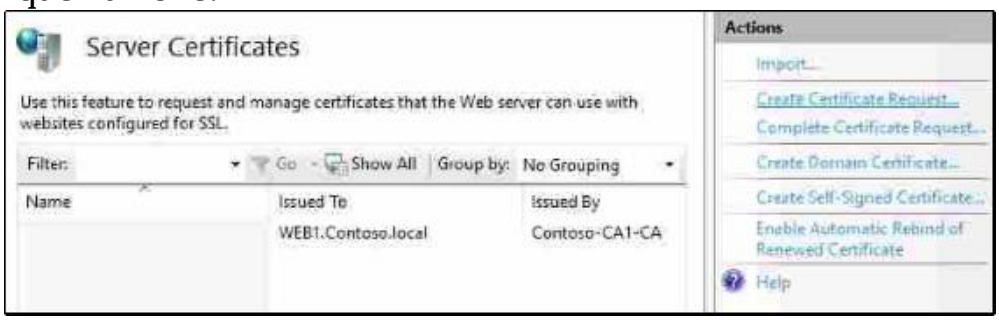
Quando installi un certificato SSL su un server web, è molto importante che il certificato conosca la tua chiave privata. Come ci assicuriamo che ciò accada? È qui che entra in gioco la richiesta di firma del certificato (CSR). Il primo passo per acquisire correttamente un certificato SSL è generare una CSR. Quando crei quel file, la piattaforma del server web crea la chiave privata necessaria e la nasconde sul tuo server. La CSR viene quindi creata in modo tale che sappia esattamente come interagire con quella chiave privata, quindi si utilizza la CSR quando si accede al sito Web della CA per richiedere il certificato.

La chiave privata non è all'interno della CSR e la CA non sa mai qual è la tua chiave privata. Questa chiave è estremamente importante e viene memorizzata solo sul tuo server web, all'interno della tua organizzazione.

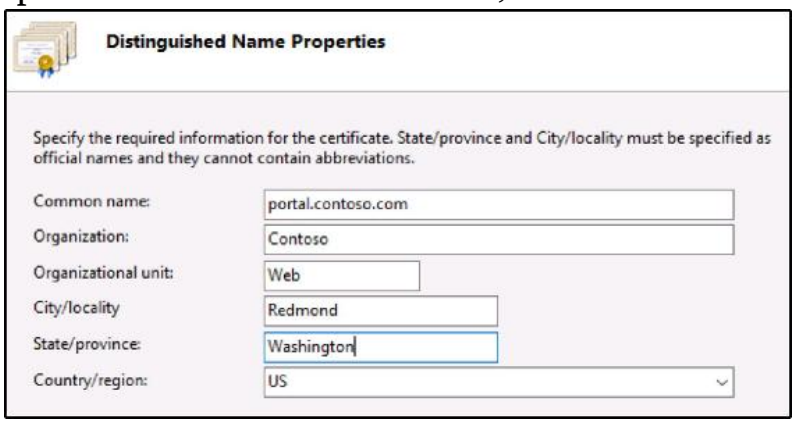
Per generare un CSR, apri IIS dal menu Strumenti di Server Manager, quindi fai clic sul nome del server web dall'albero di navigazione sul lato sinistro dello schermo. Questo popolerà una serie di applet diverse al centro della console. Quello con cui vogliamo lavorare si chiama Server Certificates. Vai avanti e fai doppio clic su quello:


Connections
Start Page
WEB1 (CONTOSO\administra
WEB1 Home
Filter:
Go
Show All
Group by:
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Handler Mappings
HTTP Respon...
Logging
MIME Types
Modules
Output Caching
Request Filtering
Server Certificates
WebDAV Authori...
Worker Processes
Features View
Content View

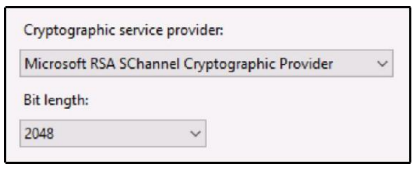
Ora, all'interno della schermata Certificati server, puoi vedere tutti i certificati esistenti che risiedono sul server qui elencato. È qui che alla fine abbiamo bisogno di vedere il nostro nuovo certificato SSL, in modo da poterlo utilizzare all'interno delle proprietà del nostro sito Web quando siamo pronti per attivare HTTPS. Il primo passo per acquisire il nostro nuovo certificato è creare la richiesta di certificato da utilizzare con la nostra CA e, se dai un'occhiata sul lato destro dello schermo, vedrai una sezione Azioni, sotto la quale è elencato Crea certificato**Richiesta.** Vai avanti e fai clic su quell'azione:



Nella procedura guidata risultante, è necessario inserire le informazioni che verranno archiviate nel certificato SSL. Il campo Nome comune è l'informazione più importante qui, deve essere il nome DNS che questo certificato proteggerà. Quindi, in pratica, inserisci qui il nome del tuo sito web. Quindi continua con la compilazione del resto delle informazioni specifiche della tua azienda. Un paio di note speciali che spesso sembrano far inciampare gli amministratori sono che l'unità organizzativa può essere qualsiasi cosa; Di solito inserisco solo la parola Web. Assicurati di precisare il nome del tuo stato; non utilizzare un'abbreviazione:



Nella pagina Proprietà del provider di servizi crittografici, in genere si desidera lasciare l'impostazione predefinita del provider di servizi crittografici, a meno che non si disponga di una scheda crittografica specializzata nel server e si preveda di utilizzarla per la gestione dell'elaborazione della crittografia per questo sito Web. Su un server IIS, avrai quasi sempre il provider di crittografia Microsoft RSA SChannel elencato qui. Quello che vuoi cambiare, tuttavia, è la lunghezza del bit. La lunghezza standard in bit per molti anni è stata di 1.024 e continua a essere la scelta predefinita in Windows Server 2019. L'industria generale della crittografia SSL ha deciso che 1.024 è troppo debole e il nuovo standard è 2.048. Quando accedi al sito Web della tua CA per richiedere un certificato, molto probabilmente scoprirai che la tua richiesta deve avere un minimo di 2.048 bit.



Ill'unica cosa che resta da fare per il nostro CSR è assegnargli una posizione e un nome file. Salvare questo csr come file di testo è il modo normale di procedere e serve bene ai nostri scopi perché tutto ciò che dobbiamo fare quando richiediamo il nostro certificato è aprire il file e quindi copiare e incollare il contenuto. Ora hai creato il tuo file csr e possiamo utilizzarlo per richiedere il certificato alla nostra CA pubblica.

Invio della richiesta di certificato

Ora, vai al sito Web della tua autorità di certificazione pubblica. Ancora una volta, tutte le società che abbiamo menzionato in precedenza, come GoDaddy o Verisign, sono adatte a questo scopo. Ogni autorità ha il proprio aspetto per la propria interfaccia web, quindi non posso darti i passaggi esatti che devono essere eseguiti per questo processo. Una volta che hai un account e accedi al sito dell'autorità, dovresti essere in grado di trovare un'opzione per l'acquisto di un certificato SSL. Una

volta che il certificato è stato acquistato, ci sarà un processo per richiedere e distribuire quel certificato.

Una volta entrati nell'interfaccia per la creazione del nuovo certificato, in genere l'unica informazione che la CA ti chiederà è il contenuto del file csr. Se apri il file di testo che abbiamo salvato in precedenza, vedrai un grosso ammasso di sciocchezze:

Questo pasticcio di dati è esattamente ciò di cui la CA ha bisogno per creare il tuo nuovo certificato SSL in modo che sappia come interagire con la chiave privata del tuo server web. Solo il server che ha generato la CSR sarà in grado di accettare e utilizzare correttamente il certificato SSL basato su questa CSR. In genere, tutto ciò che devi fare è copiare l'intero contenuto del file csr e incollarlo nel sito Web della CA.

Download e installazione del certificato

Ora siediti e aspetta. A seconda dell'autorità che stai utilizzando e della frequenza con cui la tua azienda acquista i certificati da questa autorità, il tuo certificato potrebbe essere disponibile per il download quasi immediatamente o potrebbero essere necessarie alcune ore prima che il certificato venga visualizzato nell'elenco dei download disponibili. La ragione di ciò è che molte delle CA utilizzano l'approvazione umana per i nuovi certificati e stai letteralmente aspettando che qualcuno metta gli occhi sulla richiesta di certificato e sulle tue informazioni per assicurarti che tu lavori davvero per l'azienda e che possiedi davvero questo dominio nome. Ricorda, il vero vantaggio di un certificato SSL pubblico è che la

CA garantisce che l'utente di questo certificato sia il vero affare, quindi vogliono assicurarsi di non emettere un certificato per portal.contoso.com a qualcuno nel Organizzazione Fabrikam per errore.

Una volta che sei in grado di scaricare il certificato dal sito Web della CA, vai avanti e copialo sul server Web da cui abbiamo generato la CSR. È di fondamentale importanza installare questo nuovo certificato sullo stesso server. Se dovessi installare questo nuovo certificato su un server web diverso, uno che non ha generato la CSR da cui è stato creato il certificato, quel certificato verrebbe importato correttamente, ma non sarebbe in grado di funzionare. Ancora una volta, ciò è dovuto al fatto che la chiave privata con cui il certificato intende interagire non sarebbe presente su un server diverso.

Di nuovo all'interno della console di gestione IIS, ora possiamo usare l'azione successiva in quell'elenco a destra, chiamata Certificato completo **Richiesta.** Questo avvia un breve piccolo wizard in cui trovi il nuovo file del certificato che hai appena scaricato e importalo nel nostro server. Ora che il certificato risiede sul server, è pronto per essere utilizzato dal tuo sito web.

C'è un elemento aggiuntivo che controllo sempre dopo l'installazione o l'importazione di un certificato SSL. Ora puoi vedere il tuo nuovo certificato elencato in IIS e se fai doppio clic sul tuo nuovo certificato vedrai la pagina delle proprietà per il certificato. Nella scheda Generale di queste proprietà, dai un'occhiata in fondo. Il tuo certificato dovrebbe mostrare una piccola icona a chiave e il messaggio Hai una chiave privata che corrisponde al testo del certificato. Se riesci a visualizzare questo messaggio, l'importazione è stata eseguita correttamente e il nuovo file del certificato corrisponde perfettamente alla CSR. Il server e il certificato ora condividono le informazioni fondamentali sulla chiave privata e il certificato SSL sarà in grado di funzionare correttamente per proteggere il nostro sito web. Se non vedi questo messaggio, qualcosa è andato storto durante la richiesta e il download del nostro certificato. Se non vedi il messaggio qui, devi ricominciare generando un nuovo CSR, perché il file del certificato che hai ottenuto non deve essere stato codificato in modo appropriato rispetto a quel CSR, o qualcosa del genere. Senza il testo della chiave privata nella parte inferiore di questa schermata, il certificato non convaliderà correttamente il traffico.

Ecco un esempio di come dovrebbe apparire quando funziona correttamente:

Esportazione e importazione di certificati

Spesso mi trovo a dover utilizzare lo stesso certificato SSL su più server. Ciò potrebbe accadere nel caso in cui ho più di un server IIS che serve lo stesso sito Web e sto utilizzando una qualche forma di bilanciamento del carico per dividere il traffico tra di loro. Questa necessità può sorgere anche quando si lavora con qualsiasi forma di bilanciamento del carico hardware, poiché a volte è necessario importare certificati non solo sui server Web stessi, ma nella casella del bilanciamento del carico. Un altro esempio è quando si utilizzano certificati con caratteri jolly; quando acquisti un carattere jolly, in genere intendi installarlo su più server.

Ciò significa che devo generare una nuova CSR da ogni server e richiedere più volte una nuova copia dello stesso certificato? Sicuramente no, e in effetti così facendo potresti causare altri problemi: quando una CA pubblica ripone la chiave di un certificato, in altre parole, se hai già richiesto un certificato con un nome particolare e poi torni più tardi per richiedere un'altra copia di lo stesso certificato: tale CA potrebbe invalidare il primo quando emette la seconda copia. Questo non è sempre immediatamente evidente, in quanto di solito c'è un timer impostato sull'annullamento del primo certificato. Se rivedi l'interfaccia web della CA e richiedi una nuova copia dello stesso certificato utilizzando un nuovo CSR per il tuo secondo server web, potresti scoprire che tutto funziona correttamente per alcuni giorni,

Cosa dovremmo fare? Quando devi riutilizzare lo stesso certificato SSL su più server, puoi semplicemente esportarlo da uno e importarlo sul successivo. Non è affatto necessario contattare la CA. Questo processo è abbastanza semplice e ci sono due posti comuni in cui puoi farlo: all'interno dello snap-in MMC per i certificati o dall'interno di IIS stesso. È importante notare, tuttavia, che il processo è leggermente diverso a seconda della strada che prendi e devi essere particolarmente consapevole di ciò che sta accadendo con la chiave privata mentre passi attraverso queste procedure guidate.

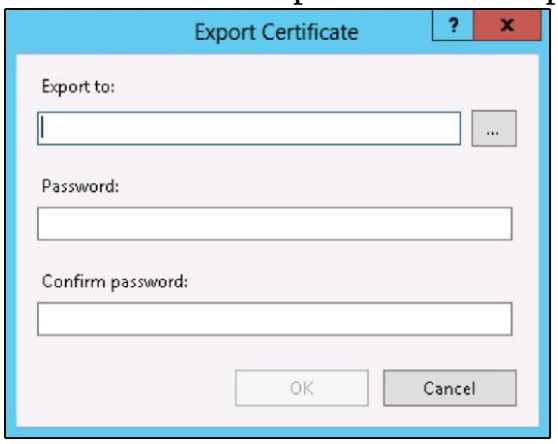
Esportazione da MMC

Torna all'archivio certificati del tuo computer locale in MMC e vai a Personale | Certificati in modo da poter vedere il tuo certificato SSL elencato. Fare clic con il pulsante destro del mouse sul certificato, quindi accedere a Tutte le attività |**Esportare.** Quando esamini questa esportazione
procedura guidata, la parte importante che volevo menzionare avviene subito nei passaggi della procedura guidata. La prima scelta che devi fare è se esportare la chiave privata. Anche in questo caso, la chiave privata è la salsa segreta che consente al certificato di interagire correttamente con il server su cui è installato. Se esporti senza la chiave privata, quel certificato non funzionerà su un altro server. Quindi è importante qui che, se stai esportando questo certificato con l'intenzione di installarlo su un secondo server web e usarlo per convalidare il traffico SSL, selezioni l'opzione in alto per Sì, esporta la chiave privata:

Poiché la procedura guidata ti avvisa sufficientemente, quando scegli di esportare un certificato che contiene le informazioni sulla chiave privata, ti viene richiesto di fornire una password, che verrà utilizzata per proteggere il file PFX esportato. È importante scegliere una buona password. Se lo dimentichi, il tuo file esportato sarà completamente inutile. Se inserisci una password molto semplice o facile da indovinare, chiunque metta le mani su questo file PFX potrebbe essere in grado di utilizzare il tuo certificato e la tua chiave privata sui propri server web, il che non andrebbe bene.

Esportazione da IIS

All'interno dell'applet Certificati server per IIS, fai clic con il pulsante destro del mouse sul certificato e scegli
Esportare. Questo avvia una procedura guidata di una sola pagina che ti chiede semplicemente una posizione e una password:



Avevamo molte più opzioni che avremmo potuto scegliere o negare quando abbiamo esportato utilizzando MMC, quindi perché è così breve? IIS fa delle ipotesi per il resto delle impostazioni al fine di accelerare il processo di esportazione. Quando esporti un certificato SSL, è probabile che tu intenda esportare anche la chiave privata. Pertanto, IIS effettua semplicemente tale presupposto e ignora il resto delle scelte. Sei costretto a inserire una password perché non puoi scegliere la chiave privata; verrà incluso automaticamente con l'esportazione del certificato. Quindi, se avessi qualche motivo per esportare un certificato che non conteneva le informazioni sulla chiave privata, non potresti utilizzare la console IIS per questa attività. Dovresti aprire MMC e seguire la procedura guidata più ampia che si trova lì.

Importazione in un secondo server

Qualunque sia la direzione che prendi per eseguire l'esportazione, una volta che hai a disposizione il file PFX completo, l'importazione nel tuo secondo server è molto semplice. Da entrambe le console, MMC o IIS, puoi fare clic con il pulsante destro del mouse e scegliere l'azione Importa. Passando attraverso i passaggi, scegli semplicemente il file PFX e quindi inserisci la password che hai usato per proteggere il file. Il certificato quindi importa e, se apri le proprietà, vedrai che l'icona della piccola chiave e il messaggio della chiave privata vengono visualizzati correttamente nella parte inferiore della schermata delle proprietà del certificato. Se non vedi il messaggio Hai una chiave privata, hai fatto qualcosa di sbagliato durante il processo di esportazione e dovrai riprovare.

Vai avanti e provalo tu stesso; trova un server con un certificato SSL e prova ad esportare quel certificato con e senza la chiave privata. Quando importi in un nuovo server, vedrai che l'importazione del file del certificato senza una chiave privata non contiene questo messaggio nella parte inferiore della pagina delle proprietà, ma il file esportato che contiene la chiave privata, restituisce qui il messaggio corretto . Per fare un ulteriore passo avanti, prova a utilizzare entrambi i certificati su un sito Web non importante e guarda cosa succede. Scoprirai che il certificato privo della chiave privata non riuscirà a convalidare il traffico SSL.

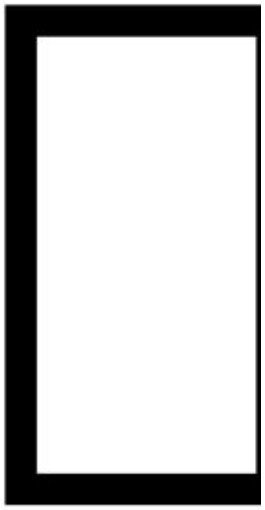
Se si tenta di esportare un certificato SSL e l'opzione per includere la chiave privata è disattivata, ciò significa che quando l'amministratore originale ha installato questo certificato sul server Web, ha scelto un'opzione speciale che blocca la possibilità di esportare la chiave privata nel futuro. In questo caso, non sarai in grado di esportare il certificato con la

Sommario

I certificati spesso hanno una cattiva reputazione, e credo che ciò sia dovuto al fatto che la gente pensa che sia un mal di testa da affrontare. Capisco il loro punto. Senza sapere come navigare tra le varie console amministrative che si occupano della tua infrastruttura di certificati, sarebbe difficile far funzionare anche gli elementi più semplici. Esaminando le attività più comuni relative ai certificati che qualsiasi amministratore di server dovrà eventualmente affrontare all'interno delle proprie reti, spero che ora tu abbia trovato un po 'di conforto e sicurezza per progredire con quei progetti che potrebbero essere attualmente sospesi, in attesa di l'infrastruttura dei certificati da costruire. Nel prossimo capitolo studieremo il networking con Windows Server 2019.

Domande

1. Qual è il nome del ruolo all'interno di Windows Server 2019 che ti consente di emettere certificati dal tuo server?
2. Che tipo di server CA viene solitamente installato per primo in un ambiente di dominio?
3. Dovresti installare il ruolo di autorità di certificazione su un controller di dominio?
4. Dopo aver creato un nuovo modello di certificato, quale passaggio successivo deve essere eseguito prima di poter emettere certificati ai computer o agli utenti da quel nuovo modello?
5. Qual è il nome generale dell'impostazione GPO che impone l'emissione di certificati senza l'intervento manuale da parte di un amministratore?
6. Un certificato SSL sarà in grado di convalidare correttamente il traffico solo se condivide _____informazioni chiave con il server web?
7. Qual è l'informazione principale di cui ha bisogno un'autorità di certificazione pubblica per emettere un nuovo certificato SSL (suggerimento: lo generi dal tuo server web)?



Collegamento in rete con Windows Server 2019

Come abbiamo discusso finora in questo libro, i server sono i tronchi degli alberi delle nostre reti. Sono l'infrastruttura principale che ci consente di portare a termine il lavoro. Se i server sono i trunk, le reti stesse devono essere le radici. La tua rete è la piattaforma che supporta l'infrastruttura aziendale; costituisce i canali che tutti i dispositivi all'interno dell'azienda utilizzano per comunicare tra loro.

Tradizionalmente, ci sono stati professionisti del server e professionisti della rete nel settore IT e in molti luoghi è ancora così. Un amministratore che lavora principalmente sui server in genere non ha abbastanza tempo durante la giornata per supportare anche l'infrastruttura di rete in un'organizzazione di qualsiasi dimensione, e anche il contrario è vero. Gli amministratori di rete generalmente si attengono alle proprie apparecchiature e strumenti di gestione e non sarebbero interessati a

immergersi troppo in profondità nel mondo di Windows Server. Tuttavia, molti di noi lavorano in aziende più piccole dove devono essere indossati molti cappelli. Alcuni giorni, sia l'amministratore del server che quello dell'amministratore di rete siedono uno sopra l'altro, quindi dobbiamo comprendere almeno una linea di base del networking e degli strumenti che possiamo utilizzare per risolvere i problemi di connessioni che non funzionano. Inoltre, Windows Server 2019 mette a fuoco una nuova mentalità di rete: la virtualizzazione delle reti. Ci sarà sempre una parvenza di rete fisica, che utilizza switch e router fisici per spostare i pacchetti tra stanze ed edifici diversi. Ma ora stiamo anche incorporando l'idea del software-defined networking (SDN) nei nostri server Windows, che ci dà la capacità di virtualizzare parte di quella configurazione. Non solo la configurazione stessa, stiamo effettivamente virtualizzando il traffico di rete e costruendo le nostre reti dall'interno di una console del server, piuttosto che utilizzare le interfacce della riga di comando per configurare i nostri router, cosa che era sempre necessaria in passato. utilizzando switch fisici e router per spostare i pacchetti tra stanze ed edifici diversi. Ma ora stiamo anche incorporando l'idea del software-defined networking (SDN) nei nostri server Windows, che ci dà la capacità di virtualizzare parte di quella configurazione. Non solo la configurazione stessa, stiamo effettivamente virtualizzando il traffico di rete e costruendo le nostre reti dall'interno di una console del server, piuttosto che utilizzare le interfacce della riga di comando per configurare i nostri router, cosa sempre necessaria in passato. utilizzando switch fisici e router per spostare i pacchetti tra stanze ed edifici diversi. Ma ora stiamo anche incorporando l'idea del software-defined networking (SDN) nei nostri server Windows, che ci dà la capacità di virtualizzare parte di quella configurazione. Non solo la configurazione stessa, stiamo effettivamente virtualizzando il traffico di rete e costruendo le nostre reti dall'interno di una console del server, piuttosto che utilizzare le interfacce della riga di comando per configurare i nostri router, che era sempre necessario in passato.

Tieni il telefono; Mi sto anticipando. Innanzitutto, parliamo di alcune delle cose nuove e utili all'interno di Windows Server 2019 che implicano il lavoro con reti fisiche o qualsiasi rete, perché queste saranno importanti per qualsiasi amministratore nel mondo delle reti di oggi.

Successivamente, dedicheremo alcuni minuti per esplorare ulteriormente questa nuova idea di virtualizzazione della rete.

seguenti sono gli argomenti che intendiamo discutere in questo capitolo: Introduzione a IPv6

- Il tuo toolbox di rete
- Creazione di una tabella di routing NIC Teaming
- Rete definita dal software

Introduzione a IPv6

Benvenuto nel lato oscuro! Sfortunatamente, questo è il numero di persone che pensano a IPv6 al momento. Sebbene IPv6 non sia affatto una novità, nella mia esperienza è ancora qualcosa che quasi nessuno ha implementato nelle proprie reti. Mentre lavoravo con centinaia di aziende diverse in tutto il mondo negli ultimi anni, mi sono imbattuto in una sola organizzazione che eseguiva IPv6 su tutta la loro rete di produzione e non era nemmeno un vero IPv6 nativo. Invece, stavano usando una tecnologia di tunneling, chiamata ISATAP, su tutta la loro rete per far parlare tra loro tutti i server e i client usando i pacchetti IPv6, ma questi pacchetti stavano ancora attraversando una rete fisica IPv4. Non fraintendermi; Ho trovato molti casi in cui le aziende stanno giocando con IPv6 e ne hanno una parvenza configurata su un pezzo sezionato delle loro reti, ma lo si utilizza per l'intera rete di produzione? La maggior parte di noi non è ancora pronta per un cambiamento così grande. Perché è così difficile mettere in atto IPv6? Poiché utilizziamo IPv4 praticamente dall'inizio dei tempi, è ciò che tutti conosciamo e comprendiamo, e non c'è davvero un grande bisogno di passare a IPv6 all'interno delle nostre reti. Apetta un minuto; Pensavo che ci fosse un grande spavento sull'esaurimento degli indirizzi IPv4? Sì, questo è vero per gli indirizzi IP sull'Internet pubblica, ma non ha nulla a che fare con le nostre reti interne. Vedete, anche se domani finissimo gli indirizzi IPv4 pubblici, le nostre reti interne alle nostre aziende non subiranno alcun impatto. Possiamo continuare a eseguire IPv4 all'interno della rete per molto tempo a venire, possibilmente per sempre e sempre, purché ci sentiamo a nostro agio nell'usare le tecnologie NAT per tradurre il traffico in IPv4 quando ci arriva da Internet. Usiamo tutti il NAT in una forma o nell'altra da quasi tutto il tempo in cui esiste IPv4, quindi è ovviamente qualcosa con cui le persone si sentono molto a loro agio.

Sia chiaro: non sto cercando di convincerti che attenersi a IPv4 è la via del futuro. Sto solo spiegando il fatto che, per la maggior parte delle organizzazioni nei prossimi anni, questa sarà semplicemente la verità. Il motivo per cui voglio parlare di IPv6 qui è che, alla fine, dovrai affrontarlo. E una volta fatto, ne sarai davvero entusiasta! Ci sono alcuni enormi vantaggi che IPv6 ha su IPv4, vale a dire, l'enorme numero di indirizzi IP che puoi contenere all'interno di una singola rete. I team di rete nelle aziende di tutto il mondo lottano ogni giorno con la necessità di costruire sempre più reti IPv4 e collegarle tra loro. Pensaci: ci sono molte aziende ora con un numero di dipendenti superiore a 10.000. Alcuni hanno molte, molte volte quel numero. Nel mondo di oggi, tutti hanno bisogno di un accesso quasi costante ai propri dati. I dati sono la nuova valuta. La maggior parte degli utenti ora ha almeno due dispositivi fisici che utilizza per il lavoro, a volte anche di più: un laptop e un tablet, o un laptop e uno smartphone, o un desktop e un laptop e un tablet e uno smartphone; hai l'idea. Nel mondo IPv4, dove hai a che fare con intervalli di indirizzi IP relativamente piccoli, devi essere molto creativo con la creazione di sottoreti per ospitare tutti questi dispositivi fisici, che hanno bisogno di un indirizzo IP univoco per comunicare sulla rete. Il più grande vantaggio di IPv6 è che risolve tutti questi problemi immediatamente e, per impostazione predefinita, fornendo la capacità di avere un numero enorme di indirizzi IP all'interno di una singola rete. Di quanti altri indirizzi stiamo parlando? Di seguito sono riportati alcuni dati di confronto per darti una piccola prospettiva: La maggior parte degli utenti ora ha almeno due dispositivi fisici che utilizza per il lavoro, a volte anche di più: un laptop e un tablet, o un laptop e uno smartphone, o un desktop e un laptop e un tablet e uno smartphone; hai l'idea. Nel mondo IPv4, dove hai a che fare con intervalli di indirizzi IP relativamente piccoli, devi essere molto creativo con la creazione di sottoreti per ospitare tutti questi dispositivi fisici, che hanno bisogno di un indirizzo IP univoco per comunicare sulla rete. Il più grande vantaggio di IPv6 è che risolve tutti questi problemi immediatamente e, per impostazione predefinita, fornendo la capacità di avere un numero enorme di indirizzi IP all'interno di una singola rete. Di quanti altri indirizzi stiamo parlando? Di seguito sono riportati alcuni dati di confronto per darti una piccola prospettiva: La

maggior parte degli utenti ora ha almeno due dispositivi fisici che utilizza per il lavoro, a volte anche di più: un laptop e un tablet, o un laptop e uno smartphone, o un desktop e un laptop e un tablet e uno smartphone; hai l'idea. Nel mondo IPv4, dove hai a che fare con intervalli di indirizzi IP relativamente piccoli, devi essere molto creativo con la creazione di sottoreti per ospitare tutti questi dispositivi fisici, che hanno bisogno di un indirizzo IP univoco per comunicare sulla rete. Il più grande vantaggio di IPv6 è che risolve tutti questi problemi immediatamente e, per impostazione predefinita, fornendo la capacità di avere un numero enorme di indirizzi IP all'interno di una singola rete. Di quanti altri indirizzi stiamo parlando? Di seguito sono riportati alcuni dati di confronto per darti una piccola prospettiva:

- Un indirizzo IPv4 è un indirizzo di lunghezza a 32 bit simile al seguente:

  192.168.1.5

- Un indirizzo IPv6 è un indirizzo di lunghezza di 128 bit simile a questo.

  2001: AABB: CCDD: AB00: 0123: 4567: 8901: ABCD

Come puoi vedere, l'indirizzo IPv4 è molto più breve, il che significa ovviamente che ci sono meno possibilità per indirizzi IP univoci. Quello che non vedi è quanto sono realmente più lunghi gli indirizzi IPv6. Questi esempi ritraggono gli indirizzi IPv4 e IPv6 come siamo abituati a vederli, nelle loro forme complete. In realtà, però, l'indirizzo IPv4 è mostrato in forma decimale e l'IPv6 in esadecimale. Gli indirizzi IPv6 vengono visualizzati e utilizzati tramite esadecimale in modo che gli indirizzi siano compressi il più possibile. In realtà, se si scava sotto il cofano, un indirizzo IPv6 nella sua forma nativa a 128 bit potrebbe assomigliare a questo (e in effetti, è così che appare all'interno del pacchetto effettivo):

00010000010000010000110110011000000000000000000010000000000000000
00010000000000000000000000001000000000000000000000000000000000001

È un insieme impressionante di cifre, ma non qualcosa di molto utilizzabile o amichevole per l'occhio umano. Quindi, invece di mostrare i bit, che dire di un indirizzo IPv6 mostrato in formato decimale, nello stesso modo in cui sono sempre stati mostrati gli indirizzi IPv4? In tal caso, un indirizzo IPv6 potrebbe essere simile a questo:

192.16.1.2.34.0.0.1.0.0.0.0.0.0.0.1

Ora comprendiamo appieno perché IPv6 viene sempre utilizzato e mostrato in esadecimale; gli indirizzi sono lunghi anche in quel formato compresso!

Comprensione degli indirizzi IP IPv6

Quando configuriamo reti IPv4, il subnetting è estremamente importante perché è ciò che ci consente di avere più di una raccolta di indirizzi IP all'interno della stessa rete. Nella forma più elementare di rete, in cui si impostano alcuni indirizzi IP e si esegue una sottorete / 24 (una maschera di sottorete di 255.255.255.0), che è molto comune su piccole reti come all'interno di una casa o di un limitato a 254 indirizzi IP univoci. Ahia! Alcune aziende hanno migliaia di server diversi, senza tenere conto di tutti i loro computer client e dispositivi che devono connettersi alla rete. Per fortuna, possiamo costruire molte sottoreti diverse all'interno di una singola rete IPv4 al fine di aumentare l'ambito del nostro indirizzo IP utilizzabile, ma ciò richiede un'attenta pianificazione e calcolo di tali sottoreti e spazi di indirizzi, ed è il motivo per cui ci affidiamo ad amministratori di rete esperti per gestire questa parte della rete per noi. Una configurazione di sottorete non valida in una tabella di instradamento può sovraccaricare il flusso del traffico di rete. L'amministrazione delle sottoreti in una grande rete IPv4 non è per i deboli di cuore.

Quando parliamo di indirizzamento IPv6, il cielo sembra quasi essere il limite. Se dovessi calcolare tutti gli indirizzi IPv6 univoci disponibili nello spazio precedente a 128 bit, scopriresti che sono disponibili più di 340 miliardi di indirizzi da creare. In altre parole, 340 trilioni, trilioni, trilioni di indirizzi. Questo è il numero che viene pubblicizzato sul

numero di indirizzi disponibili su Internet IPv6, ma cosa significa per le nostre reti interne?

Per discutere il numero di indirizzi che potremmo avere all'interno di una tipica rete interna che esegue IPv6, facciamo un primo passo indietro e guardiamo l'indirizzo stesso. L'indirizzo che ho mostrato in precedenza è solo qualcosa che ho inventato, ma ne scomporremo le parti qui:

2001: AABB: CCDD: AB00: 0123: 4567: 8901: ABCD

Rispetto a 192.168.1.5, questa cosa sembra una mostruosità. Questo perché generalmente non siamo abituati a trattare con il formato esadecimale; è solo un modo diverso di guardare i dati. Come accennato, questo è un indirizzo a 128 bit. È suddiviso in 8 diverse sezioni, ogni sezione separata da due punti è composta da 16 bit. I primi 64 bit (la prima metà) dell'indirizzo sono informazioni di instradamento e gli ultimi 64 bit sono l'ID dispositivo univoco sulla rete. Nella prima parte abbiamo due componenti differenti. I primi 48 bit (3 gruppi di esadecimali) sono un prefisso organizzativo che sarà lo stesso su tutti i nostri dispositivi nella rete. Quindi il quarto set di informazioni, i successivi 16 bit, può essere il nostro ID di sottorete. Questo ci dà la flessibilità di avere ancora molte sottoreti diverse se lo desideriamo in futuro, utilizzando più numeri qui come ID di sottorete. Dopo aver dedicato la prima metà dell'indirizzo, ora abbiamo la seconda metà con cui lavorare, gli ultimi 64 bit. Questi possiamo lasciare per gli ID dispositivo. Questa parte dell'indirizzo sarà diversa per ogni dispositivo sulla rete e definirà i singoli indirizzi IPv6 statici che verranno utilizzati per la comunicazione. Spieghiamo tutto. Prenderemo l'indirizzo di esempio dal precedente e lo suddivideremo nelle seguenti parti:

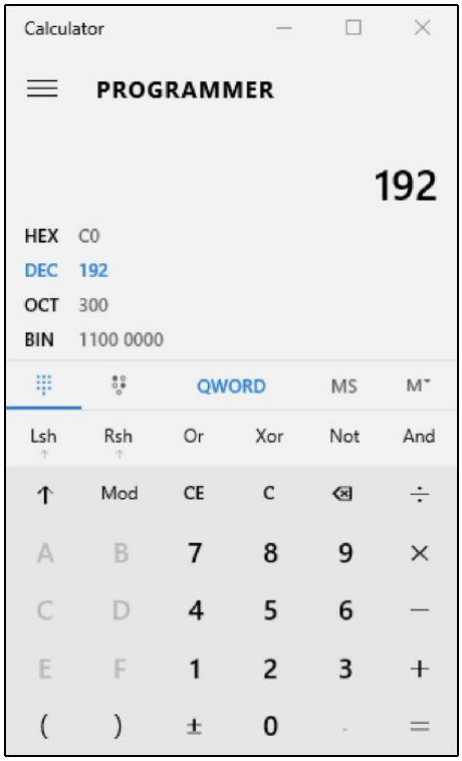
- **Prefisso organizzativo**: 2001: AABB: CCDD: AB00: 0123: 4567: 8901: ABCD
  dove 2001: AABB: CCDD è il prefisso organizzativo
- **ID sottorete**: 2001: AABB: CCDD: AB00: 0123: 4567: 8901: ABCD dove AB00 è il
  ID sottorete
- **Dispositivo**
  ID: 2001: AABB: CCDD: AB00: 0123: 4567: 8901: ABCD dove 0123: 4567: 8901
  : ABCD è un ID dispositivo univoco

Quanti dispositivi possiamo avere nella nostra rete con uno schema IP come questo? Bene, anche nel nostro esempio, dove abbiamo allocato solo una sezione a 16 bit per il subnetting e 64 bit per gli indirizzi IP effettivi, questo ci fornirebbe la capacità di avere più di 65.000 sottoreti e

quintilioni di ID dispositivo univoci nel nostro intervallo IP . Impressionante, non è vero?

Se ci atteniamo a questo e utilizziamo solo una singola sottorete per contenere tutte le nostre macchine, la prima metà dei nostri indirizzi sarà sempre la stessa, rendendo questi indirizzi lunghi molto più facili da ricordare e gestire. È sorprendente quanto velocemente ti abituerai a vedere questi grandi numeri esadecimali nel tuo ambiente, ma anche se inizierai a riconoscerli, probabilmente non salterai più rapidamente nei server o nei computer della tua rete usando lo statico Indirizzi IP. So che molti di noi hanno ancora l'abitudine di dire: devo passare rapidamente al mio server web, mi limiterò a RDP in 192.168.1.5. Il tempo necessario per digitare questi indirizzi IPv6, anche se li ricordi, generalmente non ne vale la pena. IPv6 porterà con sé una maggiore dipendenza da DHCP e DNS per renderlo più utilizzabile.

Ora che abbiamo capito quali sezioni dell'indirizzo verranno utilizzate per quali scopi, come possiamo assegnare i numeri ID dei singoli dispositivi per tutti i computer, server e altri dispositivi sulla nostra rete? Potresti iniziare con il numero 1 e salire da lì. Un'altra idea è calcolare i vecchi indirizzi IPv4 in esadecimale e usarli come gli ultimi 32 bit dell'indirizzo: apri la Calcolatrice di Windows sul tuo computer, apri il menu e cambialo in modalità Programmatore. Questo è uno strumento semplice e veloce che puoi utilizzare per convertire i decimali in esadecimali e viceversa. Prendiamo l'esempio del mio server web in esecuzione su 192.168.1.5. Voglio implementare IPv6 nella mia rete e voglio che gli indirizzi IPv6 del mio server riflettano l'indirizzo IPv4 originale nella sezione ID dispositivo del nuovo indirizzo. Nella mia calcolatrice,



Se lo facciamo con ciascuno degli ottetti nel nostro indirizzo IPv4, vedremo quanto segue:

192 = C0
168 = A8 1 = 01
5 = 05

Quindi il mio 192.168.1.5 calcola in C0A8: 0105. Ora posso utilizzarlo in combinazione conil mio prefisso organizzativo e il mio ID di sottorete per creare un indirizzo IPv6 statico per il mio server web:

2001: AABB: CCDD: 0001: 0000: 0000: C0A8: 0105

Noterai nell'indirizzo IPv6 precedente che ho inserito l'esadecimale per l'ID del dispositivo alla fine, ma ho anche apportato un paio di altre modifiche. Poiché stiamo lasciando gli ultimi 64 bit disponibili per l'ID del dispositivo, ma il mio vecchio indirizzo IPv4 consuma solo 32 bit, mi rimangono i 32 bit nel mezzo. Sarebbe un po 'strano avere dati lì che non significano nulla per noi, quindi faremo semplicemente tutti zeri per semplificare il mio schema di indirizzamento. Oltre a questa modifica, ho anche adattato l'ID della mia sottorete al numero 1, poiché questa è la prima sottorete nella mia rete.

Il nostro nuovo indirizzamento inizia a sembrare un po 'più pulito e ha più senso. Ora che vediamo questo nuovo indirizzo per il nostro server web impostato, posso vedere che ci sono alcune attività di pulizia aggiuntive che possiamo eseguire sull'indirizzo per renderlo ancora migliore. Al momento l'indirizzo elencato in precedenza è accurato al 100%. Potrei collegare questo indirizzo IP alle proprietà NIC del mio server web e funzionerebbe. Tuttavia, ci sono molti zeri nel mio indirizzo e non è necessario che li tenga tutti. Ogni volta che si hanno zeri non necessari all'interno di un segmento a 16 bit che precedono il numero effettivo, è possibile rimuoverli semplicemente. Ad esempio, il nostro ID di sottorete ei primi 32 bit del nostro ID dispositivo hanno molti zeri non necessari, quindi posso consolidare l'indirizzo come segue:

2001: AABB: CCDD: 1: 0: 0: C0A8: 0105

Quindi, per fare un ulteriore passo avanti, ogni volta che hai sezioni complete a 16 bit composte interamente da zeri, possono essere completamente consolidate in due punti doppi. Quindi, i primi 32 bit del mio ID dispositivo che sono tutti zeri, posso sostituirli con ::. Di seguito è riportato l'indirizzo completo e l'indirizzo consolidato. Questi numeri sembrano molto diversi. Il mio indirizzo consolidato è molto più facile agli occhi, ma dal punto di vista tecnologico sono esattamente lo stesso numero:

2001: AABB: CCDD: 0001: 0000: 0000: C0A8: 0105
2001: AABB: CCDD: 1 :: C0A8: 0105

In effetti, se stai configurando un laboratorio o desideri testare rapidamente IPv6, puoi utilizzare indirizzi semplici come il seguente esempio. I due indirizzi che ti mostrerò qui sono esattamente gli stessi:

2001: 0000: 0000: 0000: 0000: 0000: 0000: 0001
2001 :: 1

È importante notare che è possibile utilizzare solo due punti doppi una volta all'interno di un indirizzo IP. Se hai due punti in cui potrebbe essere applicabile all'interno dello stesso indirizzo, puoi implementarlo solo in uno di quei punti e dovrai precisare gli zeri nell'altro punto

Con le informazioni fornite qui, dovresti essere in grado di mettere insieme la tua parvenza di IPv6 e iniziare a rilasciare alcuni indirizzi IPv6 a computer o server nella tua rete. C'è così tanto da imparare su questo argomento che si potrebbe scrivere un libro intero, e in effetti molti l'hanno fatto.

La tua cassetta degli attrezzi di rete

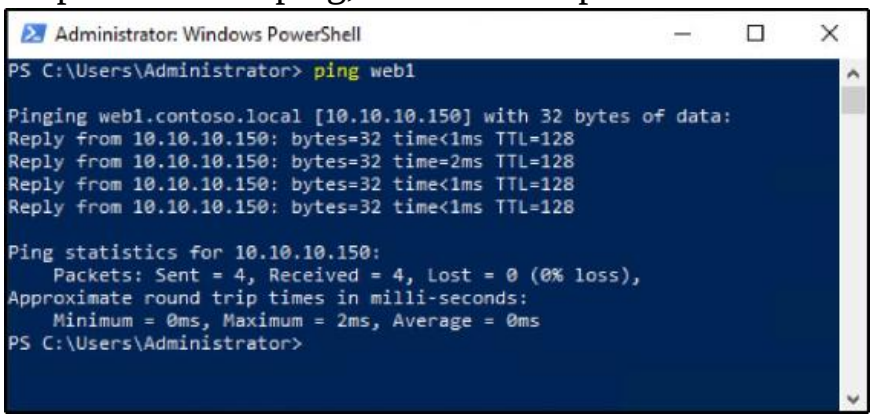
Che tu sia un amministratore di server, un amministratore di rete o una combinazione dei due, esistono numerosi strumenti utili per testare e monitorare le connessioni di rete nel mondo di Windows Server. Alcuni di questi strumenti sono integrati direttamente nel sistema operativo e possono essere utilizzati dal prompt dei comandi o da PowerShell, mentre altri sono interfacce grafiche più estese che richiedono l'installazione prima dell'esecuzione. I seguenti sono gli strumenti di rete che esamineremo:

- ping tracert
- pathping
- Connessione di prova
- telnet
- Test-NetConnection

Tutti questi strumenti sono gratuiti, quindi non hai scuse per ritardare la conoscenza di queste utili utilità.

ping

Anchei professionisti IT più recenti di solito hanno familiarità con questo. ping è un comando che puoi utilizzare da un prompt dei comandi o da PowerShell e viene semplicemente utilizzato per interrogare un nome DNS e / o un indirizzo IP per scoprire se risponde. Ping è ed è sempre stato il nostro strumento di riferimento per testare la connettività di rete tra due dispositivi su una rete. Dal mio client Windows 10 sulla LAN, posso aprire un prompt e inviare un ping a <IP_ADDRESS>.
In alternativa, poiché utilizzo il DNS nel mio ambiente, che risolverà i nomi in indirizzi IP, posso anche utilizzare ping <SERVERNAME>, come mostrato nell'esempio seguente. Puoi vedere che il mio server risponde al mio ping, facendomi sapere che è online e risponde:



Il traffico ping è tecnicamente chiamato traffico ICMP. Questo è importante perché ICMP è bloccato per impostazione predefinita sempre più spesso in questi giorni, con i firewall attivati per impostazione predefinita su così tanti dei nostri sistemi e dispositivi. Storicamente, il ping è sempre stato uno strumento su cui potevamo contare per dirci in modo abbastanza sicuro se la connettività scorreva tra due dispositivi, ma non è più così. Se costruisci una nuova scatola di Windows e la colleghi alla tua rete, quel computer potrebbe comunicare con Internet e tutti i server sulla tua rete senza problemi, ma se provi a eseguire il ping di quel nuovo computer da un'altra macchina sulla tua rete, il ping probabilmente fallirà. Perché sarebbe successo? Perché Windows ha alcune misure di sicurezza integrate per impostazione predefinita, incluso il blocco del traffico ICMP in Windows Firewall. In quel caso, è necessario disattivare

il firewall o fornirgli una regola di accesso che consenta il traffico ICMP. Una volta abilitata tale regola, i ping inizieranno a rispondere da questo nuovo computer. Tieni presente che ogni volta che crei nuovi sistemi o server nella tua rete, il ping non è sempre lo strumento più affidabile da cui dipendere nel mondo del networking di oggi.

È facile consentire le risposte ICMP collegando una regola a Windows Defender Firewall con sicurezza avanzata, anche se non vorrai comunque ricordarti di farlo manualmente su ogni nuovo sistema che introduci in una rete. Per fortuna, sai già come utilizzare Criteri di gruppo per creare un oggetto Criteri di gruppo e distribuirlo a tutte le macchine sulla tua rete, e sì, puoi assolutamente inserire regole del firewall all'interno di quel GPO. Questo è un modo comune per consentire o bloccare ICMP in un'intera organizzazione, emettendo una regola firewall tramite Criteri di gruppo.

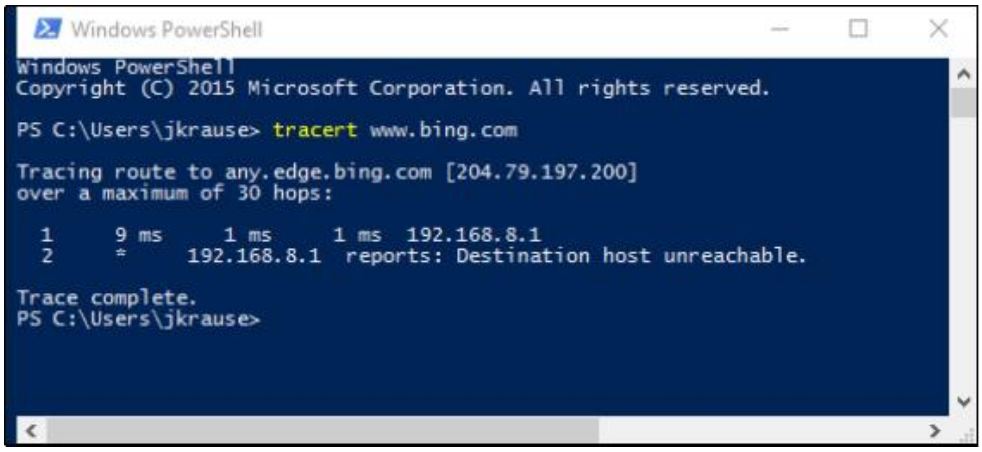
tracert

tracert, che si pronuncia Trace Route, è uno strumento utilizzato per tracciare un pacchetto di rete mentre attraversa la rete. Quello che fa davvero è guardare tutti i luoghi in cui il pacchetto si imbatte prima di raggiungere la sua destinazione. Questi ostacoli lungo la strada che un pacchetto di rete deve attraversare sono chiamati salti. Trace route mostra tutti i salti che il tuo traffico sta prendendo mentre si sposta verso il server di destinazione o qualunque cosa stia cercando di contattare. La rete del mio laboratorio di prova è molto piatta e noiosa, quindi fare un tracert l ì non ci mostrerebbe molto di niente. Tuttavia, se apro un prompt di PowerShell da una macchina connessa a Internet e traccio un servizio Web, come Bing, otteniamo alcuni risultati interessanti:

```
PS C:\WINDOWS\system32> tracert www.bing.com

Tracing route to any.edge.bing.com [204.79.197.200]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.8.1
  2     1 ms    <1 ms    <1 ms  192.168.128.1
  3     8 ms     7 ms     5 ms  172.17.224.1
  4    11 ms     9 ms    15 ms  172.19.253.1
  5    10 ms     9 ms    11 ms  172.31.255.1
  6    20 ms     9 ms    13 ms  htl-max1-1.iserv.net [206.114.55.1]
  7    15 ms    12 ms     8 ms  69.87.144.9
  8    23 ms    18 ms    19 ms  888-2.iserv.net [206.114.40.2]
  9    23 ms    20 ms    15 ms  g5-0-0.core3.grr.iserv.net [206.114.51.20]
 10    19 ms    11 ms    19 ms  g5-0-0.core1.grr.iserv.net [206.114.51.2]
 11    21 ms    28 ms    19 ms  GigabitEthernet4-1.GW5.DET5.ALTER.NET [152.179.10.81]
 12    25 ms    28 ms    28 ms  0.ae1.XL3.CHI13.ALTER.NET [140.222.225.179]
 13    27 ms    37 ms    54 ms  TenGigE0-6-0-1.GW2.CHI13.ALTER.NET [152.63.65.133]
 14    36 ms    34 ms    34 ms  microsoft-gw.customer.alter.net [152.179.105.130]
 15    58 ms    50 ms    46 ms  104.44.81.58
 16    34 ms    33 ms    36 ms  10.201.194.219
 17    26 ms    29 ms    29 ms  a-0001.a-msedge.net [204.79.197.200]

Trace complete.
PS C:\WINDOWS\system32>
```

Se utilizzi tracert ma non sono interessato a vedere tutte le informazioni DNS fornite nell'output, usa tracert -d per concentrarsi solo sul Indirizzi IP.

Queste informazioni possono essere estremamente utili quando si tenta di diagnosticare una connessione che non funziona. Se il tuo traffico si muove attraverso più salti, come router e firewall, prima di arrivare a destinazione, tracert può essere essenziale per capire dove nel flusso di connessione le cose stanno andando storte. Dato che lo screenshot precedente mostra un percorso di tracciamento riuscito a Bing, ora vediamo come appare quando le cose sono rotte. Scollegherò il mio router Internet ed eseguirò lo stesso tracertwww.bing.com di nuovo, e ora possiamo vedere che sono ancora in grado di comunicare con il mio router locale, ma non oltre:



pathping

tracert è utile e sembra essere il file *di fatto* standard per tracciare i pacchetti nella tua rete, ma questo prossimo comando è ancora più potente secondo me. pathping essenzialmente fa esattamente la stessa cosa di tracert, tranne per il fatto che fornisce una parte aggiuntiva di informazioni cruciali. Il più delle volte, con uno di questi comandi, sei interessato solo a capire dove nella catena di salti qualcosa è rotto, ma spesso quando imposto server per scopi di rete, sto lavorando con server e hardware che hanno molte schede di rete differenti. Quando si ha a che fare con più NIC in un sistema, la tabella di routing locale è importante tanto quanto i router e gli switch esterni e spesso desidero controllare il percorso di un pacchetto di rete per vedere da quale NIC locale esce. È qui che il pathping diventa più potente di tracert. La prima informazione

che tracert ti mostra è il primo salto lontano dal server locale che stai attraversando. Ma il pathping mostra anche da quale interfaccia di rete locale escono i tuoi pacchetti.

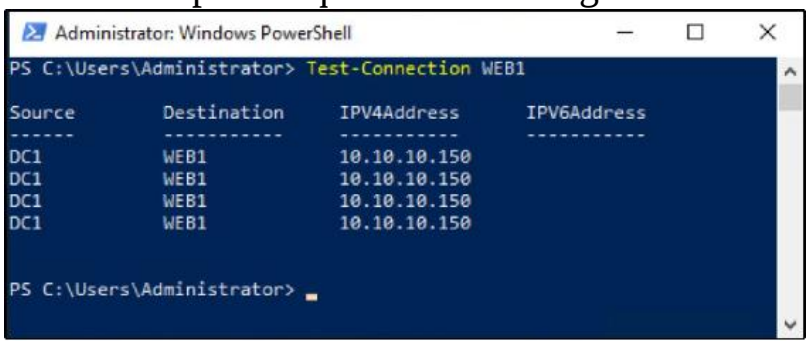
Faccio un esempio: spesso configuro server di accesso remoto con più NIC e durante questo processo creiamo molti percorsi sul server locale in modo che sappia quale traffico deve essere inviato in quale direzione, ad esempio quale traffico deve uscire dalla scheda di rete interna e il traffico necessario per uscire dalla scheda di rete esterna. Dopo aver completato tutte le nostre istruzioni di routing per la scheda di rete interna, le testiamo eseguendo un ping su un server all'interno della rete. Forse quel ping fallisce e non siamo sicuri del perché. Posso provare un comando tracert, ma non mi fornirà nulla di utile perché semplicemente non può vedere il primo salto, è semplicemente scaduto. Tuttavia, se provo invece un pathping, il primo hop scadrà ancora, ma ora posso vedere che il mio traffico sta tentando di fluire dalla mia NIC ESTERNA. Ops! Dobbiamo aver impostato qualcosa in modo errato con la nostra route statica su questo server. Quindi so che devo eliminare quel percorso e ricrearlo per fare in modo che questo traffico fluisca invece attraverso la NIC interna.

Quello che segue è lo stesso prompt di PowerShell dallo stesso computer che ho usato nello screenshot di Tracert. Puoi vedere che un pathping mi mostra l'indirizzo IP locale sul mio laptop in cui il traffico sta tentando di lasciare il sistema, mentre il comando tracert non ha mostrato queste informazioni:

```
PS C:\Users\jkrause> pathping www.bing.com

Tracing route to any.edge.bing.com [204.79.197.200]
over a maximum of 30 hops:
  0  IVO-PC-328 [192.168.8.113]
  1  192.168.8.1
  2  192.168.128.1
  3     *     192.168.8.1  reports: Destination host unreachable.

Computing statistics for 75 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           IVO-PC-328 [192.168.8.113]
                                    0/ 100 =  0%   |
  1    1ms     0/ 100 =  0%     0/ 100 =  0%  192.168.8.1
                                  100/ 100 =100%   |
  2  ---     100/ 100 =100%     0/ 100 =  0%  192.168.128.1
                                    0/ 100 =  0%   |
  3  ---     100/ 100 =100%     0/ 100 =  0%  IVO-PC-328 [0.0.0.0]

Trace complete.
PS C:\Users\jkrause>
```

Connessione di prova

I comandi che abbiamo discusso finora possono essere eseguiti dal prompt dei comandi o da PowerShell, ma ora è il momento di immergersi in uno più recente che può essere eseguito solo dal prompt di PowerShell: un cmdlet chiamato Test-Connection; è una specie di ping con gli steroidi. Se apriamo un prompt di PowerShell in laboratorio ed eseguiamo Test-Connection WEB1, otteniamo un output molto simile a quello che otterremmo con un ping regolare, ma le informazioni sono disposte in un modo che penso sia un po 'più facile per gli occhi. C'è anche una colonna di dati inaspettata qui chiamata Sorgente:



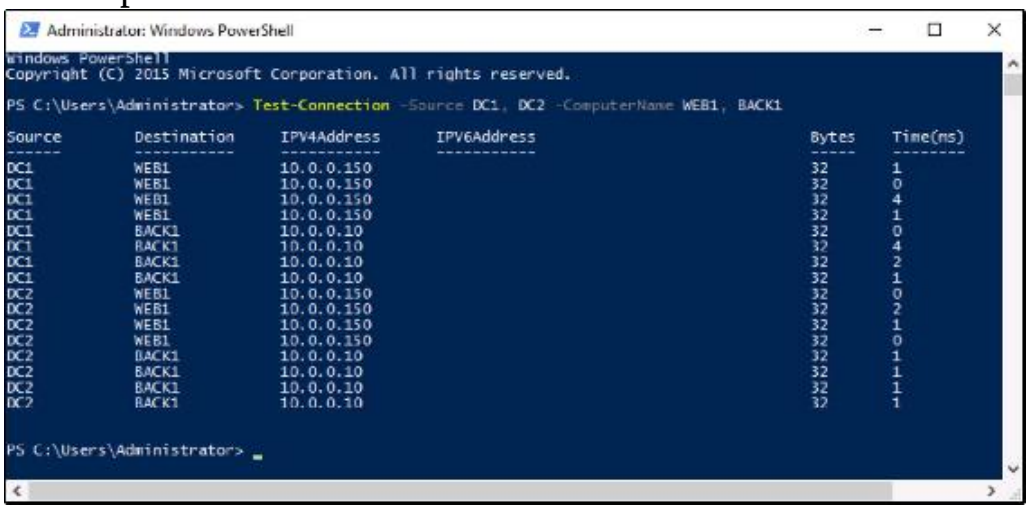
È interessante. Ero connesso al mio server DC1 quando ho eseguito questo comando, quindi il mio computer di origine per questo comando era DC1. Ma questo significa che ho la possibilità di manipolare il computer di origine per il cmdlet Test-Connection? Sì, questo è esattamente ciò che significa. Come per tutto nella gestione di Windows Server 2019, la necessità di essere connessi a un server locale è disaccoppiata. Specifico per il cmdlet Test-Connection, ciò significa che hai la possibilità di aprire un prompt di PowerShell ovunque sulla rete e di testare le connessioni tra due diversi endpoint, anche se non hai effettuato l'accesso a nessuno di essi. Proviamolo.

Sono ancora connesso al mio server DC1, ma userò un cmdlet Test-Connection in per testare le connessioni tra un certo numero di miei server nella rete. Vedete, non solo è possibile specificare un computer di origine diverso da quello a cui si è attualmente connessi, ma è anche possibile fare un ulteriore passo avanti e specificare più origini e destinazioni con questo potente cmdlet. Quindi, se voglio testare le

connessioni da un paio di macchine sorgente diverse a un paio di destinazioni diverse, è facile farlo con il seguente comando:

Test-connessione -Sorgente DC1, DC2 -ComputerName WEB1, BACK1

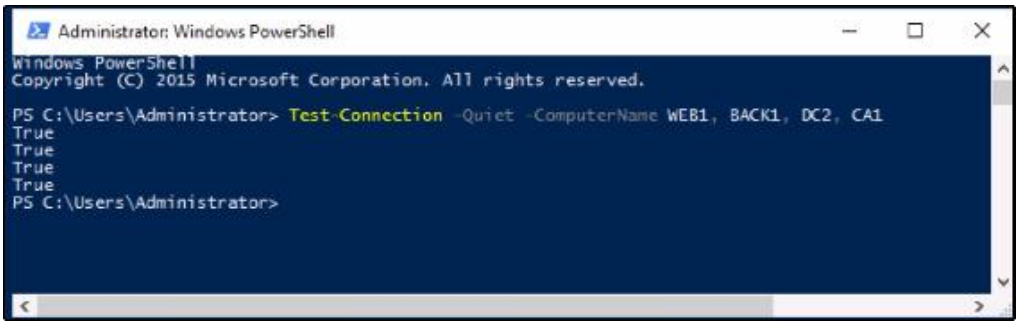
voiNella schermata seguente posso vedere che ho statistiche di ping da DC1 e DC2, a ciascuno dei server WEB1 e BACK1 nella mia rete. Test-Connection ha il potenziale per essere uno strumento di monitoraggio molto potente:



Un'altra funzione utile da sottolineare è che puoi ripulire l'output del comando abbastanza facilmente usando l'opzione -Quiet. Aggiungendo -Quiet a un comando Test-Connection, disinfetta l'output e mostra solo un semplice True o False per verificare se la connessione ha avuto successo, invece di mostrare ogni singolo pacchetto ICMP che è stato inviato. Sfortunatamente, non puoi combinare sia lo switch -Source che lo switch -Quiet, ma se stai usando Test-Connection dal computer di origine originale a cui hai effettuato l'accesso, come la maggior parte di noi farà comunque, Quiet funziona alla grande. La maggior parte delle volte, tutto ciò che ci interessa davvero è Sì o No sul fatto che queste connessioni funzionino e non vogliamo necessariamente vedere tutti e quattro i tentativi. Usando -Quiet otteniamo esattamente questo:

Test-Connection -Quiet -ComputerName WEB1, BACK1, DC2, CA1

Se dovessi utilizzare Test-Connection nel modo standard per provare a contattare tutti i server in formato la mia rete, che si trasformerebbe in un bel po 'di output. Ma utilizzando l'opzione -Quiet, ottengo un semplice True o False se ogni singolo server può essere contattato:



telnet

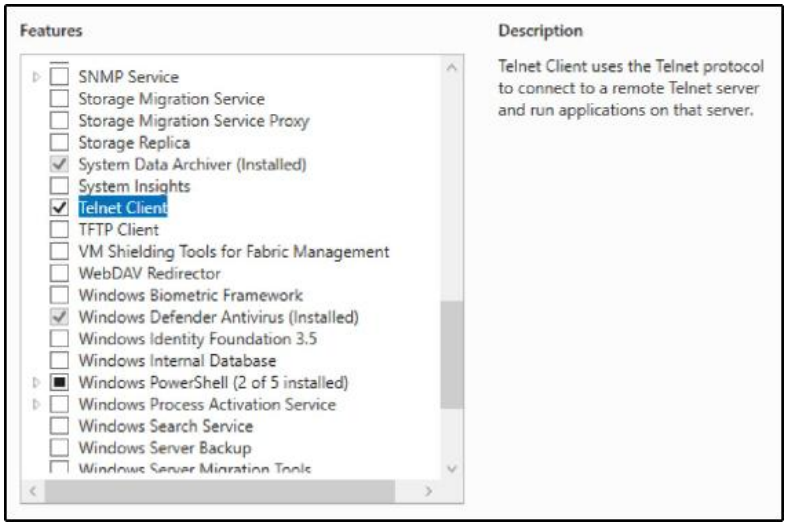
telnet fornisce un bel po 'di a distanza gestione capacità; esso essenzialmente offerte il capacità di stabilire una connessione tra due computer per manipolare la macchina remota tramite una connessione terminale virtuale. Sorprendentemente, non siamo qui per discutere nessuna delle funzionalità effettive fornite da telnet, perché per quanto riguarda il networking trovo che sia abbastanza utile come semplice strumento di verifica della connessione, senza sapere nulla di quale funzionalità il comando telnet stesso fornisce effettivamente.

Quando abbiamo discusso del ping, abbiamo parlato dello svantaggio di ICMP: è facilmente bloccabile e sta diventando sempre più comune nelle reti odierne non consentire che i ping abbiano successo. Questo è un peccato poiché il ping è sempre stato la forma più comune di test della connessione di rete, ma la realtà è che, se il ping rende più facile la nostra vita, rende anche più facile la vita degli hacker. Se non possiamo fare affidamento sul ping per dirci con certezza se possiamo contattare un sistema remoto, cosa usiamo invece? Un altro caso che vedo spesso è dove un server stesso potrebbe rispondere correttamente, ma un particolare servizio in esecuzione su quel server ha un problema e non risponde. Un semplice ping può mostrare che il server è online, ma non può dirci nulla in particolare sul servizio. Utilizzando i comandi del client Telnet, possiamo facilmente interrogare un server da remoto. Ancora più importante, possiamo scegliere di interrogare un singolo servizio su quel server, per assicurarci che sia in ascolto come previsto. Lascia che ti

faccia un esempio che uso sempre. Ho spesso configurato nuovi server web con connessione a Internet.

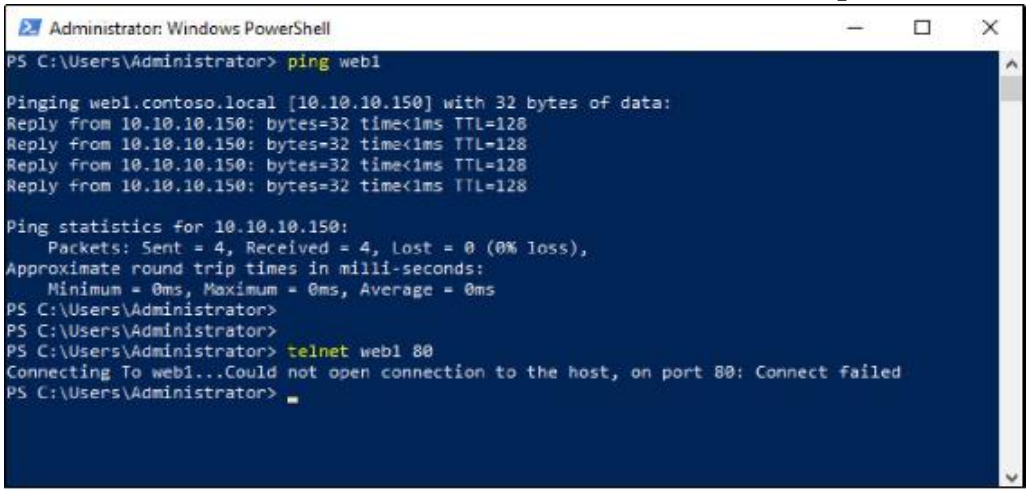
Dopo aver installato un nuovo server Web, è logico che io voglia testare l'accesso ad esso da Internet per assicurarmi che risponda, giusto? Ma forse il sito Web stesso non è ancora online e funzionante, quindi non posso accedervi con Internet Explorer. È molto probabile che abbiamo disabilitato i ping su questo server oa livello di firewall, perché il blocco di ICMP su Internet è molto comune per ridurre l'impronta di vulnerabilità della sicurezza sul web. Quindi il mio nuovo server è in esecuzione e pensiamo di avere la rete completamente quadrata, ma non posso testare il ping del mio nuovo server perché, per impostazione predefinita, non riesce a rispondere. Cosa posso usare per testarlo? telnet. Emettendo un semplice comando telnet, posso dire al mio computer di interrogare una porta specifica sul mio nuovo server web e scoprire se si connette a quella porta. In questo modo viene stabilita una connessione socket alla porta su quel server, che è molto più simile al traffico utente reale di quanto non sarebbe un ping. Se un comando telnet si connette correttamente, sai che il tuo traffico si sta dirigendo verso il server e il servizio del server in esecuzione sulla porta che abbiamo interrogato sembra rispondere correttamente.

La possibilità di utilizzare Telnet non è installata per impostazione predefinita in Windows Server 2019 o in qualsiasi sistema operativo Windows, quindi dobbiamo prima accedere a Server Manager e Aggiungi ruoli e funzionalità per installare la funzionalità chiamata Telnet Client:

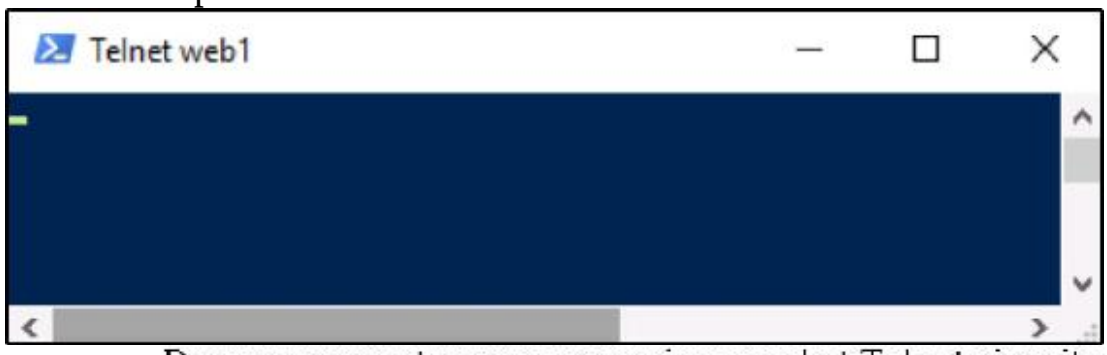


È sufficiente installare il client Telnet sulla macchina da cui si desidera eseguire il test della riga di comando. Non è necessario eseguire alcuna operazione sul server remoto a cui ci si connette.

Ora che la funzionalità del client Telnet è stata installata, possiamo utilizzarla da un prompt dei comandi o da PowerShell per lavorare per noi, tentando di effettuare connessioni socket dal nostro computer al servizio remoto. Tutto quello che dobbiamo fare è dirgli quale server e quale porta interrogare. Quindi telnet si collegherà semplicemente o andrà in timeout e, in base a quel risultato, possiamo vedere se quel particolare servizio sul server sta rispondendo. Proviamolo con il nostro server web. Per il nostro esempio ho disattivato il sito Web all'interno di IIS, quindi ora siamo nella posizione in cui il server è online ma il sito Web è morto. Se eseguo un ping su WEB1, posso ancora vederlo rispondere felicemente. Puoi vedere dove gli strumenti di monitoraggio del server che si basano su ICMP potrebbero mostrare falsi positivi, indicando che il server era online e in esecuzione, anche se il nostro sito web è inaccessibile. Appena sotto il ping riuscito nello screenshot seguente, puoi vedere che ho anche provato a interrogare la porta 80 sul server WEB1. Il comando che ho usato per questo è telnet web1 80. Che è scaduto. Questo ci mostra che il sito Web, che è in esecuzione sulla porta 80, non risponde:



Se riaccendo il sito web, possiamo prova di nuovo telnet web1 80 e questa volta non ricevo un messaggio di timeout. Questa volta, il mio prompt di PowerShell si pulisce da solo e rimane in attesa su un cursore lampeggiante in alto. Anche se non mi dice yay, sono connesso !, questo cursore lampeggiante indica che è stata stabilita una connessione socket con successo alla porta 80 sul mio server web, indicando che il sito web è online e risponde:



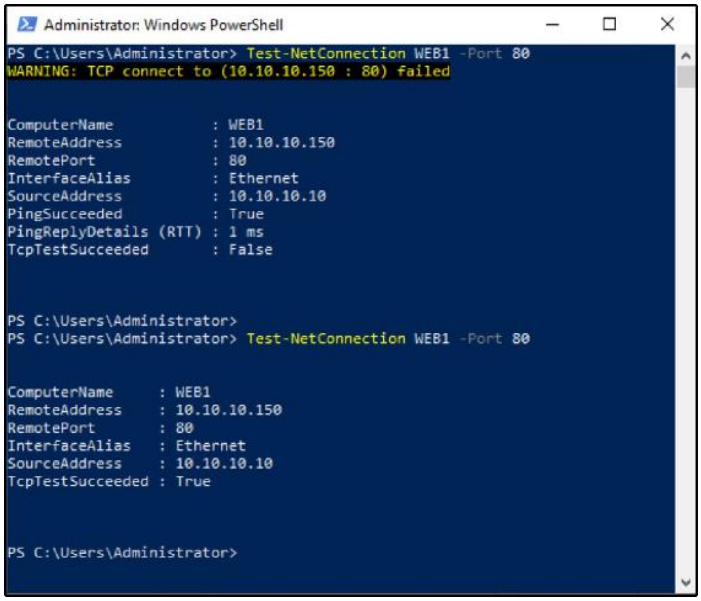
Dopo aver creato una connessione socket Telnet riuscita, potresti chiederti come tornare alla normale interfaccia di PowerShell. Premi contemporaneamente i tasti Ctrl +] (il secondo è un tasto parentesi quadra chiusa, di solito accanto al tasto barra rovesciata sulla tastiera), digita la parolasmetterec quindi premere INVIO. Questo dovrebbe riportarti a un prompt

Test-NetConnection

Se ping ha un cmdlet PowerShell equivalente e migliorato chiamato Test-Connection, PowerShell contiene anche uno strumento migliorato che funziona in modo simile a telnet per testare le connessioni socket alle risorse? Certo che lo fa. Test-NetConnection è un altro modo per interrogare particolari porte o servizi su un sistema remoto e l'output visualizzato è più amichevole di quello di Telnet.

Esaminiamo gli stessi test, una volta interrogando di nuovo la porta 80 su WEB1. Puoi vedere nello screenshot seguente che ho eseguito il comando due volte. La prima volta che il sito Web su WEB1 è stato disabilitato e la mia connessione alla porta 80 non è riuscita. La seconda volta, ho riattivato il sito Web e ora vedo una connessione riuscita.

Test-NetConnection WEB1 -Port 80



Traccia dei pacchetti con Wireshark o Message Analyzer

Alla fine, potresti dover esaminare un po 'più a fondo i tuoi pacchetti di rete. Ora stiamo entrando in un territorio in cui potrebbe essere coinvolto anche il tuo team di rete, ma se hai familiarità con questi strumenti, potresti essere in grado di risolvere il problema prima di dover chiamare l'assistenza. L'uso di strumenti della riga di comando per controllare lo stato di server e servizi è molto utile, ma a volte potrebbe non essere sufficiente. Ad esempio, hai un'applicazione client che non si connette al server delle applicazioni, ma non sai perché. Utilità come ping e persino telnet potrebbero essere in grado di connettersi correttamente, indicando che il routing di rete è impostato correttamente, ma l'applicazione non riesce a connettersi quando si apre. Se i log degli eventi dell'applicazione non ti aiutano a risolvere i problemi che sta succedendo,

È qui che tornano utili gli strumenti Wireshark e Message Analyzer. Entrambi sono gratuiti e facilmente scaricabili e svolgono sostanzialmente le stesse funzioni. Sono progettati per catturare il traffico di rete mentre parte da o arriva a un sistema e acquisiscono le informazioni che si trovano all'interno dei pacchetti stessi in modo che tu possa dare uno sguardo più approfondito a ciò che sta accadendo. Nel nostro esempio di un'applicazione che non può connettersi, è possibile eseguire uno di questi strumenti sul computer client per controllare il traffico in uscita e anche sul server delle applicazioni per controllare il traffico in entrata dal client.

Ogni strumento ha un bel po 'di funzionalità individuali e non abbiamo lo spazio per coprirlo tutto qui, quindi ti lascerò con i collegamenti da cui ottenere questi strumenti in modo che tu possa provarli tu stesso:

- **Wireshark**: https: //www.WireShark.org /Scarica.html
- **Microsoft Message Analyzer**: https: //www.microsoft.com /en-noi/Scarica/dettagli.aspx?id =44226

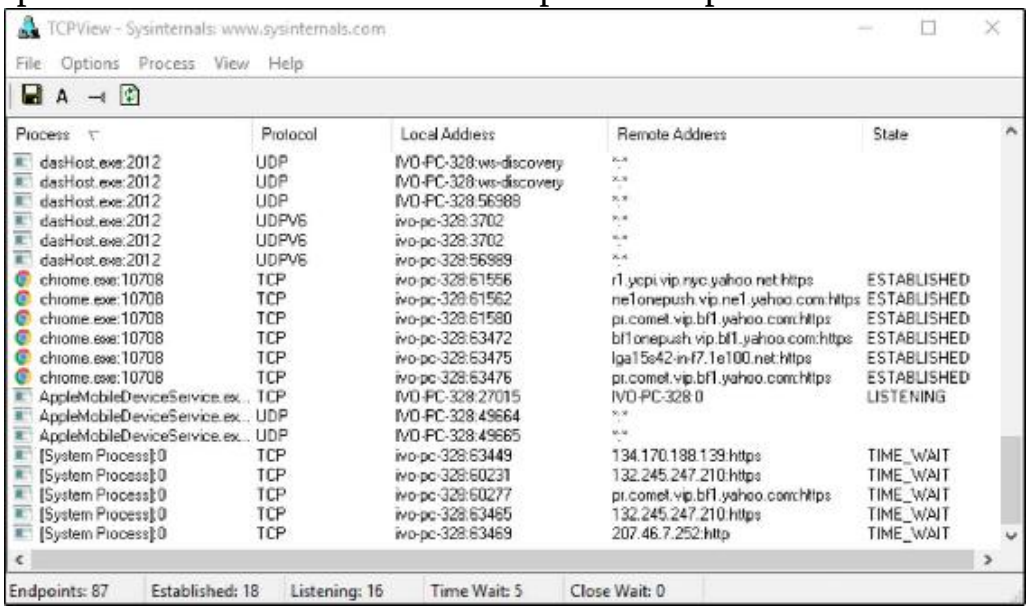
TCPView

Gli strumenti di cui abbiamo discusso finora sono fantastici e possono essere utilizzati quotidianamente per cercare e stimolare le singole risorse che vuoi testare, ma a volte ci sono situazioni in cui devi fare un passo indietro e capire cosa stai cercando in primo luogo. Forse stai lavorando con un'applicazione su un computer e non sei sicuro di quale server stia parlando. O forse sospetti che una macchina abbia un virus e cerchi di telefonare a casa da qualche parte su Internet e vorresti identificare la posizione con cui sta cercando di parlare o il processo che sta effettuando la chiamata. In queste situazioni, sarebbe utile se ci fosse uno strumento da avviare sul computer locale che mostra tutti i flussi di traffico di rete attivi su questo computer o server, in modo chiaro e conciso. Questo è esattamente ciò che fa TCPView. TCPView è uno strumento originariamente creato da Sysinternals; potresti aver sentito parlare di alcuni dei loro altri strumenti, come ProcMon e FileMon. L'esecuzione di TCPView su una macchina mostra in tempo reale tutte le connessioni TCP

e UDP attive che avvengono su quel computer. Altrettanto importante è il fatto che non è necessario installare nulla per far funzionare TCPView; è un eseguibile autonomo, che lo rende estremamente facile da usare e da pulire una volta terminato.

Puoi scaricare TCPView
a partire dal https://technet.microsoft.com/en-us/sysinternals/tcpview.aspx.

Copia semplicemente il file su un computer o server che desideri monitorare e fai doppio clic su di esso. Quello che segue è uno screenshot dell'interfaccia TCPView in esecuzione sul mio computer locale, che mostra tutte le connessioni che Windows e le mie applicazioni stanno attualmente effettuando. Puoi mettere in pausa questo output per dare un'occhiata più da vicino e puoi anche impostare filtri per ridurre i dati e trovare ciò che stai veramente cercando. I filtri eliminano il rumore, per così dire, e ti consentono di osservare più da vicino una particolare destinazione o un ID processo specifico:



Costruire una tabella di instradamento

Quando si sente il termine tabella di routing, è facile farlo passare come qualcosa di cui gli utenti della rete devono occuparsi, qualcosa che è configurato all'interno dei router e dei firewall di rete. Non si applica agli amministratori del server, giusto? Il collegamento in rete dei server è stato reso piuttosto semplice per noi richiedendo solo un indirizzo IP, una maschera di sottorete e un gateway predefinito e possiamo comunicare istantaneamente con tutto all'interno del resto della nostra rete. Sebbene ci sia davvero molta magia di rete in corso sotto il cofano che ci è stata fornita dalle apparecchiature di rete e dagli amministratori di rete, è importante capire come funziona il routing all'interno di Windows perché ci saranno alcuni casi in cui sarà necessario modificare o costruire una tabella di routing direttamente su un server Windows stesso.

Server multi-homed

L'esecuzione di server multi-homed è un caso in cui avresti sicuramente bisogno di capire e lavorare con una tabella di routing di Windows locale, quindi iniziamo da qui. Se pensi che questo non si applichi a te perché non hai mai sentito parlare di multi-homed prima, ripensaci. Multi-homed è solo una parola dall'aspetto divertente che significa che il tuo server ha più di una NIC. Questo potrebbe certamente essere il tuo caso, anche se sei un piccolo negozio che non ha molti server. Spesso i server Small Business o Essentials dispongono di più interfacce di rete, che separano il traffico interno da quello Internet. Un'altra istanza di un server multi-homed sarebbe un server di accesso remoto che fornisce funzionalità DirectAccess, VPN o proxy ai margini della rete. Un altro motivo per essere interessati e comprendere il multi-homing sono i server Hyper-V.

Ora che abbiamo stabilito cos'è un server multi-homed, potresti ancora chiederti perché ne stiamo discutendo. Se ho più di un NIC, non configuro semplicemente ogni NIC individualmente all'interno di Windows, dando a ciascuno un indirizzo IP, proprio come farei per qualsiasi NIC su qualsiasi server? Sì e no. Sì, configuri un indirizzo IP su ogni NIC, perché ne ha bisogno per l'identificazione e il trasporto dei pacchetti sulla rete. No, non si impostano tutte le NIC sul server nello stesso modo. C'è un elemento critico che devi tenere a mente e rispettare per fare in modo che il traffico fluisca correttamente sul tuo server multihomed.

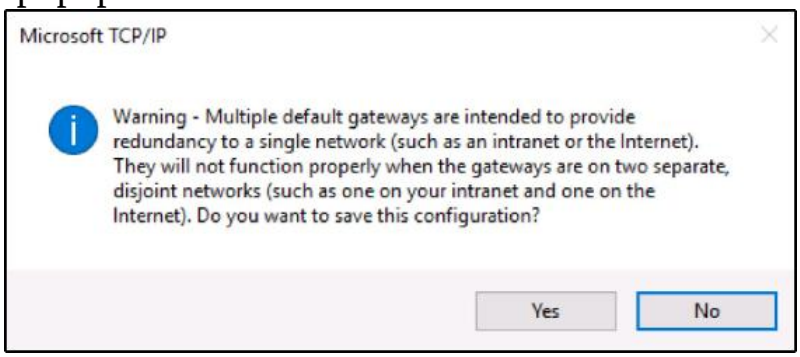
Un solo gateway predefinito

Questo è il biglietto d'oro. Quando si esegue la multi-home di un server con più NIC, è possibile avere un solo gateway predefinito. Uno per l'intero server. Ciò significa che avrai una NIC con un gateway predefinito e una o più NIC che NON hanno un gateway predefinito nelle loro impostazioni TCP / IP. Questo è estremamente importante. Lo scopo di un gateway predefinito è quello di essere il percorso di ultima risorsa. Quando Windows vuole inviare un pacchetto a una destinazione, esplora la tabella di instradamento locale (sì, c'è una tabella di instradamento

anche se non l'hai configurata o non l'hai mai guardata) e controlla se si tratta di una rotta statica specifica esiste per la sottorete di destinazione in cui deve andare questo pacchetto. Se esiste un percorso, spara il pacchetto a tale percorso e l'interfaccia di rete verso la destinazione. Se non esiste alcuna route statica nella tabella di routing, ricade sull'utilizzo del gateway predefinito e invia il traffico a quell'indirizzo del gateway predefinito. Su tutti i singoli server NIC, il gateway predefinito è un router designato con tutte le informazioni di instradamento per la rete, quindi il server lo passa semplicemente al router e il router fa il resto del lavoro.

Quando abbiamo più NIC su un server Windows, non possiamo assegnare a ciascuno un gateway predefinito perché confonderà il flusso di traffico dal tuo server. Sarà un gioco da ragazzi su quale flusso di traffico del gateway predefinito scorre con ogni trasmissione di rete. Ho aiutato molte persone a risolvere i problemi dei server sul campo esattamente con questo problema. Avevano bisogno di utilizzare il loro server come ponte tra due reti o di collegare il server a più reti diverse per qualsiasi motivo, e ora stanno lottando perché a volte il traffico sembra funzionare, a volte no. Iniziamo a esaminare le proprietà NIC solo per scoprire che ogni NIC ha il proprio indirizzo gateway predefinito nelle proprietà TCP / IP. Bingo, questo è il nostro problema. Il sistema è completamente confuso quando tenta di inviare traffico, perché non lo fa

Se hai mai provato ad aggiungere gateway predefiniti a più di una scheda NIC sullo stesso server, probabilmente hai familiarità con il prompt di avviso che viene visualizzato quando lo fai. Proviamolo. Ho aggiunto un altro NIC a uno dei miei server e ho configurato le impostazioni IP solo su uno dei NIC. Ora aggiungerò un nuovo indirizzo IP, una subnet mask e un gateway predefinito alla mia seconda NIC. Quando faccio clic sul pulsante OK per salvare tali modifiche, viene visualizzato il seguente popup:



Questo è uno di quegli avvertimenti che è facile interpretare male a causa della sua natura leggermente criptica, ma ne capisci l'essenza: procedi a tuo rischio e pericolo! E poi cosa fa la maggior parte degli amministratori a questo punto? Basta fare clic su di esso e salvare comunque le modifiche. Quindi iniziano i problemi di routing. Forse non oggi, ma forse la prossima volta che riavvierai quel server, o forse tre settimane

dopo, ma a un certo punto il tuo server inizierà a inviare pacchetti alle destinazioni sbagliate e ti causerà problemi.

Costruire un percorso

Allora qual è la nostra risposta a tutto questo? Costruire una tabella di instradamento statica. Quando si dispone di più NIC su un server, rendendolo quindi multi-homed, è necessario indicare a Windows quale NIC utilizzare per quale traffico all'interno della tabella di routing. In questo modo, quando il traffico di rete deve lasciare il server per una particolare destinazione, la tabella di instradamento è a conoscenza delle diverse direzioni e percorsi che il traffico dovrà prendere per arrivarci e lo invierà di conseguenza. Continuerai a fare affidamento sui router per portare il traffico per il resto del percorso, ma portare i pacchetti al router corretto inviandoli tramite l'appropriato NIC fisico è la chiave per assicurarti che il traffico fluisca rapidamente e in modo appropriato dal tuo multi-homed server.

Ora che abbiamo capito perché la tabella di instradamento è importante e concettualmente come dobbiamo usarla, approfondiamo e aggiungiamo un paio di rotte sul mio server dual-NIC. Aggiungeremo un percorso utilizzando il prompt dei comandi e ne aggiungeremo anche uno utilizzando PowerShell, poiché è possibile eseguire questa attività da entrambe le piattaforme, ma la sintassi utilizzata è diversa a seconda di quale si preferisce.

Aggiunta di una rotta con il prompt dei comandi

Prima di poter pianificare il nostro nuovo percorso, dobbiamo ottenere la disposizione del terreno per l'attuale configurazione di rete su questo server. Ha due NIC: uno è collegato alla mia rete interna e uno è collegato alla mia DMZ che si affaccia su Internet. Poiché posso avere solo un indirizzo gateway predefinito, va sulla scheda NIC DMZ perché non è possibile aggiungere percorsi per ogni sottorete che potrebbe dover essere contattata su Internet. Mettendo il gateway predefinito sul mio NIC DMZ, il NIC interno non ha un gateway predefinito ed è molto limitato in ciò che può contattare al momento. La sottorete interna a cui sono fisicamente

collegato è 10.10.10.0/24, quindi al momento posso contattare qualsiasi cosa in questa piccola rete da 10.10.10.1 a 10.10.10.254. Questo è noto come percorso sul collegamento; poiché sono collegato direttamente a questa sottorete, il mio server sa automaticamente come instradare il traffico all'interno di questa sottorete. Ma al momento non posso contattare nient'altro tramite il mio NIC interno, perché la tabella di instradamento non sa nulla delle altre sottoreti che ho all'interno della mia rete interna. Ad esempio, ho una sottorete aggiuntiva, 192.168.16.0/24, e ci sono alcuni server in esecuzione all'interno di questa sottorete che devo essere in grado di contattare da questo nuovo server. Se dovessi provare a contattare uno di quei server in questo momento, i pacchetti sparirebbero dalla mia NIC DMZ, perché la tabella di instradamento sul mio server non ha idea di come gestire il traffico 192.168, quindi lo invierebbe verso l'impostazione predefinita gateway. Quella che segue è la sintassi generale dell'istruzione route che dobbiamo seguire per far fluire questo traffico dal nostro server alla nuova sottorete: Ma al momento non posso contattare nient'altro tramite il mio NIC interno, perché la tabella di instradamento non sa nulla delle altre sottoreti che ho all'interno della mia rete interna. Ad esempio, ho una sottorete aggiuntiva, 192.168.16.0/24, e ci sono alcuni server in esecuzione all'interno di questa sottorete che devo essere in grado di contattare da questo nuovo server. Se dovessi provare a contattare uno di quei server in questo momento, i pacchetti sparirebbero dalla mia NIC DMZ, perché la tabella di instradamento sul mio server non ha idea di come gestire il traffico 192.168, quindi lo invierebbe verso l'impostazione predefinita gateway. Quella che segue è la sintassi generale dell'istruzione route che dobbiamo seguire per far fluire questo traffico dal nostro server alla nuova sottorete: Ma al momento non posso contattare nient'altro tramite il mio NIC interno, perché la tabella di instradamento non sa nulla delle altre sottoreti che ho all'interno della mia rete interna. Ad esempio, ho una sottorete aggiuntiva, 192.168.16.0/24, e ci sono alcuni server in esecuzione all'interno di questa sottorete che devo essere in grado di contattare da questo nuovo server. Se dovessi provare a contattare uno di quei server in questo momento, i pacchetti sparirebbero dalla mia NIC DMZ, perché la tabella di instradamento sul mio server non ha idea di come gestire il traffico 192.168, quindi lo invierebbe verso l'impostazione predefinita gateway. Quella che segue è la sintassi generale

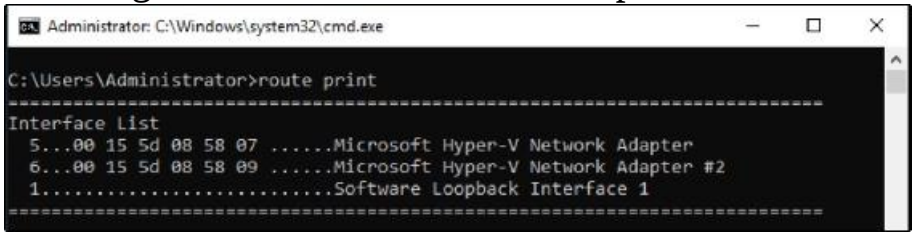
dell'istruzione route che dobbiamo seguire per far fluire questo traffico dal nostro server alla nuova sottorete: perché la tabella di instradamento non sa nulla delle altre sottoreti che ho all'interno della mia rete interna. Ad esempio, ho una sottorete aggiuntiva, 192.168.16.0/24, e ci sono alcuni server in esecuzione all'interno di questa sottorete che devo essere in grado di contattare da questo nuovo server. Se dovessi provare a contattare uno di quei server in questo momento, i pacchetti sparirebbero dalla mia NIC DMZ, perché la tabella di instradamento sul mio server non ha idea di come gestire il traffico 192.168, quindi lo invierebbe verso l'impostazione predefinita gateway. Quella che segue è la sintassi generale dell'istruzione route che dobbiamo seguire per far fluire questo traffico dal nostro server alla nuova sottorete: perché la tabella di instradamento non sa nulla delle altre sottoreti che ho all'interno della mia rete interna. Ad esempio, ho una sottorete aggiuntiva, 192.168.16.0/24, e ci sono alcuni server in esecuzione all'interno di questa sottorete che devo essere in grado di contattare da questo nuovo server. Se dovessi provare a contattare uno di quei server in questo momento, i pacchetti sparirebbero dalla mia NIC DMZ, perché la tabella di instradamento sul mio server non ha idea di come gestire il traffico 192.168, quindi lo invierebbe verso l'impostazione predefinita gateway. Quella che segue è la sintassi generale dell'istruzione route che dobbiamo seguire per far fluire questo traffico dal nostro server alla nuova sottorete: e ci sono alcuni server in esecuzione all'interno di questa sottorete che devo essere in grado di contattare da questo nuovo server. Se dovessi provare a contattare uno di quei server in questo momento, i pacchetti sparirebbero dalla mia NIC DMZ, perché la tabella di instradamento sul mio server non ha idea di come gestire il traffico 192.168 e quindi lo invierebbe verso l'impostazione predefinita gateway. Quella che segue è la sintassi generale dell'istruzione route che dobbiamo seguire per far fluire questo traffico dal nostro server alla nuova sottorete: e ci sono alcuni server in esecuzione all'interno di questa sottorete che devo essere in grado di contattare da questo nuovo server. Se dovessi provare a contattare uno di quei server in questo momento, i pacchetti sparirebbero dalla mia NIC DMZ, perché la tabella di instradamento sul mio server non ha idea di come gestire il traffico 192.168 e quindi lo invierebbe verso l'impostazione predefinita gateway.

Quella che segue è la sintassi generale dell'istruzione route che dobbiamo seguire per far fluire questo traffico dal nostro server alla nuova sottorete:

Route add -p <SUBNET_ID> mask <SUBNET_MASK> <GATEWAY> IF <INTERFACE_ID>

Primapossiamo digitare la nostra dichiarazione di route univoca per aggiungere la rete 192.168, dobbiamo fare un piccolo lavoro di investigazione e capire cosa useremo in questi campi. Di seguito è riportato un elenco delle parti e dei pezzi necessari per creare un'istruzione di route:

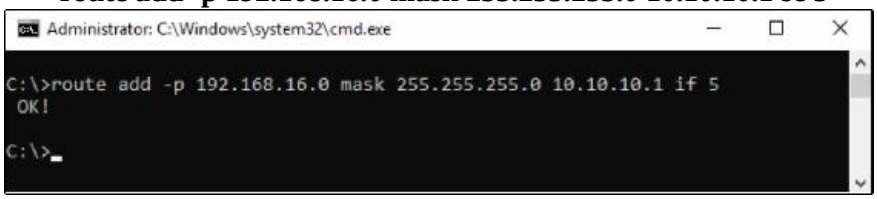
- -p: questo rende il comando persistente. Se dimentichi di mettere -p nella rotta aggiungi dichiarazione, questa nuova rotta scomparirà al prossimo riavvio del server. Non bene.
- SUBNET_ID : Questa è la sottorete che stiamo aggiungendo; nel nostro caso lo è 192.168.16.0 . MASCHERA DI SOTTORETE : Questo è il numero della subnet mask per la nuova rotta, 255.255.255.0 .
- GATEWAY: Questo è un po 'confuso. È molto comune pensare che sia necessario inserire l'indirizzo del gateway per la nuova sottorete, ma ci ò non sarebbe corretto. Quello che stai effettivamente definendo qui è il primo salto che il server deve colpire per inviare questo traffico. O in altre parole, se avessi configurato un indirizzo gateway predefinito sulla scheda di rete interna, quale sarebbe questo indirizzo? Per la nostra rete è il 10.10.10.1.
- INTERFACE_ID: Specificare un numero ID di interfaccia non è del tutto necessario per creare un percorso, ma se non lo specifichi, c' è la possibilit à che il tuo percorso possa legarsi alla NIC sbagliata e inviare il traffico nella direzione sbagliata. L'ho gi à visto accadere, quindi ho sempre specificato un numero ID dell'interfaccia NIC. Si tratta in genere di un numero a una o due cifre che è l'identificatore di Windows per la scheda NIC interna stessa. Possiamo capire qual è il numero ID dell'interfaccia guardando il comando di stampa della rotta:



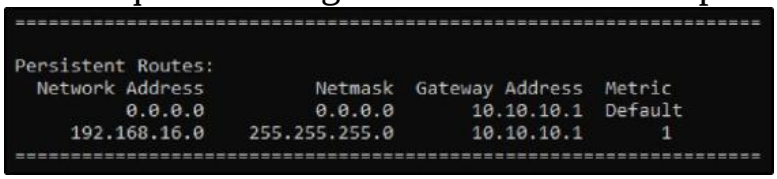
Nella parte superiore della stampa del percorso vengono visualizzati tutti i NIC in un sistema elencati. Nel nostro caso, il filela scheda di rete interna è la prima nell'elenco; L'ho identificato guardando l'indirizzo MAC per questa scheda NIC dall'output di un comando ipconfig / all. Come puoi vedere, il numero ID dell'interfaccia della mia NIC interna è 5. Quindi nella mia istruzione di aggiunta della rotta, userò IF 5 alla fine della mia istruzione per assicurarmi che la mia nuova rotta si leghi a quella NIC fisica interna.

Quanto segue è la nostra dichiarazione di aggiunta del percorso completata:

route add -p 192.168.16.0 mask 255.255.255.0 10.10.10.1 se 5



Se ora esegui un comando di stampa della rotta, puoi vedere la nostra nuova rotta 192.168.16.0 elencata nella sezione Percorsi persistenti della tabella di instradamento e ora possiamo inviare pacchetti in quella sottorete da questo nuovo server. Ogni volta che il nostro server ha traffico che deve entrare nella sottorete 192.168.16.x, invierà quel traffico fuori tramite la NIC interna, verso il router in esecuzione su 10.10.10.1. Il router quindi raccoglie il traffico da lì e lo porta nella sottorete 192.168:



Eliminazione di una rotta

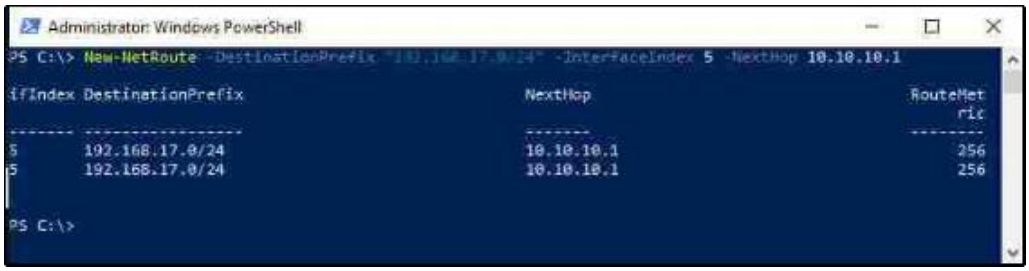
Occasionalmente, potresti inserire un'istruzione di route in modo errato. Il modo migliore per gestirlo è eliminare semplicemente la rotta errata e quindi rieseguire l'istruzione di aggiunta della rotta con la sintassi corretta. Ci sono forse altri motivi per cui potresti aver bisogno di eliminare le rotte di tanto in tanto, quindi ti consigliamo di avere familiarità con questo comando. Eliminare le rotte è molto più semplice che aggiungerne di nuove. Tutto quello che devi sapere è l'ID di sottorete per il percorso che desideri rimuovere, quindi semplicemente elimina il percorso <SUBNET_ID>. Ad esempio, per eliminare il nostro percorso 192.168.16.0 che abbiamo creato mentre stavamo lavorando all'interno del prompt dei comandi, emetterei semplicemente questo comando:

eliminazione del percorso 192.168.16.0

Aggiunta di una route con PowerShell

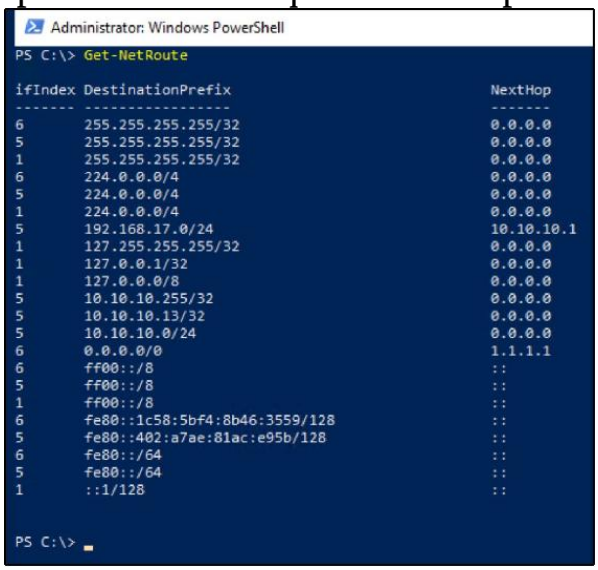
Poiché PowerShell è il re quando si tratta della maggior parte delle attività orientate alla riga di comando all'interno di Windows Server, dovremmo portare a termine la stessa missione anche da questa interfaccia. Puoi utilizzare lo stesso comando di aggiunta della route dall'interno del prompt di PowerShell e funzionerà perfettamente, ma c'è anche un cmdlet specializzato che possiamo usare. Utilizziamo New-NetRoute per aggiungere un'altra sottorete alla nostra tabella di instradamento; questa volta aggiungeremo 192.168.17.0. Quello che segue è un comando che possiamo utilizzare:

New-NetRoute -DestinationPrefix "192.168.17.0/24" -InterfaceIndex 5 - NextHop 10.10.10.1



Puoi vedere che la struttura è simile, ma un po 'più amichevole. Invece di dover digitare la parola maschera e specificare l'intero numero di maschera di sottorete, è possibile utilizzare il metodo barra per identificare la sottorete e la maschera all'interno dello stesso identificatore. Inoltre, dove prima stavamo specificando il gateway, che è sempre un po 'confuso, con il cmdlet New-NetRoute, specifichiamo invece ciò che viene chiamato NextHop. Questo ha un po 'più senso per me.

Dove in precedenza abbiamo utilizzato la stampa del percorso per vedere la nostra tabella di instradamento completa, il file Il cmdlet di PowerShell per visualizzare quella tabella per noi è semplicemente Get-NetRoute:



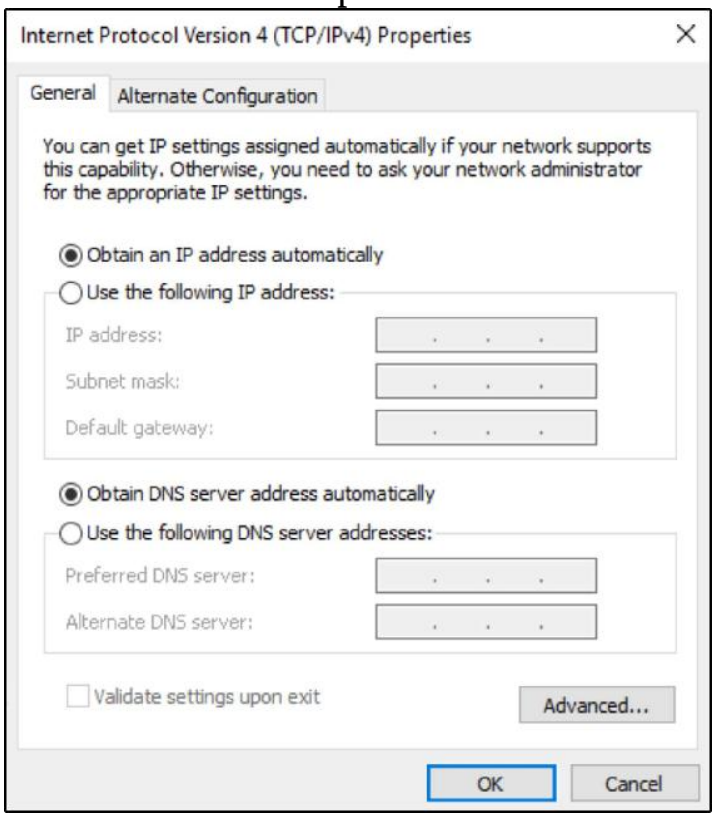
NIC Teaming

Passando a un altro argomento di rete che sta diventando sempre più popolare sull'hardware del server, esaminiamo i passaggi per creare NIC Teaming. La capacità di unire insieme le schede NIC consiste essenzialmente nell'associare due o più interfacce di rete fisiche insieme, in modo che si comportino come se fossero un'unica interfaccia di rete all'interno di Windows. Ciò consente di collegare due cavi fisici a due diverse porte dello switch, utilizzando tutte le stesse impostazioni. In questo modo, se una porta NIC, una porta switch o un cavo patch si guasta, il server continua a funzionare e a comunicare senza esitazione, perché il teaming consente alla NIC ancora funzionante di gestire il traffico di rete.

NIC Teaming in sé non è una novità, esiste da 10 anni o più all'interno del sistema operativo Windows Server. Tuttavia, le prime versioni erano problematiche e, sul campo, trovo che Server 2016 sia il primo sistema operativo per server che la maggior parte del personale IT considera sufficientemente stabile da utilizzare NIC Teaming in produzione. Quindi, sulla base di ciò, è ancora relativamente nuovo in natura.

Per iniziare a collaborare con le tue NIC, devi assicurarti di avere più schede di rete sul tuo server. Al momento ho quattro porte NIC su questa macchina. Ho in programma di creare due team: il mio primo e secondo NIC si uniranno per diventare un team di rete interna e il mio terzo e quarto NIC diventeranno un team di rete DMZ. In questo modo, ho la ridondanza della scheda di rete su entrambi i lati del flusso di rete su questo server.

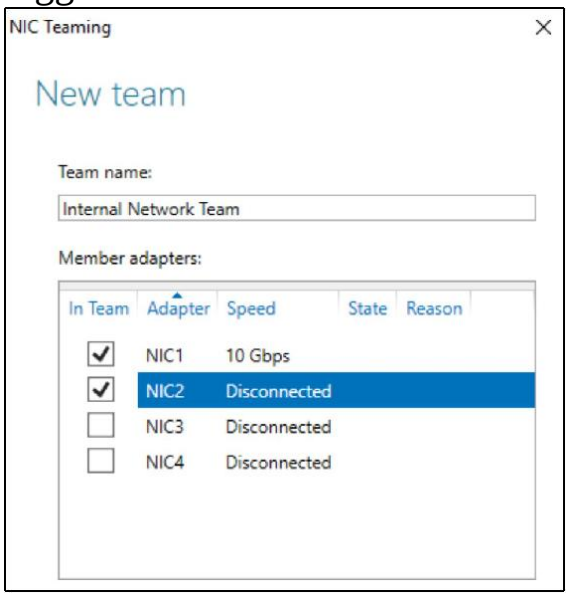
La prima cosa che voglio fare è cancellare tutte le impostazioni di indirizzamento IP che potrebbero esistere sui miei NIC. Vedete, una volta che legherete insieme più NIC in un team, configurerete le impostazioni di indirizzamento IP nel team: non vi immergerete più nelle singole proprietà NIC per assegnare gli indirizzi IP. Quindi apri le proprietà di ogni NIC e assicurati che siano prive di informazioni IP statiche, in questo modo:



Ora apri Server Manager e fai clic su Server locale. Guardando all'interno delle informazioni sulle proprietà per il tuo server, vedrai elenchi per ciascuna delle tue NIC, oltre a un'opzione chiamata NIC Teaming, che è attualmente impostata su Disabilitato:

Vai avanti e fai clic sulla parola Disabilitato, quindi cerca una sezione intitolata Team. Fare clic sul pulsante Attività e scegliere di creare un nuovo team.

Assegna al tuo nuovo team un nome appropriato e seleziona le schede NIC che desideri far parte di questo team. Una volta terminato, puoi eseguire gli stessi passaggi tutte le volte che desideri per creare team aggiuntivi con i tuoi NIC rimanenti:



Una volta terminato, vedrai i tuoi team elencati all'interno di Server Manager e se apri la schermata Connessioni di rete all'interno di Windows, puoi vedere che, oltre alle quattro NIC fisiche, ora ho due nuove voci elencate qui, che sono le posizioni di configurazione per i nostri nuovi team. Da qui posso fare clic con il pulsante destro del mouse su ciascuno dei miei team di rete e configurare le informazioni sull'indirizzamento IP proprio come avrei fatto su una singola scheda NIC. Gli IP inseriti nelle proprietà del team avranno effetto su tutti i NIC che fanno parte del team:

Rete definita dal software

La flessibilità e l'elasticità del cloud computing non possono essere negate e la maggior parte dei dirigenti tecnologici sta attualmente esplorando le proprie opzioni per l'utilizzo delle tecnologie cloud. Uno dei grandi ostacoli all'adattamento è la fiducia. I servizi cloud forniscono un'enorme potenza di calcolo, tutti immediatamente accessibili con la semplice pressione di un pulsante. Affinché le aziende possano archiviare i propri dati su questi sistemi, il livello di fiducia che la tua organizzazione ha in quel cloud provider deve essere molto alto. Dopo tutto, non possiedi nessuno dell'hardware o dell'infrastruttura di rete su cui si trovano i tuoi dati quando sono nel cloud, quindi il tuo controllo su tali risorse è limitato nella migliore delle ipotesi. Vedendo questo ostacolo, Microsoft ha compiuto molti sforzi negli ultimi aggiornamenti per portare la tecnologia simile al cloud nel data center locale. L'introduzione dell'elasticità dei server nei nostri data center significa virtualizzazione. Virtualizziamo i server da molti anni, anche se le capacità vengono continuamente migliorate. Ora che abbiamo la capacità di avviare nuovi server così facilmente attraverso le tecnologie di virtualizzazione, ha senso che il prossimo ostacolo sia la nostra capacità di spostare facilmente questi server virtuali in qualsiasi momento e ovunque ne abbiamo bisogno.

Hai un server che desideri spostare in un data center in tutto il paese? Stai pensando di migrare un intero data center in una nuova colocation in città? Forse hai recentemente acquisito una nuova società e hai bisogno di portare la sua infrastruttura nella tua rete, ma hai configurazioni di rete sovrapposte. Hai acquistato un po 'di spazio presso un fornitore di servizi cloud e ora stai cercando di guadare attraverso il caos della pianificazione della migrazione di tutti i tuoi server nel cloud? Queste sono tutte domande a cui occorreva una risposta e quella risposta è SDN.

SDN è un termine ampio e generico che comprende molte tecnologie che lavorano insieme per rendere possibile questa idea. Il suo scopo è estendere i confini della tua rete quando e dove ne hai bisogno. Diamo un'occhiata ad alcune delle parti e dei pezzi disponibili in Windows Server 2019 che lavorano in tandem per creare un ambiente di rete virtuale, il primo passo nell'adozione della nostra ideologia di rete definita dal software.

Virtualizzazione di rete Hyper-V

Il più grande componente su cui ci si concentra in questo momento che offre la possibilità di raccogliere le reti e farle scorrere su un livello di virtualizzazione si trova in Hyper-V. Questo ha senso, perché questo è lo stesso posto che stai toccando e accedendo per virtualizzare i tuoi server. Con Hyper-V Network Virtualization, stiamo creando una separazione tra le reti virtuali e le reti fisiche. Non è più necessario soddisfare le limitazioni dello schema IP sulla rete fisica quando si configurano nuove reti virtuali, perché queste ultime possono viaggiare sopra la rete fisica, anche se le configurazioni delle due reti sarebbero normalmente incompatibili.

Questo concetto è un po 'difficile da comprendere se è la prima volta che ne senti parlare, quindi parliamo di alcune situazioni del mondo reale che trarrebbero beneficio da questo tipo di separazione.

Cloud privati

I cloud privati si stanno diffondendo nei data center di tutto il mondo, perché hanno un enorme senso. Chiunque sia interessato a portare i grandi vantaggi del cloud nei propri ambienti, rimanendo allo stesso tempo lontano dagli aspetti negativi del cloud, può trarne vantaggio. La creazione di un cloud privato offre la possibilità di disporre di risorse di elaborazione in espansione e riduzione dinamica e la capacità di ospitare più tenant o divisioni all'interno della stessa infrastruttura di elaborazione. Fornisce interfacce di gestione direttamente a tali divisioni in modo che il lavoro di installazione e configurazione essenziale possa essere svolto dal tenant e non è necessario spendere tempo e risorse a livello di provider di infrastruttura per realizzare configurazioni piccole e dettagliate.

I cloud privati abilitano tutte queste funzionalità rimanendo lontani dal grande spavento dei tuoi dati ospitati nel data center di un provider di servizi cloud su cui non hai alcun controllo reale e da tutti i problemi di privacy che lo circondano.

Al fine di fornire un cloud privato all'interno della tua infrastruttura, in particolare quello in cui desideri fornire l'accesso a più tenant, i vantaggi della virtualizzazione della rete diventano evidenti e persino un requisito. Supponiamo che tu fornisca risorse di elaborazione a due divisioni di un'azienda e ognuna ha le proprie esigenze per l'hosting di alcuni server web. Non è un grosso problema, ma queste due divisioni dispongono entrambe di team amministrativi che desiderano utilizzare schemi IP entro 10.0.0.0. Entrambi devono essere in grado di utilizzare gli stessi indirizzi IP, sulla stessa rete principale che fornisci, ma devi mantenere tutto il loro traffico completamente separato e separato. Questi requisiti sarebbero stati impossibili su una rete fisica tradizionale, ma utilizzando la potenza della virtualizzazione della rete, puoi facilmente concedere sottoreti IP e schemi di indirizzi di qualsiasi calibro scelto da ciascuna divisione. Possono eseguire server su qualsiasi sottorete e indirizzo IP desiderino e tutto il traffico è incapsulato in modo univoco in modo che rimanga separato, completamente inconsapevole dell'altro traffico in esecuzione sulla stessa rete principale fisica che gira sotto il livello di virtualizzazione. Questo scenario si adatta bene anche alle acquisizioni aziendali. Due società che stanno unendo le forze a livello IT spesso hanno conflitti con i domini e il subnetting di rete. Con la virtualizzazione della rete, è possibile consentire all'infrastruttura e ai server esistenti di continuare a funzionare con la configurazione di rete corrente, ma portarli all'interno della stessa rete fisica utilizzando la virtualizzazione di rete Hyper-V. Possono eseguire server su qualsiasi sottorete e indirizzo IP desiderino e tutto il traffico è incapsulato in modo univoco in modo che rimanga separato, completamente inconsapevole dell'altro traffico in esecuzione sulla stessa rete principale fisica che gira sotto il livello di virtualizzazione. Questo scenario si adatta bene anche alle acquisizioni aziendali. Due aziende che stanno unendo le forze a livello IT spesso hanno conflitti con i domini e il subnetting di rete. Con la virtualizzazione della rete, è possibile consentire all'infrastruttura e ai server esistenti di continuare a funzionare con la

configurazione di rete corrente, ma portarli all'interno della stessa rete fisica utilizzando la virtualizzazione di rete Hyper-V. Possono eseguire server su qualsiasi sottorete e indirizzo IP desiderino e tutto il traffico è incapsulato in modo univoco in modo che rimanga separato, completamente inconsapevole dell'altro traffico in esecuzione sulla stessa rete principale fisica che gira sotto il livello di virtualizzazione. Questo scenario si adatta bene anche alle acquisizioni aziendali. Due società che stanno unendo le forze a livello IT spesso hanno conflitti con i domini e il subnetting di rete. Con la virtualizzazione della rete, è possibile consentire all'infrastruttura e ai server esistenti di continuare a funzionare con la configurazione di rete corrente, ma portarli all'interno della stessa rete fisica utilizzando la virtualizzazione di rete Hyper-V. completamente inconsapevole dell'altro traffico che circola sulla stessa rete principale fisica che gira sotto il livello di virtualizzazione. Questo scenario si adatta bene anche alle acquisizioni aziendali. Due aziende che stanno unendo le forze a livello IT spesso hanno conflitti con domini e subnetting di rete. Con la virtualizzazione della rete, è possibile consentire all'infrastruttura e ai server esistenti di continuare a funzionare con la configurazione di rete corrente, ma portarli all'interno della stessa rete fisica utilizzando la virtualizzazione di rete Hyper-V. completamente inconsapevole dell'altro traffico che circola sulla stessa rete principale fisica che gira sotto il livello di virtualizzazione. Questo scenario si adatta bene anche alle acquisizioni aziendali. Due aziende che stanno unendo le forze a livello IT spesso hanno conflitti con domini e subnetting di rete. Con la virtualizzazione della rete, è possibile consentire all'infrastruttura e ai server esistenti di continuare a funzionare con la configurazione di rete corrente, ma portarli all'interno della stessa rete fisica utilizzando la virtualizzazione di rete Hyper-V.

Un altro esempio più semplice è quello in cui si desidera semplicemente spostare un server all'interno di una rete aziendale. Forse hai un server line-of-business legacy a cui molti dipendenti devono ancora accedere, perché il loro carico di lavoro quotidiano include l'applicazione LOB per funzionare in ogni momento. Il problema con lo spostamento del server è che l'applicazione LOB sui computer client ha un indirizzo IPv4 statico configurato mediante il quale comunica con il server. Quando l'utente

apre la sua app, fa qualcosa come parlare al server al 10.10.10.10. Tradizionalmente, ciò potrebbe trasformarsi in un rompicapo per lo spostamento del server, perché spostare quel server dal suo data center attuale a una nuova posizione significherebbe cambiare l'indirizzo IP del server e ciò interromperebbe la capacità di tutti di connettersi ad esso. Con le reti virtuali, questo non è un problema. Con la capacità di gestire il traffico di rete e le sottoreti IP sul livello di virtualizzazione, quel server può spostarsi da New York a San Diego e conservare tutte le impostazioni dell'indirizzo IP, perché la rete fisica in esecuzione al di sotto non ha alcuna importanza. Tutto il traffico viene incapsulato prima di essere inviato sulla rete fisica, quindi l'indirizzo IP del server legacy può rimanere a 10.10.10.10 e può essere raccolto e spostato ovunque nell'ambiente senza interruzioni.

Nuvole ibride

Sebbene l'aggiunta di flessibilità alle reti aziendali sia già un enorme vantaggio, le funzionalità fornite dalla virtualizzazione delle reti si espandono in modo esponenziale quando finalmente decidi di iniziare a esplorare le risorse cloud reali. Se e quando decidi di spostare alcune risorse affinché siano ospitate da un provider di servizi di cloud pubblico, probabilmente eseguirai un ambiente di cloud ibrido. Ciò significa che costruirai alcuni servizi nel cloud, ma manterrai anche alcuni server e servizi in loco. Prevedo che la maggior parte delle aziende rimarrà in uno scenario di cloud ibrido per il resto dell'eternità, poiché un passaggio al 100% al cloud non è semplicemente possibile visti i modi in cui molte delle nostre aziende fanno affari. Quindi, ora che desideri configurare un cloud ibrido, stiamo nuovamente esaminando tutti i tipi di mal di testa associati al movimento delle risorse tra le nostre reti fisiche e cloud. Quando voglio spostare un server dal sito al cloud, devo regolare tutto in modo che la configurazione di rete sia compatibile con l'infrastruttura cloud, giusto? Non dovrò riconfigurare la NIC sul mio server in modo che corrisponda alla subnet in esecuzione nella mia rete cloud? No, non se la tua infrastruttura di virtualizzazione della rete è attiva e funzionante. Ancora una volta, la rete definita dal software consente di risparmiare la giornata, dandoci la possibilità di conservare le informazioni sull'indirizzo IP esistente sui nostri server in movimento e di eseguirle semplicemente con quegli indirizzi IP nel cloud. Ancora una volta, poiché tutto il traffico viene incapsulato prima di essere trasportato,

Come funziona?

Finora suona tutto come un po 'di magia; come funziona effettivamente e quali elementi devono combaciare per rendere la virtualizzazione della rete una realtà nella nostra organizzazione? Qualcosa di così completo ha sicuramente molte parti mobili e non può essere attivato semplicemente premendo un interruttore. Esistono varie tecnologie e componenti in esecuzione all'interno di una rete abilitata per la virtualizzazione della rete. Spieghiamo un po 'qui in modo da avere una migliore comprensione

delle tecnologie e della terminologia con cui avrai a che fare una volta che inizi il tuo lavoro con il networking definito dal software.

System Center Virtual Machine Manager

Microsoft System Center è un pezzo chiave del puzzle per la creazione del modello di rete definito dal software, in particolare il componente Virtual Machine Manager (VMM) di System Center. La capacità di raccogliere indirizzi IP e spostarli in altre località in tutto il mondo richiede un certo coordinamento dei dispositivi di rete e VMM è qui per aiutarti. Questo è il componente con cui ci si interfaccia come punto di gestione centrale per definire e configurare le reti virtuali. System Center è un argomento enorme con molte opzioni e punti dati che non rientrano in questo libro, quindi ti lascerò un collegamento come punto di partenza per l'apprendimento di VMM:https: //documenti.microsoft.com /en-noi/precedente-versioni /sistema-centro/sistema-centro-2012-R2 /gg610610 (v =sc.12).

Rete controller

Il controller di rete di Microsoft è un ruolo che è stato inizialmente introdotto in Windows Server 2016 e, come suggerisce il nome, viene utilizzato per il controllo delle risorse di rete all'interno dell'organizzazione. Nella maggior parte dei casi, lavorerà fianco a fianco con VMM per rendere le configurazioni di rete il più centralizzate e senza soluzione di continuità possibile. Il controller di rete è un ruolo autonomo e può essere installato su Server 2016 o 2019 e quindi accedervi direttamente, senza VMM, ma non prevedo che molte distribuzioni lo lascino così. L'interfacciamento con il controller di rete direttamente è possibile attingendo alle sue API con PowerShell, ma è ulteriormente migliorato aggiungendo un'interfaccia grafica da cui configurare nuove reti, monitorare reti e dispositivi esistenti o risolvere problemi all'interno del modello di rete virtuale.

Il controller di rete può essere utilizzato per configurare molti aspetti diversi delle reti fisiche e virtuali. Puoi configurare sottoreti e indirizzi IP, configurazioni e VLAN su switch Hyper-V e puoi persino usarlo per configurare NIC sulle tue VM. Il controller di rete consente inoltre di creare e gestire regole di tipo ACL (Access Control List) all'interno dello switch Hyper-V in modo da poter creare la propria soluzione di

firewalling a questo livello, senza la necessità di configurare firewall locali sulle VM stesse o con firewall dedicato hardware. Il controller di rete può anche essere utilizzato per configurare il bilanciamento del carico e fornire l'accesso VPN tramite i server RRAS.

Incapsulamento del routing generico

Incapsulamento del routing generico (GRE) è solo un protocollo di tunneling, ma è fondamentale per far sì che la virtualizzazione della rete avvenga con successo. In precedenza, quando abbiamo parlato dello spostamento delle sottoreti IP e di come è possibile collocare reti virtuali su reti fisiche senza riguardo per assicurarsi che le loro configurazioni IP siano compatibili, dovremmo aggiungere che tutte queste funzionalità sono fornite in primo luogo da GRE . Quando la tua rete fisica esegue 192.168.0.x ma desideri ospitare alcune VM su una sottorete in quel data center, puoi creare una rete virtuale di 10.10.10.x senza problemi, ma quel traffico deve essere in grado di farlo attraversare la rete fisica 192.168 per far funzionare qualsiasi cosa. È qui che entra in gioco l'incapsulamento del routing. Tutti i pacchetti dalla rete 10.10.10.x vengono incapsulati prima di essere trasportati attraverso la rete fisica 192.168.0.x.

Esistono due diversi protocolli di incapsulamento del routing specifici supportati nel nostro ambiente di virtualizzazione della rete Microsoft Hyper-V. Nelle versioni precedenti del sistema operativo Windows Server, potevamo concentrarci solo su NVGRE (Network Virtualization Generic Routing Encapsulation), poiché questo era l'unico protocollo supportato dalla versione Windows della virtualizzazione di rete. Tuttavia, esiste un altro protocollo, chiamato VXLAN (Virtual Extensible Local Area Network), che esiste da un po 'di tempo e molti degli switch di rete, in particolare Cisco, che hai nel tuo ambiente hanno maggiori probabilità di supportare VXLAN di quanto non lo siano. NVGRE. Quindi, per le nuove piattaforme di virtualizzazione della rete fornite con Windows Server 2016+, ora siamo in grado di supportare NVGRE o VXLAN, a seconda di quale si adatta meglio alle esigenze della tua azienda.

Non devi necessariamente capire come funzionano questi protocolli GRE per farli funzionare per te, poiché saranno configurati per te dagli strumenti di gestione che esistono in questo stack di virtualizzazione di rete Hyper-V. Ma è importante capire nel concetto generale di questo ambiente di rete virtuale che GRE esiste e che è il segreto per far funzionare tutto questo.

Rete virtuale di Microsoft Azure

Una volta che la virtualizzazione della rete Hyper-V è in esecuzione all'interno della rete aziendale e ti sei abituato alla mentalità di separare le reti fisiche e virtuali, molto probabilmente vorrai esplorare le possibilità di interagire con il cloud
reti di fornitori di servizi. Quando si utilizza Microsoft Azure come provider di servizi cloud, si ha la possibilità di creare un ambiente cloud ibrido che collega le reti fisiche locali con le reti virtuali remote ospitate in Azure. La rete virtuale di Azure è il componente all'interno di Azure che ti consente di portare i tuoi indirizzi IP e le tue subnet nel cloud. Puoi ottenere maggiori informazioni (e persino registrarti per una versione di prova gratuita della rete virtuale di Azure) qui:https: //azzurro.microsoft.com /en-noi/Servizi/virtuale-Rete/.

Windows Server Gateway / SDN Gateway

Quando si lavora con reti fisiche, reti virtuali e reti virtuali archiviate in ambienti cloud, è necessario un componente per colmare queste lacune, consentendo alle reti di interagire e comunicare tra loro. È qui che entra in gioco un gateway di Windows Server (chiamato anche gateway SDN). Windows Server Gateway è il termine più recente; in precedenza era ea volte è ancora chiamato Hyper-V Network Virtualization Gateway, quindi potresti vedere quel gergo in alcuni documenti. Lo scopo di un gateway di Windows Server è piuttosto semplice: essere la connessione tra reti virtuali e fisiche. Queste reti virtuali possono essere ospitate nel tuo ambiente locale o nel cloud. In entrambi i casi, quando desideri connettere le reti, dovrai utilizzare un Windows Server Gateway.

Un gateway di Windows Server è generalmente una macchina virtuale ed è integrato con Hyper-V Network Virtualization. Un singolo gateway può essere utilizzato per instradare il traffico per molti clienti, tenant o divisioni diversi. Anche se questi diversi clienti hanno reti separate che devono mantenere la separazione dal traffico degli altri clienti, il cloud provider, pubblico o privato, può comunque utilizzare un unico gateway per gestire questo traffico, perché i gateway mantengono un isolamento completo tra questi flussi di traffico.

La funzionalità Windows Server Gateway esisteva in Server 2016, ma una volta messa in pratica, sono state scoperte alcune limitazioni delle prestazioni che limitavano la velocità effettiva del traffico di rete. Questi costi generali sono stati ora notevolmente aumentati in Windows Server 2019, il che significa che è possibile trasferire più traffico e tenant aggiuntivi attraverso un singolo gateway di quanto fosse possibile in precedenza.

Crittografia della rete virtuale

I team di sicurezza sono continuamente interessati alla crittografia dei dati. Indipendentemente dal fatto che i dati siano archiviati o in movimento, è essenziale assicurarsi che siano adeguatamente protetti e al

riparo da manomissioni. Prima di Server 2019, ottenere la crittografia del traffico di rete interno durante lo spostamento era generalmente responsabilità dell'applicazione software stessa, non compito della rete. Se il software è in grado di crittografare il traffico mentre scorre tra il client e il server o tra il server delle applicazioni e il server del database, ottimo! Se l'applicazione non dispone di funzionalità di crittografia native, è probabile che le comunicazioni da tale applicazione fluiscano in testo non crittografato tra il client e il server. Anche per le applicazioni che eseguono la crittografia, i codici di crittografia e gli algoritmi a volte vengono violati e compromessi,

Fortunatamente, Windows Server 2019 ci offre una nuova funzionalità entro i confini del networking definito dal software. Questa capacità è chiamata crittografia della rete virtuale e fa esattamente ciò che suggerisce il nome. Quando il traffico si sposta tra macchine virtuali e tra server Hyper-V (all'interno della stessa rete), intere sottoreti possono essere contrassegnate per la crittografia, il che significa che tutto il traffico che scorre in tali sottoreti viene automaticamente crittografato a livello di rete virtuale. I server VM e le applicazioni in esecuzione su tali server non devono essere configurati o modificati in alcun modo per sfruttare questa crittografia, come accade all'interno della rete stessa, crittografando automaticamente tutto il traffico che scorre su quella rete.

Con Server 2019 SDN, qualsiasi subnet in una rete virtuale può essere contrassegnata per la crittografia specificando un certificato da utilizzare per tale crittografia. Se il futuro dovesse portare lo scenario in cui gli attuali standard di crittografia sono obsoleti o insicuri, il fabric SDN può essere aggiornato a nuovi standard di crittografia e quelle sottoreti continueranno a essere crittografate utilizzando i nuovi metodi, ancora una volta senza dover effettuare modifiche alle VM o alle applicazioni. Se utilizzi SDN e reti virtuali nei tuoi ambienti, abilitare la crittografia su tali sottoreti è un gioco da ragazzi!

Colmare il divario con Azure

La maggior parte delle aziende che ospitano server in Microsoft Azure dispone ancora di reti fisiche in sede e una delle grandi domande a cui è sempre necessario rispondere è: come collegheremo il nostro data center fisico al nostro data center Azure? Di solito, le aziende stabiliscono uno dei due metodi diversi per farlo accadere. È possibile distribuire server gateway ai margini delle reti in loco e di Azure e connetterli tramite VPN da sito a sito. Questo stabilisce un tunnel continuo tra le due reti. In alternativa, Microsoft fornisce un servizio chiamato Azure Express Route che fa effettivamente la stessa cosa: crea un tunnel permanente tra la tua rete fisica e quella delle tue reti virtuali di Azure. Uno di questi metodi funziona alla grande una volta configurato,

Scheda di rete di Azure

Nel caso in cui si disponga di un server in sede che è necessario connettersi rapidamente al proprio ambiente Azure (e non si dispone già di una connessione permanente stabilita tra i propri siti fisici e Azure), è disponibile una nuovissima funzionalità di cloud ibrido chiamata Scheda di rete di Azure. Per poter utilizzare uno di questi nuovi adattatori di rete, devi utilizzare il nuovo Windows Admin Center per gestire i tuoi server.

Utilizzando Windows Admin Center, è possibile aggiungere rapidamente una scheda di rete di Azure a un server locale, che lo connette direttamente alla rete di Azure utilizzando una connessione VPN da punto a sito. Freddo!

Ancora meglio, questa capacità è stata trasferita in modo da poter aggiungere uno di questi adattatori non solo alle macchine Server 2019, ma anche alle macchine Server 2016 e Server 2012 R2.

Per far sì che ciò accada, ci sono alcuni requisiti che devono essere in atto: devi avere una sottoscrizione di Azure attiva e devi avere almeno una rete virtuale di Azure configurata.

Successivamente, devi registrare il tuo Windows Admin Center con Azure. Ciò si ottiene aprendo Windows Admin Center e visitando Impostazioni. Una volta dentro, vai a GATEWAY | Azure e segui il processo di registrazione:

Ora che il tuo WAC è registrato con Azure, apri il server che stai gestendo dall'interno di WAC e vai alla sezione Rete. Vedrai elencate qui tutte le schede NIC presenti sul tuo server e vicino alla parte superiore della finestra c'è una casella a discesa per le azioni. All'interno, fare clic su Aggiungi scheda di rete Azure.

Scoprirai che tutti i valori necessari ad Azure per stabilire questa connessione vengono compilati automaticamente, in base alla rete e alla sottoscrizione di Azure. Se non disponi già di una rete virtuale di Azure, questa procedura guidata può persino crearne una per te. Hai anche la possibilità di specificare il tuo certificato per l'autenticazione di questa connessione e ciò sarebbe una buona pratica se prevedi che questa sia una connessione a lungo termine ad Azure; in caso contrario, è possibile procedere senza alcun input consentendo a WAC / Azure di generare un certificato autofirmato e fare semplicemente clic sul pulsante Crea. Windows Admin Center andrà avanti e creerà una connessione tra il tuo server locale e la rete virtuale di Azure. Erano solo un paio di clic del mouse!

Se in seguito è necessario disconnettere questo server dalla rete Azure, è possibile aprire le connessioni di rete su quel server locale, proprio come faresti quando provi a modificare le proprietà NIC sul tuo server e scoprirai che ciò che WAC ha fatto sotto il cappuccio è configurare una connessione VPN da punto a sito, che è elencata in Connessioni di rete. Puoi semplicemente fare clic con il pulsante destro del mouse su quella connessione VPN di Azure e disconnetterla.

Sommario

L'amministrazione del server e l'amministrazione della rete erano separate in modo abbastanza chiaro nella maggior parte delle organizzazioni, ma nel tempo queste linee si sono confuse. Esistono numerose configurazioni e attività di rete che ora devono essere eseguite dagli amministratori di Windows Server, senza la necessità di coinvolgere un team di rete, quindi è importante che tu abbia una buona conoscenza di come la tua infrastruttura si connette insieme. La familiarità con gli strumenti descritti in questo capitolo ti consentirà di configurare, monitorare e risolvere i problemi della maggior parte delle reti Microsoft.

La nostra introduzione al networking definito dal software può essere una sezione parzialmente confusa se non hai mai incontrato questa idea prima, ma si spera che ti spinga a scavare un po 'più a fondo e prepararti ad affrontare questo problema in futuro. Che tu sia pronto o meno, il cloud è qui per restare. Le reti Microsoft in sede ora hanno numerosi modi per interagire con Microsoft Azure e presto sarà fondamentale che il personale IT abbia familiarità con questi concetti. L'idea di SDN crescerà in popolarità nei prossimi anni; al momento, può sembrare scoraggiante, ma tra cinque anni, potremmo tutti guardare indietro e chiederci come abbiamo fatto a far funzionare le cose senza reti virtuali. Ci sono molte più informazioni sia in Microsoft Docs che nei libri pubblicati su Hyper-V Virtual Networking e System Center Virtual Machine Manager. Consiglio una maggiore familiarità con questo materiale se sei interessato a provarlo di persona. Il prossimo capitolo tratta dell'abilitazione della tua forza lavoro mobile.

Domande

1. Quanti bit è lungo un indirizzo IPv6?
2. Riscrivi il seguente indirizzo IPv6 in forma ridotta: 2001: ABCD: 0001: 0002: 0000: 0000: 0000: 0001
3. Qual è il nome del comando che è simile a trace route, ma visualizza la NIC locale da cui esce il traffico?
4. Vero o falso: su un server con più schede NIC, è possibile immettere un indirizzo gateway predefinito in ciascuna di queste schede.
5. Qual è il cmdlet di PowerShell che può essere utilizzato per creare nuove rotte su un server Windows
6. Quali sistemi operativi Windows Server possono essere utilizzati con una scheda di rete di Azure per collegarli direttamente alle reti virtuali di Azure?

Abilitare il tuo cellulare Forza lavoro

Dare ai dipendenti la possibilità di accedere da remoto alle risorse aziendali era un grande vantaggio per la maggior parte delle aziende, ma non necessariamente un requisito. Questo è certamente cambiato negli ultimi anni, dove la maggior parte delle aziende e dei dipendenti ora si aspetta di poter portare a termine il proprio lavoro ovunque si trovi. I telefoni cellulari sono una parte importante di questa equazione, ma sono limitati dalla portata di ciò che può essere fatto con schermi piccoli e sistemi operativi limitati. Per garantire ai lavoratori remoti la possibilità di svolgere il proprio lavoro da casa, bar o hotel, abbiamo utilizzato tradizionalmente reti private virtuali (VPN).

La maggior parte delle VPN nelle aziende odierne è fornita da prodotti di società diverse da Microsoft. Il ruolo di accesso remoto in Windows Server 2019 è qui per cambiarlo. Con molti miglioramenti apportati ai componenti VPN direttamente in Windows Server, ora è una piattaforma

fattibile e sicura per fornire l'accesso alle risorse aziendali da computer remoti. Oltre alle VPN, abbiamo un paio di nuove tecnologie integrate in Windows Server 2019 progettate anche per fornire l'accesso remoto alle risorse aziendali, in un modo diverso rispetto a una VPN tradizionale. Gli argomenti che tratteremo in questo capitolo sono i seguenti:

- Sempre su VPN
- DirectAccess
- Console di gestione dell'accesso remoto DA, VPN o AOVPN? Qual è il migliore? Requisiti del proxy dell'applicazione Web per WAP
- Ultimi miglioramenti al WAP

Sempre su VPN

Dare a un utente l'accesso a una connessione VPN significa tradizionalmente fornire loro uno speciale collegamento di connessione di rete che possono avviare, immettere le credenziali per passare l'autenticazione e quindi essere connessi alla rete del proprio ambiente di lavoro per comunicare con le risorse aziendali. Dopo aver avviato una VPN, gli utenti possono aprire la posta elettronica, trovare documenti, avviare le loro applicazioni line-of-business o lavorare in altro modo nello stesso modo in cui possono farlo quando sono fisicamente seduti in ufficio. Inoltre, quando si è connessi tramite una VPN, è possibile la gestione del proprio laptop, consentendo un flusso di comunicazione corretto per sistemi come Criteri di gruppo e SCCM. Le connessioni VPN offrono un'ottima connettività alla tua rete, ma (ricorda, stiamo parlando di tradizionali,

Ogni volta che un utente non si è connesso alla propria VPN, naviga in Internet senza connettività al data center aziendale. Ciò significa anche che una connessione VPN tradizionale ovviamente non ha alcuna forma di connettività nella schermata di accesso di Windows, perché, fino a quando non si connettono al computer e non trovano la strada per il desktop di Windows, gli utenti non hanno modo di avviare quel tunnel VPN. Ciò significa che tutto ciò che potrebbe tentare di accadere nella schermata di accesso, come le ricerche di autenticazione dal vivo o durante il processo di accesso, come l'elaborazione dei Criteri di gruppo o gli script di accesso, non funzionerà tramite una VPN tradizionale.

Sempre su VPN (AOVPN), proprio come probabilmente avrai intuito in base al nome, è semplicemente l'idea di rendere continua e automaticamente connessa una connessione VPN. In altre parole, ogni volta che l'utente ha il proprio laptop fuori dalle mura dell'ufficio ed è connesso a Internet, viene stabilito automaticamente un tunnel VPN per tornare alla rete aziendale, idealmente con zero input da parte dell'utente al processo. Ciò consente agli utenti di dimenticare del tutto la VPN, poiché è semplicemente sempre connessa e pronta per essere utilizzata. Possono accedere alle loro macchine, avviare le loro applicazioni e

iniziare a lavorare. Significa anche che le funzioni di gestione IT come le politiche di sicurezza, gli aggiornamenti e i pacchetti di installazione possono eseguire il push sui computer client una percentuale maggiore del tempo, poiché non aspettiamo più che l'utente decida quando desidera riconnettersi al lavoro;

Esistono in realtà tre diversi modi in cui è possibile attivare Always On VPN sul computer client e nessuno di questi implica che l'utente debba avviare una connessione VPN:

- AOVPN può essere configurato per essere veramente Always On, il che significa che non appena l'accesso a Internet sarà disponibile, tenterà sempre di connettersi.
- Un'altra opzione è l'attivazione dell'applicazione, il che significa che è possibile configurare AOVPN in modo che si avvii solo quando vengono aperte applicazioni specifiche sulla workstation.

- La terza opzione è l'attivazione basata sul nome DNS. Ciò richiama la connessione VPN in azione quando vengono richiesti particolari nomi DNS, cosa che generalmente accade quando gli utenti avviano applicazioni specifiche.

Dal momento che ovviamente non hai bisogno di Always On VPN per essere connesso e funzionare quando il tuo laptop si trova all'interno della rete aziendale, dovremmo anche discutere del fatto che AOVPN è abbastanza intelligente da spegnersi quando l'utente attraversa quelle porte di vetro. I computer abilitati AOVPN decideranno automaticamente quando si trovano all'interno della rete, disabilitando quindi i componenti VPN, e quando sono fuori dalla rete e devono avviare la connessione tunnel VPN. Questo processo di rilevamento è noto come rilevamento di rete attendibile.
Se configurati correttamente, i componenti Always On VPN sanno qual è il suffisso DNS interno della tua azienda, quindi monitora le impostazioni del tuo profilo NIC e firewall per stabilire se lo stesso suffisso è stato assegnato a quei componenti. Quando vede una corrispondenza, sa che sei all'interno della rete e quindi disattiva AOVPN.

Tipi di tunnel AOVPN

Prima di iniziare con i dettagli dei componenti client e server necessari per realizzare AOVPN, c'è un importante argomento centrale che deve essere compreso per prendere decisioni appropriate su come utilizzare AOVPN nella tua azienda. Esistono due tipi molto diversi di tunnel VPN che possono essere utilizzati con Always On VPN: un tunnel utente e un tunnel del dispositivo. Come imparerai più avanti in questo capitolo, la possibilità di avere due diversi tipi di tunnel è qualcosa incluso in AOVPN per avvicinarlo alla parità di funzionalità con DirectAccess, che ha anche questa mentalità a doppio tunnel. Prendiamoci un minuto ed esploriamo gli scopi dietro i due tunnel.

Tunnel utente

Il modo più comune per eseguire AOVPN in natura (finora), un tunnel utente viene autenticato a livello di utente. I certificati utente vengono emessi da una PKI interna ai computer e questi certificati vengono quindi utilizzati come parte del processo di autenticazione durante la connessione. I tunnel utente trasportano tutto il traffico della macchina e degli utenti, ma è molto importante notare che i tunnel utente non possono essere stabiliti mentre il computer è seduto sulla schermata di accesso, perché l'autenticazione dell'utente non è avvenuta a quel punto. Quindi, un tunnel utente si avvierà solo una volta che un utente avrà effettuato correttamente l'accesso al computer. Con solo un tunnel utente in gioco, il computer non avrà la connettività di nuovo alla rete aziendale per le funzioni di gestione fino a quando qualcuno non avrà effettuato l'accesso al computer,

Tunnel del dispositivo

Un tunnel del dispositivo ha lo scopo di colmare le lacune lasciate eseguendo solo un tunnel utente. Un tunnel del dispositivo viene autenticato tramite un certificato macchina, emesso anche dalla PKI interna. Ciò significa che il Device Tunnel può stabilirsi anche prima dell'autenticazione dell'utente. In altre parole, funziona anche stando seduti nella schermata di accesso di Windows. Ciò consente agli strumenti di gestione come Criteri di gruppo e SCCM di funzionare indipendentemente dall'input dell'utente e consente anche l'autenticazione in tempo reale contro i controller di dominio, consentendo agli utenti di accedere alla workstation che non vi hanno mai effettuato l'accesso prima. Ciò consente anche la reimpostazione della scadenza della password in tempo reale.

Requisiti del tunnel dei dispositivi

Un tunnel utente può funzionare praticamente con qualsiasi macchina Windows 10, ma ci sono alcuni requisiti rigidi per poter utilizzare un tunnel di dispositivi. Per implementare un tunnel di dispositivi, è necessario soddisfare i seguenti requisiti:

- Il client deve essere aggiunto a un dominio.
- Al client deve essere emesso un certificato macchina.
- Il client deve eseguire Windows 10 1709 o versioni successive e solo Enterprise o
  Formazione scolastica Gli SKU hanno questa capacità.
- Un tunnel di dispositivi può essere solo IKEv2. Questo non è necessariamente un requisito, ma è importante capire una volta che si è arrivati a discutere di cosa sia IKEv2 e perché potrebbe essere o meno il miglior metodo di connettività per i propri clienti.

Requisiti del client AOVPN

È importante capire che la parte Always On di Always On VPN è in realtà una funzionalità lato client. Puoi utilizzare AOVPN su un computer client per connetterti a molti diversi tipi di infrastruttura VPN sul back-end. Ne parleremo a breve, nella sezione dei componenti del server AOVPN.

Sebbene la creazione di connessioni VPN manuali e regolari sia possibile sui sistemi operativi client Windows da 15 o 20 anni, Always On VPN è piuttosto nuova. La tua forza lavoro dovrà eseguire Windows 10 per far sì che ciò accada. In particolare, dovranno eseguire Windows 10 versione 1607 o una versione più recente.

Di seguito sono riportati gli SKU supportati:

- Windows 10 1607+
- Windows 10 1709+
- Windows 10 1803+

Aspetta un minuto, non ha alcun senso. Perché elencare questi tre elementi separatamente se sono comprensivi l'uno dell'altro? Perché, sebbene tecnicamente Always On VPN sia stato ufficialmente introdotto in Windows 10 1607, ha avuto alcuni miglioramenti lungo la strada. Elenchiamoli di nuovo, con un breve riassunto di ciò che è cambiato negli anni:

- **Windows 10 1607**: La capacità originale di avviare automaticamente una connessione VPN, abilitando così Always On VPN.
- **Windows 10 1709**: Gli aggiornamenti e le modifiche includevano l'aggiunta di Device Tunnel. Se intendi eseguire un tunnel di dispositivi per scopi di gestione del computer (e la maggior parte delle aziende lo farà), considera 1709 come requisito minimo del sistema operativo.
- **Windows 10 1803**: Include alcune correzioni scoperte dal 1709. In realtà, ciò significa che non vedo mai nessuno implementare Always On VPN a meno che non stia eseguendo 1803. Per fortuna, la piattaforma di aggiornamento di Windows 10 è molto migliorata, il che significa che molte più aziende stanno rotolando le versioni più recenti di Win10 su base continuativa e l'aggiornamento alla 1803 è molto meno doloroso rispetto, ad esempio, a una migrazione da Windows XP a Windows 7.

Che tu stia eseguendo 1607, 1709, 1803 o 1809, il particolare SKU all'interno di queste piattaforme non ha importanza. Beh, non importa. Always On VPN funziona con Windows 10 Home, Pro, Enterprise e tutte le altre versioni. Cioè, il tunnel utente funziona con tutti questi.

È abbastanza importante sottolinearlo ancora una volta: se si desidera utilizzare un tunnel di dispositivi con Always On VPN, l'utilizzo di SKU di Windows 10 Enterprise o Education è un requisito fondamentale.

Aggiunto a un dominio

Come abbiamo già stabilito, quando sei interessato a utilizzare AOVPN Device Tunnel, i tuoi computer client devono essere aggiunti a un dominio. Tuttavia, se puoi eseguire solo il tunnel utente per l'accesso AOVPN, non ci sono requisiti di appartenenza al dominio. I client devono ancora eseguire Windows 10 1607 o versioni successive, ma potrebbero essere qualsiasi SKU e persino computer domestici uniti a semplici gruppi di lavoro; non è richiesto alcun dominio.

Ciò è sottolineato in modo specifico nella documentazione Microsoft in molti punti, perché consente di utilizzare Always On VPN (in qualche modo) con la folla Bring Your Own Device (BYOD). Anche se questo è interessante, non prevedo che sia affatto comune che le aziende consentano ai personal computer dei dipendenti di essere collegati alla loro VPN. La maggior parte delle organizzazioni sta cercando di soddisfare in piccola parte il mercato BYOD fornendo l'accesso ad alcune risorse tramite il cloud, come Office 365 per posta elettronica e documenti. Ma connettere nuovamente quei personal computer e dispositivi alla tua rete con un tunnel VPN di livello 3 su vasta scala? Non credo proprio. Questa è la materia degli incubi degli amministratori della sicurezza.

Implementazione delle impostazioni

Supponiamo che tu abbia tutte le parti e i pezzi lato server pronti per la connettività VPN e in effetti hai stabilito con successo il fatto che puoi creare connessioni VPN tradizionali ad hoc alla tua infrastruttura senza problemi. Grande! Sembra che tu sia pronto dal lato infrastrutturale. Ora, cosa è necessario per convincere i client a iniziare a fare connessioni Always On?

Questo è attualmente un requisito un po 'rigido per alcune aziende. La configurazione stessa delle impostazioni dei criteri Always On VPN non è particolarmente difficile; devi solo avere familiarità con le diverse opzioni disponibili, decidere quali sono importanti per la tua distribuzione e mettere insieme il file / script di configurazione. Anche se non abbiamo lo spazio qui per coprire tutte queste opzioni in dettaglio, il metodo per mettere insieme queste impostazioni è generalmente quello di creare una connessione VPN ad avvio manuale, adattarla alle impostazioni di sicurezza e autenticazione che desideri per la tua forza lavoro e quindi eseguire un'utilità che esporta tale configurazione in alcuni file di configurazione. Queste impostazioni del profilo VPN sono disponibili in versioni XML e PS1 (script PowerShell), e potresti aver bisogno di uno o entrambi questi file per trasferire le impostazioni alla tua forza lavoro.

Quanto segue è un ottimo punto di partenza per lavorare con queste configurazioni:https: //documenti.microsoft.com /en-noi/finestre-server/a distanza/a distanza-accesso/vpn /sempre-su-vpn /distribuire /vpn-schierarecliente-vpn-collegamenti.

Dopo aver creato i file di configurazione, dovrai affrontare il compito di inviare tale configurazione ai client. Idealmente, è necessario disporre di una soluzione di gestione dei dispositivi mobili (MDM) di qualche tipo per distribuire le impostazioni alla forza lavoro. Sebbene molte tecnologie in circolazione possano essere considerate MDM, le due su cui Microsoft si concentra sono System Center Configuration Manager (SCCM) e Microsoft Intune.

Se disponi di SCCM in sede, fantastico! È possibile configurare e distribuire facilmente le impostazioni di configurazione basate su PowerShell ai computer client e abilitarle per Always On VPN.

Forse non hai SCCM, ma sei concentrato sul cloud e hai tutti i tuoi computer collegati a Intune? Meraviglioso! In alternativa, puoi usare Intune per distribuire le impostazioni AOVPN tramite la configurazione XML. Uno dei vantaggi di prendere la rotta di Intune è che Intune può gestire computer non aggiunti a un dominio, quindi è possibile teoricamente includere i computer domestici e personali degli utenti nell'infrastruttura gestita di Intune e configurarli per la connessione.

SCCM e Intune sono ottimi, ma non tutti li eseguono. Esiste una terza opzione per distribuire le impostazioni di Always On VPN tramite script di PowerShell. Sebbene questo sia il piano B di Microsoft (preferirebbero davvero che implementassi AOVPN tramite un MDM), temo che PowerShell sarà la realtà per molti clienti SMB che desiderano utilizzare AOVPN. Il più grande svantaggio dell'utilizzo di PowerShell per mettere in atto le impostazioni di AOVPN è che PowerShell deve essere eseguito in modalità elevata, il che significa che è difficile da automatizzare perché l'utente connesso (che è dove è necessario stabilire la connessione VPN) deve essere un amministratore locale affinché lo script venga eseguito correttamente.

Spero e sto aspettando con ansia il giorno in cui annunceranno un modello di criteri di gruppo per l'implementazione delle impostazioni VPN Always On, ma finora non si sa se sarà o meno un'opzione. Tutti hanno Criteri di gruppo; non tutti hanno MDM. Leggerai tra qualche istante che l'implementazione delle impostazioni di connettività di Microsoft DirectAccess (un'alternativa ad AOVPN) viene eseguita tramite Criteri di gruppo, che è incredibilmente facile da capire e gestire. Per quanto mi riguarda, al momento della stesura di questo articolo, DirectAccess detiene un grande vantaggio su AOVPN nel modo in cui gestisce l'implementazione delle impostazioni sul lato client. Ma assicurati di controllare Microsoft Docs online per trovare le informazioni più recenti su questo argomento, poiché AOVPN viene continuamente migliorato e probabilmente ci saranno alcuni cambiamenti in arrivo in quest'area della tecnologia.

Componenti del server AOVPN

Ora che abbiamo capito cosa è necessario dal lato client per realizzare Always On VPN, quali parti e pezzi sono necessari sul lato server / infrastruttura per consentire che queste connessioni avvengano? È interessante notare che il componente Always On di AOVPN non ha nulla a che fare con l'infrastruttura del server; la parte Always On viene gestita completamente sul lato client. Pertanto, tutto ciò che dobbiamo fare sul lato server è assicurarci di poter ricevere connessioni VPN in entrata. Se attualmente hai una forza lavoro che sta effettuando connessioni VPN di successo, allora ci sono buone probabilità che tu abbia già l'infrastruttura server necessaria per portare AOVPN nel tuo ambiente.

Server di accesso remoto

Ovviamente, hai bisogno di un server VPN per poter ospitare connessioni VPN, giusto? Beh, non così ovviamente. In Windows Server, il ruolo che ospita le connessioni VPN, AOVPN e DirectAccess è chiamato ruolo di accesso remoto, ma puoi effettivamente fare in modo che Always On VPN funzioni senza un server Windows come server di accesso remoto. Poiché la parte Always On è la funzionalità lato client, ciò consente alle infrastrutture lato server VPN di essere ospitate da fornitori di terze parti. Anche se tecnicamente accurato, non è proprio quello che Microsoft si aspetta; né è quello che trovo sul campo. In realtà, quelli di noi interessati a utilizzare Microsoft Always On VPN utilizzeranno Microsoft Windows Server per ospitare il ruolo di accesso remoto, che sarà il sistema in entrata a cui si connetteranno i nostri client remoti.

Molte persone presumono automaticamente che AOVPN sia sposato con Windows Server 2019 perché è una tecnologia nuovissima e Server 2019 è stato appena rilasciato, ma in realtà non è affatto così. Puoi ospitare la tua infrastruttura VPN (il ruolo di accesso remoto) su Server 2019, Server 2016 o anche Server 2012 R2. Funziona allo stesso modo sul back-end, offrendo ai clienti un posto in cui attingere con le loro connessioni VPN.

Dopo aver installato il ruolo di accesso remoto sul tuo nuovo Windows Server, scoprirai che la maggior parte della configurazione VPN avviene dalla console di Routing e Accesso remoto (RRAS). Durante la configurazione della tua VPN, scoprirai che ci sono più protocolli che possono essere utilizzati per stabilire una connessione VPN tra client e server e dovresti avere almeno una breve comprensione di quali sono questi diversi protocolli. Li elencherò qui in ordine di più forte e più sicuro, fino in fondo per non toccare questo!

IKEv2

IKEv2 è il modo più nuovo, più potente e, nel complesso, migliore per connettere i tuoi computer client tramite VPN o AOVPN, IKEv2 è l'unico modo per connettere l'AOVPN Device Tunnel. IKEv2 richiede

l'emissione di certificati macchina ai computer client per l'autenticazione. Ciò significa generalmente che se si desidera che i client si connettano tramite IKEv2, tali client verranno aggiunti a un dominio. È molto importante notare che IKEv2 utilizza le porte UDP 500 e 4500 per effettuare la connessione.

SSTP

Considerato il metodo di fallback per la connessione di connessioni AOVPN, SSTP utilizza un flusso SSL per connettersi. Per questo motivo, richiede l'installazione di un certificato SSL sul server di accesso remoto, ma non richiede i certificati del computer sui computer client. SSTP utilizza la porta TCP 443, quindi è in grado di connettersi anche da reti molto restrittive in cui IKEv2 potrebbe non funzionare (a causa della dipendenza di IKEv2 da UDP).

L2TP

Non generalmente utilizzato per le distribuzioni AOVPN, L2TP è in grado di stabilire connessioni VPN utilizzando certificati o una chiave precondivisa. Dato che hai già due protocolli migliori a tua disposizione, non dovresti usare questo.

PPTP

Sebbene sia ancora un'opzione di configurazione valida all'interno di RRAS, stai lontano da questo ragazzo! PPTP è stato essenzialmente violato e se stai ancora eseguendo connessioni VPN basate su PPTP, devi fondamentalmente considerare quei flussi di traffico come non crittografati e con testo in chiaro su Internet.

Autorità di certificazione (CA)

Certificati macchina, certificati utente, certificati SSL ... Oh, mio! Chiaramente è necessario avere familiarità con l'utilizzo e la distribuzione di certificati per poter utilizzare Always On VPN. Questo sta diventando sempre più comune con le nuove tecnologie ben protette di qualsiasi gusto. Il requisito principale qui è che dovrai avere PKI all'interno del tuo ambiente e almeno un server CA Windows per emettere i certificati necessari. Di seguito è riportato un elenco dei luoghi in cui i certificati potrebbero essere utilizzati da un'infrastruttura AOVPN:

- **Certificati utente**: Sono i certificati rilasciati agli utenti VPN da una CA interna, utilizzati per l'autenticazione del tunnel utente.
- **Certificati macchina**: Si tratta di certificati rilasciati alle workstation (principalmente laptop) da una CA interna, utilizzati per l'autenticazione del tunnel dei dispositivi.
- **Certificato SSL**: Installato sul server di accesso remoto per convalidare il traffico in entrata per le connessioni VPN SSTP.

- **Certificati macchina VPN e NPS**: Il tuo server di accesso remoto, così come i tuoi server NPS, di cui parleremo tra un minuto, richiedono certificati macchina emessi dalla tua CA interna.

Server dei criteri di rete (NPS)

NPS è fondamentalmente il metodo di autenticazione per le connessioni VPN. Quando arriva una richiesta di connessione VPN, il server di accesso remoto passa la richiesta di autenticazione a un server dei criteri di rete per convalidare l'identità dell'utente e anche per verificare che l'utente disponga delle autorizzazioni per accedere tramite VPN.

Più comunemente, quando si lavora con le connessioni Microsoft VPN, configuriamo NPS in modo che consenta solo agli utenti che fanno parte di un determinato gruppo di sicurezza di Active Directory. Ad esempio, se crei un gruppo chiamato Utenti VPN e quindi punti NPS a quel gruppo, consentirà solo agli utenti che hai inserito all'interno di quel gruppo di effettuare connessioni VPN di successo.

NPS è un altro ruolo di Windows Server che può essere ospitato sul proprio sistema o distribuito su più server per la ridondanza. Come per il ruolo di accesso remoto stesso, non è previsto alcun requisito Server 2019 per Server dei criteri di rete. Potresti facilmente distribuirlo anche sulle versioni precedenti di Windows Server.

Negli ambienti di piccole dimensioni che dispongono di un solo server di accesso remoto, è comune ospitare il ruolo NPS direttamente sullo stesso server che fornisce la connettività VPN.

Accesso diretto

Durante la nostra discussione su Always On VPN, ho menzionato Microsoft DirectAccess un paio di volte. DirectAccess è un'altra forma di connettività automatica simile a VPN, ma richiede un approccio diverso da quello di Always On VPN. Laddove AOVPN utilizza semplicemente protocolli VPN noti e ben noti e fa una magia astuta per avviare automaticamente quei tunnel VPN altrimenti tradizionali, i tunnel DirectAccess sono piuttosto proprietari.
I tunnel sono protetti da IPsec e sono essenzialmente impenetrabili e anche impersonabili. Trovo che i team di sicurezza adorino le protezioni e la complessità che circondano i tunnel DA perché è una piattaforma di connessione che gli aggressori non hanno idea di come manomettere o come replicare.

Nella mia esperienza, a questo punto del gioco, Microsoft DirectAccess è il motivo più comune per cui gli amministratori distribuiscono il ruolo di accesso remoto su un server Windows. Come affermato, il modo più semplice per pensare a DirectAccess è pensarlo come una VPN automatica. Simile alla VPN, il suo scopo è connettere i computer degli utenti alla rete aziendale quando si trovano fuori dall'ufficio. Diverso dalla VPN, tuttavia, è il metodo utilizzato dai dipendenti per rendere possibile questa connessione. DirectAccess non è un componente software, è una serie di componenti già integrati nel sistema operativo Windows, che lavorano in tandem per fornire un accesso completamente trasparente per l'utente. Cosa intendo per seamless? Allo stesso modo in cui AOVPN si connette senza l'interazione dell'utente, l'utente non deve fare nulla per connettersi a DirectAccess. Lo fa da solo. Non appena il computer portatile riceve una connessione Internet, indipendentemente dal fatto che si tratti di una connessione Wi-Fi domestica, Internet pubblica in un bar o una connessione hotspot del telefono cellulare, i tunnel DirectAccess si costruiscono automaticamente utilizzando qualsiasi connessione Internet disponibile, senza alcun utente ingresso.

Sia che utilizzi Always On VPN o DirectAccess, quando il tuo computer si connette automaticamente ti fa risparmiare tempo e denaro. Il tempo viene risparmiato perché l'utente non deve più avviare una connessione VPN. Si risparmia denaro perché il tempo è uguale al denaro, ma anche perché avere una connessione sempre attiva significa che l'applicazione di patch, le politiche di sicurezza e la gestione di quei computer remoti avvengono sempre, anche quando l'utente lavora da remoto. Non è più necessario attendere che gli utenti tornino in ufficio o che scelgano di avviare la connessione VPN manuale per inviare nuove impostazioni e criteri ai propri computer; succede tutto ovunque si trovino, purché abbiano accesso a Internet. Chiaramente, con l'avvento di due diverse tecnologie di accesso remoto, entrambe focalizzate sulla connettività automatica per gli utenti remoti, Microsoft sta aprendo la strada a una forza lavoro più produttiva. I termini user-friendly e VPN non sono mai andati di pari passo prima, ma nelle ultime versioni dei sistemi operativi Windows, questo è esattamente l'obiettivo.

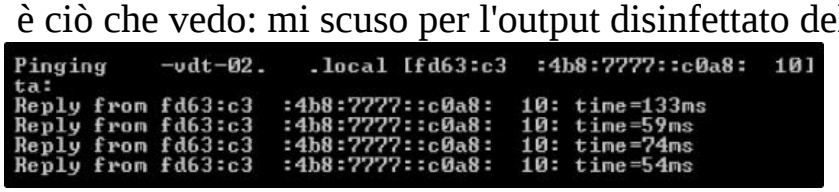
DirectAccess esiste dal rilascio di Windows Server 2008 R2, eppure mi imbatto regolarmente in persone che non ne hanno mai sentito parlare. All'inizio era piuttosto difficile da distribuire e presentava molti requisiti scomodi, ma molto è cambiato negli ultimi anni e DirectAccess è ora più facile che mai da distribuire e più vantaggioso che mai da eseguire nel proprio ambiente .

La verità su DirectAccess e IPv6

Uno dei requisiti scomodi che ho menzionato era la necessità di IPv6 all'interno della tua rete. Con la prima versione di DirectAccess, questo era un requisito sfortunato. Dico sfortunato perché, anche oggi, nel 2019, quasi nessuno esegue IPv6 all'interno delle proprie reti aziendali, figuriamoci anni fa, quando è stata rilasciata questa tecnologia, molti amministratori non sapevano nemmeno cosa fosse IPv6. Fortunatamente, il requisito per IPv6 all'interno delle tue reti non esiste più. Ripeto, nel caso in cui qualcuno non prestasse attenzione o leggesse documenti TechNet vecchi e obsoleti, non è necessario IPv6 per utilizzare

DirectAccess! Ho visto troppi casi in cui DirectAccess è stato considerato da un'azienda, ma il progetto è stato messo da parte perché la lettura su TechNet ha fatto credere loro che IPv6 fosse un requisito e hanno scartato DirectAccess come qualcosa che non avrebbe t lavoro. Non è assolutamente necessario eseguire IPv6 nella rete per far funzionare DirectAccess, ma è importante capire in che modo DirectAccess utilizza IPv6, perché inizierai a incontrarlo una volta avviata la distribuzione.

Quando sono seduto a casa, lavorando sul mio laptop aziendale, DirectAccess mi connette alla rete aziendale. La mia rete interna al lavoro non ha assolutamente IPv6 in esecuzione al suo interno; al momento siamo una rete completamente IPv4. Questo è vero per la maggior parte delle aziende oggi. Tuttavia, quando apro il prompt dei comandi ed eseguo il ping di uno dei miei server dal mio laptop DirectAccess, questo è ciò che vedo: mi scuso per l'output disinfettato dello screenshot:



Che diavolo è quello? A me sembra IPv6. È qui che entra in gioco IPv6 con DirectAccess. Tutto il traffico che si sposta sulla parte Internet della connessione, tra il mio laptop e il server DirectAccess che si trova nel mio data center, è traffico IPv6. La mia rete interna è IPv4 e il mio server DirectAccess ha solo indirizzi IPv4, eppure il mio tunnel DirectAccess trasporta il mio traffico utilizzando IPv6. Questo è il fulcro del funzionamento di DirectAccess e non può essere modificato. Il tuo laptop DA invia pacchetti IPv6 crittografati IPsec su Internet al server DA e quando il server DA riceve quei pacchetti, ha la capacità di convertirli in IPv4 per inviarli al server di destinazione all'interno della rete aziendale. Ad esempio, quando apro il mio Outlook e provo a connettermi al mio server Exchange, i miei pacchetti di Outlook scorrono sul tunnel DirectAccess come IPv6. Una volta che questi pacchetti raggiungono il mio server DirectAccess, quel server DA raggiunge il DNS interno per capire se il mio server Exchange è IPv4 o IPv6. Se si esegue effettivamente IPv6 all'interno della rete e il server Exchange è disponibile tramite IPv6, il server DA invierà semplicemente i pacchetti IPv6 al server Exchange. Connessione completata! Se, d'altra parte, stai eseguendo IPv4 all'interno della tua rete, il server DA vedrà solo un singolo record host nel DNS, il che significa che il server Exchange è solo IPv4. Il server DirectAccess manipolerà quindi il pacchetto IPv6, trasformandolo in IPv4 e quindi lo invierà al server Exchange. Le due tecnologie che gestiscono questa manipolazione dei pacchetti sono DNS64 e NAT64, che probabilmente hai visto in parte della

documentazione se hai letto qualcosa su DirectAccess in linea. Lo scopo di queste tecnologie è quello di cambiare il flusso di pacchetti IPv6 in entrata in IPv4 per le reti in cui è richiesto, che è praticamente ogni rete al momento, e ruotare il traffico di ritorno da IPv4 in IPv6 in modo che possa farsi strada torna al computer client DirectAccess tramite il tunnel IPsec basato su IPv6 che connette il client DA al server DA su Internet.

È importante comprendere che DirectAccess utilizza IPv6 in questa capacità, perché qualsiasi criterio di sicurezza che potresti avere in atto per eliminare IPv6 nei computer client per impostazione predefinita impedirà a DirectAccess di funzionare correttamente nel tuo ambiente. Dovrai invertire questi criteri per consentire ai client di inviare pacchetti IPv6 e ottenere il loro traffico su Internet. Tuttavia, è anche molto importante capire che non è necessaria alcuna parvenza di IPv6 in esecuzione all'interno della rete aziendale per farlo funzionare, poiché il server DirectAccess può convertire tutto il traffico in IPv4 prima che raggiunga quella rete interna e la maggior parte Le implementazioni DA che sono attive oggi vengono eseguite esattamente in questo modo.

Prerequisiti per DirectAccess

DirectAccess ha molte parti mobili e sono disponibili molti modi diversi per configurarlo. Tuttavia, non tutti questi modi sono buone idee. Quindi, in questa sezione, discuteremo alcune delle grandi decisioni che dovrai prendere durante la progettazione del tuo ambiente DirectAccess.

Aggiunto a un dominio

Il primo grande requisito è che i sistemi coinvolti con DirectAccess debbano essere aggiunti a un dominio. Il tuo server DA, o i tuoi server, devono essere tutti uniti al tuo dominio e tutti i computer client che desideri siano collegati a DA devono essere uniti anche a un dominio. L'appartenenza al dominio è necessaria per scopi di autenticazione e anche perché le impostazioni del client DirectAccess che devono essere applicate ai computer portatili arrivano a questi computer tramite Criteri di gruppo. Mi piace sempre sottolineare questo requisito nelle prime fasi del processo di pianificazione, perché significa che gli utenti che acquistano i propri laptop in un punto vendita in genere non saranno in grado di utilizzare DirectAccess, a meno che tu non sia d'accordo con l'aggiunta di computer di casa al tuo dominio, quindi DA è davvero una tecnologia progettata per la gestione e collegando le risorse aziendali che

puoi aggiungere al dominio. È inoltre importante comprendere questo requisito dal punto di vista della sicurezza, poiché il server o i server DirectAccess si troveranno in genere ai margini della rete. È comune che la scheda NIC esterna su un server DA si trovi all'interno di una DMZ, ma devono anche essere aggiunte a un dominio, il che potrebbe non essere qualcosa a cui sei abituato con i sistemi in una rete perimetrale. dal momento che il tuo server o i tuoi server DirectAccess si troveranno in genere ai margini della tua rete. È comune che la scheda NIC esterna su un server DA si trovi all'interno di una DMZ, ma devono anche essere aggiunte a un dominio, il che potrebbe non essere qualcosa a cui sei abituato con i sistemi in una rete perimetrale. poiché il tuo server o i tuoi server DirectAccess si troveranno in genere al limite della tua rete. È comune che la scheda NIC esterna su un server DA si trovi all'interno di una DMZ, ma devono anche essere aggiunte a un dominio, il che potrebbe non essere qualcosa a cui sei abituato con i sistemi in una rete perimetrale.

Sistemi operativi client supportati

Non tutti i sistemi operativi client Windows contengono i componenti necessari per far funzionare una connessione DirectAccess. Enterprise sì, che copre la maggior parte delle aziende più grandi che possiedono sistemi operativi Microsoft, ma che certamente non include tutti. Vedo ancora molte piccole imprese che utilizzano SKU professionali o anche domestiche sui loro computer client e queste versioni non includono i componenti DirectAccess. Di seguito è riportato un elenco dei sistemi operativi che supportano DirectAccess. Durante la pianificazione, dovrai assicurarti che i tuoi computer portatili eseguano uno di questi:

- Windows 10 Enterprise
- Windows 10 Education
- Windows 8.0 o 8.1 Enterprise
- Windows 7 Enterprise
- Windows 7 Ultimate

I server DirectAccess ottengono uno o due NIC

Una grande domanda a cui è necessario rispondere anche prima di installare il ruolo di accesso remoto sul nuovo server è: quante schede NIC sono necessarie su questo server? Esistono due metodi supportati per l'implementazione di DirectAccess.

Modalità NIC singola

Il tuo server DirectAccess può essere installato con un solo NIC. In questo caso, in genere si collega quella connessione di rete direttamente alla rete interna in modo che abbia accesso a tutte le risorse interne che i computer client dovranno contattare durante le sessioni DA dell'utente. Per ottenere traffico da Internet al server DirectAccess, è necessario stabilire una NAT (Network Address Translation) da un indirizzo IP pubblico a qualsiasi indirizzo IP interno assegnato al server DA. A molti

amministratori della sicurezza di rete questo metodo non piace, perché significa creare un NAT che porta il traffico direttamente nella rete aziendale senza passare attraverso alcun tipo di DMZ.

Posso anche dirti per esperienza che la modalità NIC singola non funziona sempre correttamente. Fa un ottimo lavoro di avviare un laboratorio di prova veloce o una prova di concetto, ma ho riscontrato troppi problemi sul campo con persone che cercano di eseguire ambienti DirectAccess di produzione su una singola scheda NIC. La possibilità di utilizzare solo una singola scheda di rete è stata aggiunta a DirectAccess nelle versioni più recenti, quindi non era originariamente progettata per funzionare in questo modo. Pertanto, ti consiglio vivamente, per la tua installazione DA di produzione, di farlo nel modo giusto e di andare con ...

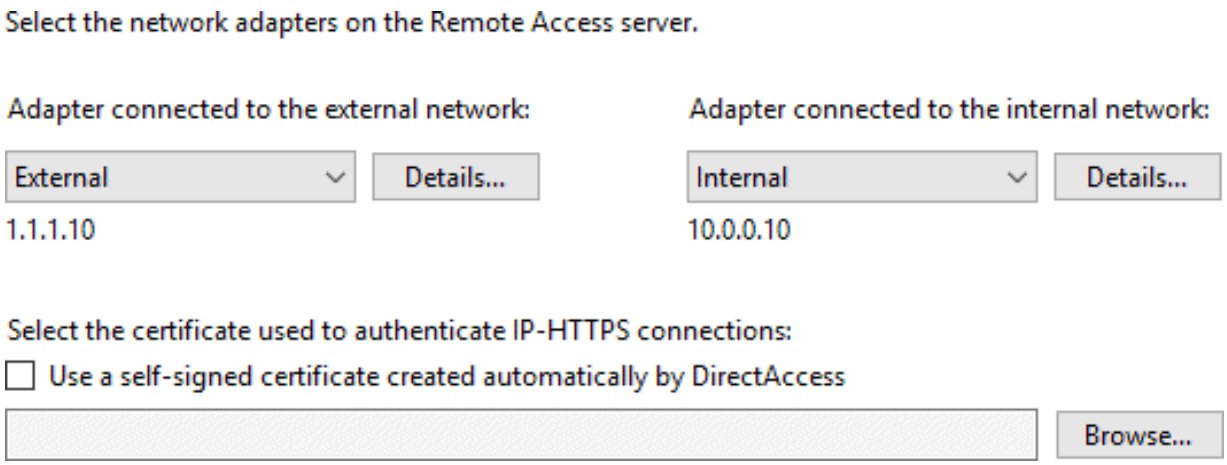
Dual NIC

Qui abbiamo due schede di rete nel server DirectAccess. La scheda NIC interna in genere viene collegata direttamente alla rete aziendale e la posizione fisica della scheda NIC esterna può variare a seconda dell'organizzazione. Discuteremo i pro ei contro di dove posizionare la scheda NIC esterna subito dopo questa sezione del capitolo. La modalità Edge con due NIC è il modo in cui DirectAccess funziona meglio. Come ricorderai in precedenza nel libro, l'implementazione di un server Windows con più NIC significa che effettuerai il multihoming di questo server e dovrai configurare le impostazioni di rete di conseguenza. Con un server di accesso remoto, la scheda NIC esterna è sempre quella che riceve le impostazioni del gateway predefinito, quindi è necessario assicurarsi di seguire questa regola e non configurare un gateway predefinito sulla scheda NIC interna. D'altro canto, si desidera configurare gli indirizzi del server DNS nelle proprietà della NIC interna, ma non si desidera configurare i server DNS per la NIC esterna. Poiché questo server è multihomed, sarà probabilmente necessario creare alcune istruzioni di route per aggiungere le sottoreti aziendali alla tabella di routing di Windows di questo server prima che sia in grado di inviare e ricevere traffico correttamente. Le uniche reti che non avrebbero bisogno di ospitare l'aggiunta di route statiche sarebbero le piccole reti, in cui tutti i dispositivi interni si trovano su una singola sottorete. In tal caso, non è necessario immettere route statiche. Ma la maggior parte delle reti aziendali si estende su più sottoreti e in questo caso dovresti fare

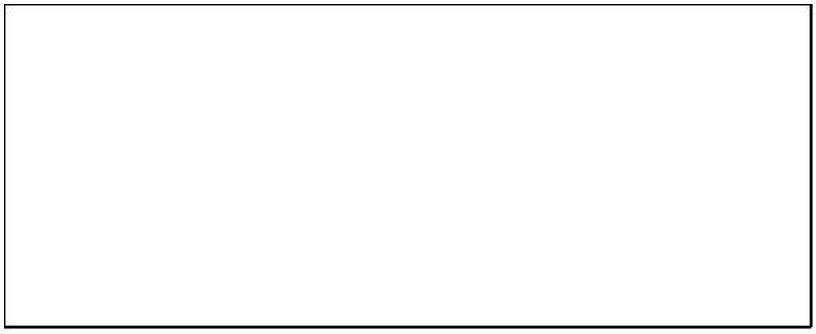
riferimento a probabilmente sarà necessario creare alcune istruzioni di route per aggiungere le sottoreti aziendali alla tabella di routing di Windows di questo server prima che sia in grado di inviare e ricevere traffico con successo. Le uniche reti che non avrebbero bisogno di ospitare l'aggiunta di route statiche sarebbero le piccole reti, in cui tutti i dispositivi interni si trovano su una singola sottorete. In tal caso, non è necessario immettere route statiche. Ma la maggior parte delle reti aziendali si estende su più sottoreti e in questo caso dovresti fare riferimento a probabilmente sarà necessario creare alcune istruzioni di route per aggiungere le sottoreti aziendali alla tabella di routing di Windows di questo server prima che sia in grado di inviare e ricevere traffico con successo. Le uniche reti che non avrebbero bisogno di ospitare l'aggiunta di route statiche sarebbero le piccole reti, in cui tutti i dispositivi interni si trovano su una singola sottorete. In tal caso, non è necessario immettere route statiche. Ma la maggior parte delle reti aziendali si estende su più sottoreti e in questo caso dovresti fare riferimento a dove tutti i tuoi dispositivi interni si trovano su una singola sottorete. In tal caso, non è necessario immettere route statiche. Ma la maggior parte delle reti aziendali si estende su più sottoreti e in questo caso dovresti fare riferimento a dove tutti i tuoi dispositivi interni si trovano su una singola sottorete. In tal caso, non è necessario immettere route statiche. Ma la maggior parte delle reti aziendali si estende su più sottoreti e in questo caso dovresti fare riferimento aCapitolo 5, Collegamento in rete con Windows Server 2019, in cui abbiamo discusso del multihoming e di come creare tali istruzioni di route.

Più di due NIC

No, non andarci. Se hai familiarità con la configurazione di router o firewall, sai che hai il potenziale per installare molti diversi NIC su un server e collegarli tutti a sottoreti diverse. Sebbene ci siano molte ragioni per cui suddividere l'accesso alla rete in questo modo su un server di accesso remoto potrebbe essere vantaggioso, non funzionerà come desideri. La configurazione di DirectAccess stessa è in grado di gestire solo due diverse interfacce di rete.



Come puoi vedere nello screenshot seguente, nel corso delle procedure guidate di installazione, dovrai definire una NIC come Esterna e l'altra come Interna. Sfortunatamente, qualsiasi altra scheda NIC esistente in quel server non verrà utilizzata da DirectAccess. Forse questo è qualcosa che cambierà nelle versioni future!



A NAT o non a NAT?

Ora che hai deciso di utilizzare due NIC nel tuo server DirectAccess, dove colleghiamo la NIC esterna? Esistono due luoghi comuni a cui è possibile connettere questa interfaccia di rete esterna, ma a seconda di quale si sceglie, il risultato dell'ambiente DirectAccess può essere notevolmente diverso. Prima di parlare del posizionamento effettivo della scheda NIC, vorrei definire un paio di protocolli che è importante capire, perché riguardano molto la risposta a questa domanda sul posizionamento della scheda NIC. Quando il laptop DirectAccess effettua una connessione al server DirectAccess, lo farà utilizzando uno dei tre protocolli di tunneling di transizione IPv6. Questi protocolli sono 6to4, Teredo e IP-HTTPS.

Quando il client DA connette i suoi tunnel DA, sceglierà automaticamente quale di questi protocolli è meglio usare, a seconda della connessione Internet corrente dell'utente. Tutti e tre i protocolli svolgono la stessa funzione per una connessione DirectAccess: il loro compito è prendere il flusso di pacchetti IPv6 che esce dal laptop e incapsularlo all'interno di IPv4 in modo che il traffico possa farsi strada con successo attraverso Internet IPv4. Quando i pacchetti arrivano al server DirectAccess, vengono decappati in modo che il server DA possa elaborare questi pacchetti IPv6.

6to4

I client DA tenteranno di connettersi utilizzando 6to4 solo quando un laptop remoto ha un vero indirizzo IP pubblico. Questo non accade quasi mai in questi giorni, con la carenza di indirizzi Internet IPv4 disponibili, quindi 6to4 in genere non viene utilizzato da alcun computer client DirectAccess. In effetti, può presentare una serie di sfide quando gli utenti si connettono con le schede del telefono cellulare nei loro laptop, quindi è pratica comune disabilitare l'adattatore 6to4 sui computer client come impostazione di best practice per DirectAccess.

Teredo

Quando i client DA sono connessi a Internet utilizzando un indirizzo IP privato, ad esempio dietro un router domestico o un router Wi-Fi pubblico, tenteranno di connettersi utilizzando il protocollo Teredo. Teredo utilizza un flusso UDP per incapsulare i pacchetti DA e quindi, finché la connessione Internet dell'utente consente UDP 3544 in uscita, Teredo si connetterà generalmente ed è il protocollo di transizione preferito per quella connessione DirectAccess.

IP-HTTPS

Se Teredo non riesce a connettersi, ad esempio nel caso in cui l'utente si trovi in una rete che blocca UDP in uscita, la connessione DirectAccess tornerà a utilizzare IP-HTTPS, pronunciato IP su HTTPS. Questo protocollo incapsula i pacchetti IPv6 nelle intestazioni IPv4, ma poi li avvolge in un'intestazione HTTP e li crittografa con TLS / SSL, prima di inviare il pacchetto su Internet. Ciò rende effettivamente la connessione DirectAccess un flusso SSL, proprio come quando si esplora un sito Web HTTPS.

Installazione sul vero limite: su Internet

Quando colleghi la scheda di rete esterna del tuo server DirectAccess direttamente a Internet, ti concedi la possibilità di inserire veri indirizzi IP pubblici su quella scheda di rete. In questo modo, abiliti tutti e tre i precedenti protocolli di tunneling di transizione, in modo che i computer client DirectAccess possano scegliere tra di essi per la migliore forma di connettività. Quando si installa tramite il metodo true edge, si inseriscono non solo uno, ma due indirizzi IP pubblici su quella NIC esterna. Assicurati che gli indirizzi IP pubblici siano simultanei poiché questo è un requisito per Teredo. Quando il server DirectAccess dispone di due indirizzi IP pubblici simultanei assegnati alla scheda NIC esterna, consentirà al protocollo Teredo di essere disponibile per le connessioni.

La scheda NIC non deve essere necessariamente collegata direttamente a Internet affinché funzioni. A seconda delle capacità del firewall, potresti avere la possibilità di stabilire una DMZ con bridge in cui non è in corso alcun NAT. È necessario verificare con il fornitore del firewall per scoprire se questa è un'opzione per la propria organizzazione. In questo scenario, puoi ancora configurare i veri indirizzi IP pubblici sulla scheda NIC esterna, ma il traffico passa prima attraverso

Installazione dietro un NAT

È molto più comune che il team di rete desideri posizionare la scheda di rete esterna del server DirectAccess dietro un firewall, all'interno di una DMZ. Questo in genere significa creare un NAT per portare questo traffico nel server. Sebbene ciò sia del tutto possibile e protegga meglio il server DirectAccess stesso da Internet, presenta un grosso svantaggio. Quando installi un server DA dietro un NAT, Teredo non funziona più. In effetti, le procedure guidate di configurazione di DirectAccess riconosceranno quando hai un indirizzo IP privato elencato nella scheda di rete esterna e non attiveranno nemmeno Teredo.

Quando Teredo non è disponibile, tutti i client DirectAccess si connetteranno utilizzando IP-HTTPS. Allora perché è importante anche se Teredo non è disponibile? Perché è un protocollo più efficiente di IP-HTTPS. Quando Teredo esegue il tunneling dei pacchetti, incapsula semplicemente IPv6 all'interno di IPv4. Il flusso di traffico DirectAccess è già e sempre crittografato con IPsec, quindi non è necessario che il tunnel Teredo esegua alcuna crittografia aggiuntiva. D'altra parte, quando IP-HTTPS esegue il tunneling dei pacchetti, prende il flusso di traffico IPsec già crittografato e lo crittografa una seconda volta utilizzando SSL. Ciò significa che tutti i pacchetti che vanno e vengono sono soggetti a doppia crittografia, che aumenta l'elaborazione e i cicli della CPU e rende la connessione più lenta. Crea inoltre un carico hardware aggiuntivo sul server DirectAccess stesso,

Questo è un problema particolarmente evidente quando si esegue Windows 7 su computer client, poiché l'elaborazione della doppia crittografia causerà una connessione notevolmente più lenta per gli utenti. DirectAccess funziona ancora bene, ma se siedi un laptop

connesso a Teredo accanto a un laptop connesso IP-HTTPS, noterai la differenza di velocità tra i due.

Per fortuna, in Windows 8 e Windows 10, sono state aggiunte alcune contromisure per aiutare con questa discrepanza di velocità. Questi nuovi sistemi operativi client sono ora abbastanza intelligenti da poter negoziare la parte SSL del tunnel IP-HTTPS utilizzando l'algoritmo di crittografia NULL, il che significa che IP-HTTPS non sta eseguendo una seconda crittografia e le prestazioni IP-HTTPS sono ora alla pari con Teredo.

Tuttavia, questo funziona solo per i sistemi operativi client più recenti (Win7 eseguirà sempre la doppia crittografia con IP-HTTPS) e in alcuni casi non funziona ancora. Ad esempio, quando abiliti il tuo server DirectAccess per fornire anche la connettività VPN o se scegli di utilizzare un sistema OTP (One-Time-Password) insieme a DirectAccess, l'algoritmo NULL verrà disabilitato perché è un rischio per la sicurezza in queste situazioni e quindi anche i computer Windows 8 e Windows 10 eseguiranno la doppia crittografia quando si connettono tramite IP-HTTPS. Puoi vedere dove sarebbe utile avere Teredo abilitato e disponibile in modo che tutti i computer che possono connettersi tramite Teredo lo faranno.

Per riassumere, puoi certamente installare la scheda di rete esterna del tuo server DirectAccess dietro un NAT, ma tieni presente che tutti i computer client DA si connetteranno utilizzando il protocollo IP-HTTPS ed è importante comprendere il potenziale effetto collaterale dell'implementazione in questo modo.

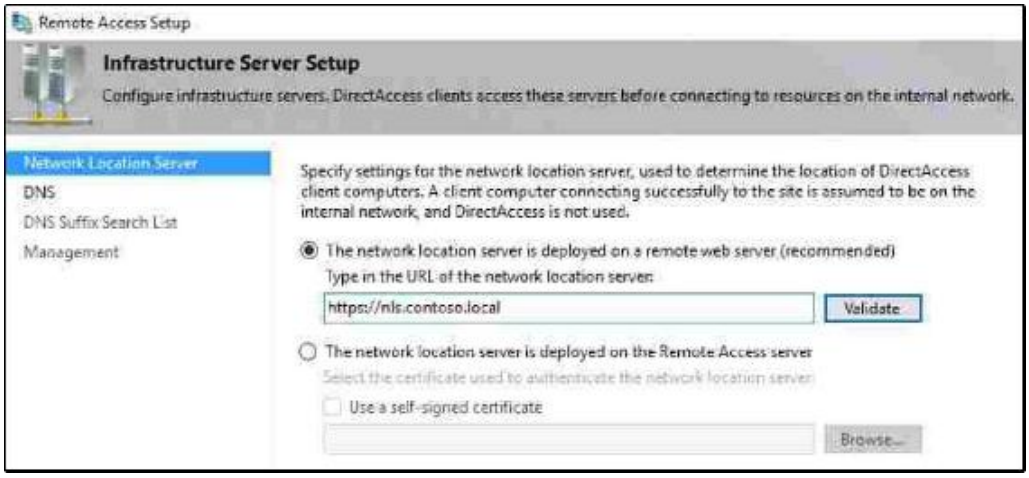
Network Location Server

Questo componente principale in un'infrastruttura DirectAccess è qualcosa che non esiste nemmeno sul server DA stesso, o almeno non dovrebbe se si stanno impostando le cose correttamente. Network Location Server (NLS) è semplicemente un sito Web che viene eseguito all'interno di
rete aziendale. Questo sito Web non deve essere disponibile per l'accesso su Internet; infatti, non dovrebbe essere. NLS viene utilizzato come parte del meccanismo di rilevamento interno / esterno sui computer client DirectAccess, in modo simile al modo in cui funziona Rilevamento rete attendibile per Always On VPN. Ogni volta che un client DA ottiene una connessione di rete, inizia a cercare il sito Web NLS. Se può vedere il sito, allora sa che sei all'interno della rete aziendale e DirectAccess non è richiesto, quindi si spegne. Tuttavia, se il tuo sito Web NLS non può essere contattato, significa che sei fuori dalla rete aziendale e i componenti DirectAccess inizieranno ad accendersi da soli.

Questo prerequisito è facilmente soddisfatto; tutto ciò che devi fare è avviare una VM e installare IIS su di essa per ospitare questo nuovo sito Web, oppure puoi persino aggiungere un nuovo sito Web a un server Web esistente nella tua rete. Ci sono solo due cose a cui prestare attenzione quando si configura il proprio sito web NLS.
Il primo è che deve essere un sito HTTPS e quindi richiede un certificato SSL. Discuteremo i certificati usati in DA, compreso questo, nella prossima sezione di questo capitolo. Oltre ad assicurarti che il sito web sia accessibile tramite HTTPS, devi anche assicurarti che il nome DNS che stai utilizzando per contattare questo sito web sia univoco. Si desidera eseguire questa operazione perché, qualunque sia il nome scelto per il sito Web NLS, quel nome non sarà risolvibile quando i computer client si trovano all'esterno della rete aziendale. Questo è in base alla progettazione, perché ovviamente non vuoi che i tuoi client DA siano in grado di contattare correttamente il sito Web NLS quando lavorano in remoto, in quanto ciò disabiliterebbe la loro connessione DirectAccess.

Il motivo per cui visualizzo il nome DNS univoco è che spesso vedo nuovi amministratori di DirectAccess che utilizzano un sito Web interno esistente come sito Web NLS. Ad esempio, se si dispone di https: // intranet in esecuzione come sito di SharePoint, è possibile utilizzarlo semplicemente nella configurazione DA come definizione del server NLS. Tuttavia, una volta impostato in questo modo, ti renderai presto conto che nessuno che lavora in remoto può accedere al sito Web https: // intranet. Questo è in base alla progettazione, perché l'ambiente DA ora considera il tuo sito Web intranet come il server NLS e non puoi risolverlo mentre sei mobile. La soluzione a questo problema? Assicurati di scegliere un nuovo nome DNS da utilizzare per questo sito Web NLS. Qualcosa piace https: //nls.contoso.local è adeguata.

La parte più importante del server dei percorsi di rete che voglio sottolineare è che dovresti assolutamente implementare questo sito Web su un server nella tua rete che non è il server DirectAccess stesso. Quando esegui le procedure guidate di configurazione DA, vedrai sullo schermo in cui definiamo NLS che è consigliabile distribuire NLS su un server web remoto, ma ti dà anche la possibilità di ospitare autonomamente il sito web NLS direttamente sul Server DirectAccess stesso. Non farlo! Ci sono molte cose che possono andare storte quando si co-host NLS sul server DA. L'esecuzione di NLS sul tuo server DA limita anche il tuo potenziale di DirectAccess in futuro, perché alcune delle configurazioni DA avanzate richiedono di rimuovere comunque NLS dal server DA, quindi potresti farlo correttamente la prima volta che lo configuri. Cambiare il tuo sito web NLS dopo aver eseguito DA in produzione può essere molto complicato e spesso va di traverso. Ho aiutato numerose aziende a spostare il loro sito Web NLS dopo aver realizzato che non possono co-ospitare NLS sul server DA se e quando desiderano aggiungere un secondo server DirectAccess per la crescita o la ridondanza. Di seguito uno screenshot della sezione della procedura guidata di configurazione DA in cui si sceglie la posizione di NLS. Assicurati di restare con la scatola superiore!


Remote Access Setup
Infrastructure Server Setup
Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.
Network Location Server
DNS
DNS Suffix Search List
Management
Specify settings for the network location server, used to determine the location of DirectAccess client computers. A client computer connecting successfully to the site is assumed to be on the internal network, and DirectAccess is not used.
The network location server is deployed on a remote web server (recommended)
Type in the URL of the network location server:
https://nls.contoso.local
Validate
The network location server is deployed on the Remote Access server
Select the certificate used to authenticate the network location server
Use a self-signed certificate
Browse...

Certificati utilizzati con DirectAccess

A parte la lettura e le incomprensioni su come DirectAccess utilizza IPv6, ecco la prossima più grande svolta per gli amministratori interessati a provare DirectAccess.
Una volta che inizi a leggere come funziona DA, ti renderai presto conto che i certificati sono richiesti in alcuni posti diversi. Sebbene le VPN generalmente richiedano anche l'uso di certificati, è certamente difficile distinguere quali certificati devono andare dove quando si sta guadando Microsoft Docs, quindi questa sezione chiarisce qualsiasi confusione esistente sui certificati DirectAccess. Non è davvero molto complicato, una volta che sai cosa è necessario e cosa non deve essere fatto.

Il prerequisito fondamentale è che tu abbia un server Windows CA da qualche parte nella tua rete. La statura della tua implementazione PKI non è così importante per DirectAccess. Abbiamo semplicemente bisogno della capacità di emettere certificati al nostro server DA e ai nostri client. Esistono solo tre posizioni in cui i certificati vengono utilizzati in DirectAccess e due di questi sono certificati SSL.

Certificato SSL sul server web NLS

Come accennato in precedenza, il tuo sito web NLS deve eseguire HTTPS. Ciò significa che sarà necessario installare un certificato SSL sul server che ospita il tuo sito web NLS. Supponendo che tu abbia un server CA interno, questo certificato può essere facilmente acquisito da quella CA interna, quindi non ci sono costi associati a questo certificato. Non è necessario acquistarne uno da una CA pubblica, poiché sarà possibile accedere e verificare questo certificato solo dai computer aggiunti al dominio, i client DirectAccess. Poiché i computer aggiunti a un dominio considerano automaticamente attendibili i server CA nella rete, questo certificato può essere semplicemente emesso dalla CA interna e farà esattamente ciò di cui abbiamo bisogno ai fini di DirectAccess.

Certificato SSL sul server DirectAccess

È inoltre necessario installare un certificato SSL sul server DirectAccess stesso, ma questo dovrebbe essere acquistato dall'autorità di certificazione pubblica. Questo certificato verrà utilizzato per convalidare i flussi di traffico IP-HTTPS in arrivo dai computer client, poiché si tratta di traffico SSL e quindi abbiamo bisogno di un certificato SSL per convalidarlo. Poiché il listener IP-HTTPS si trova di fronte a Internet pubblico, si consiglia vivamente di utilizzare un certificato di una CA pubblica, piuttosto che provare a utilizzare un certificato dalla PKI interna.

Se la tua azienda ha già un certificato SSL con caratteri jolly, usalo qui per risparmiare sui costi!

Certificati macchina sul server DA e su tutti i client DA

L'ultima e più complicata parte del rompicapo del certificato DirectAccess sono i certificati del computer. Una volta che sai cosa è richiesto, però, non è affatto difficile. Richiediamo semplicemente che un computer o un certificato macchina sia installato sul server DirectAccess, nonché su ogni computer client DirectAccess. Questo certificato macchina viene utilizzato come parte del processo di autenticazione per i tunnel IPsec. È una parte importante del modo in cui DirectAccess verifica che tu sia veramente chi dici di essere quando il tuo computer effettua la connessione DA.

Il modo migliore per emettere questi certificati macchina è accedere al server CA e creare un nuovo modello di certificato duplicato dal modello di computer integrato. Quando imposti il tuo nuovo modello di certificato, assicurati che soddisfi i seguenti criteri:

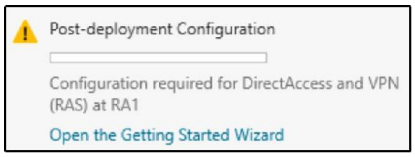
- Il nome comune (oggetto) del certificato deve corrispondere al nome di dominio completo del computer
- Il nome alternativo soggetto (SAN) del certificato deve essere uguale al nome DNS del computer
- Il certificato deve servire agli scopi previsti (utilizzo avanzato della chiave) sia dell'autenticazione client che dell'autenticazione server

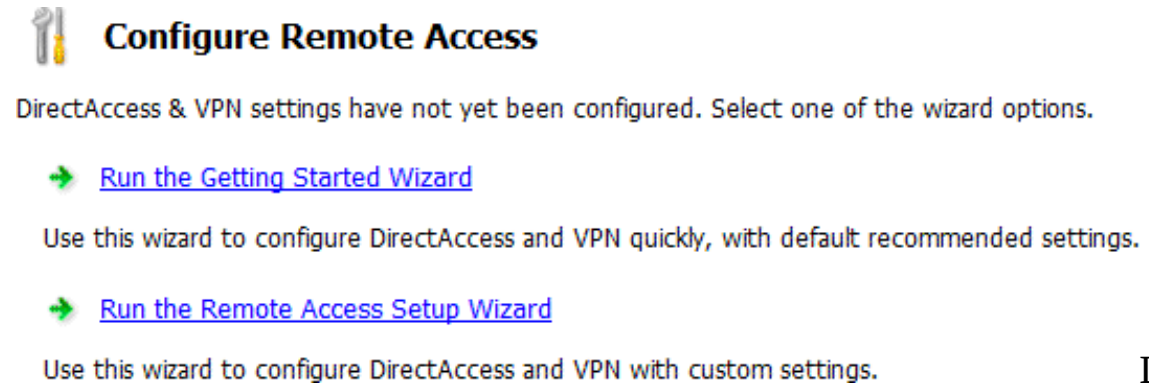
Dovrei notare qui, anche se non voglio, che il rilascio di questi certificati non è assolutamente necessario per far funzionare DirectAccess. Se stai eseguendo Windows 8 o versioni successive sul lato client, è possibile far funzionare DA senza certificati macchina.
I computer nella rete possono invece utilizzare qualcosa chiamato Kerberos Proxy per l'autenticazione del computer quando vengono creati i tunnel IPsec, ma consiglio vivamente di attenersi ai certificati. L'utilizzo dei certificati come parte del processo di autenticazione rende la connessione più stabile e più sicura. Inoltre, come con il posizionamento di NLS, se desideri eseguire funzioni avanzate con DirectAccess, come il

bilanciamento del carico o il multisito, o anche se desideri semplicemente connettere alcuni computer Windows 7 tramite DA, ti verrà richiesto di emettere certificati comunque. Quindi, attenersi innanzitutto alle best practice e rilasciare questi certificati prima ancora di iniziare a testare DirectAccess.

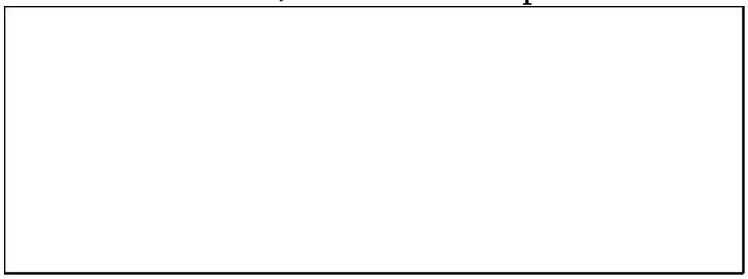
Non utilizzare la procedura guidata per l'avvio (GSW)!

Dopo aver preso le decisioni di progettazione necessarie e aver implementato i prerequisiti di cui abbiamo parlato finora, è finalmente giunto il momento di installare il ruolo Accesso remoto sul tuo nuovo server DirectAccess! Dopo aver terminato l'installazione del ruolo, analogamente a molti ruoli in Windows Server 2019, verrà visualizzato un messaggio che informa che è necessaria una configurazione aggiuntiva per utilizzare questo ruolo. Infatti, se segui il punto esclamativo giallo all'interno di Server Manager, l'unica opzione che ti viene presentata è Apri la procedura guidata per iniziare. Uffa! Questo non è ciò su cui vuoi fare clic:





La tua casa per le configurazioni DirectAccess è la Console di gestione dell'accesso remoto, che è disponibile dal menu Strumenti di Server Manager ora che il nostro ruolo di Accesso remoto è stato installato. Vai avanti e lancialo, e ora ci viene presentata una scelta:



Non fare clic su Esegui la procedura guidata per iniziare! GSW è un metodo di scelta rapida per l'implementazione di DirectAccess, progettato solo per rendere DA attivo e funzionante il più rapidamente possibile, forse per una rapida dimostrazione del concetto. In nessuna circostanza dovresti fidarti di GSW per il tuo ambiente DA di produzione, perché nel tentativo di rendere la configurazione semplice e veloce, vengono prese molte decisioni di configurazione che non sono best practice.

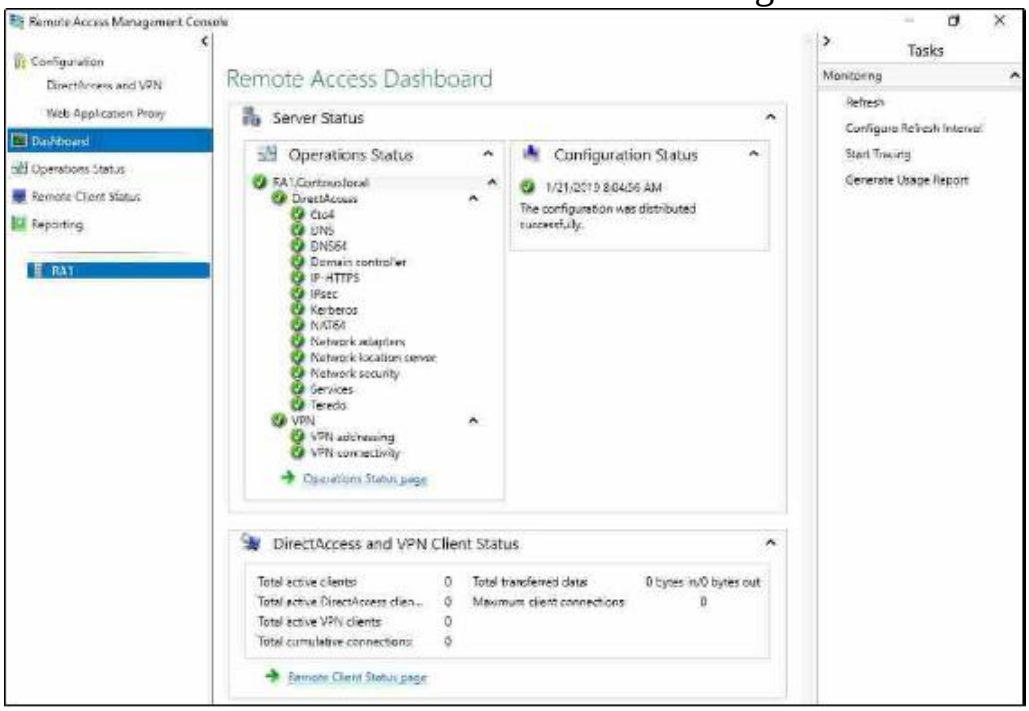
Devi assicurarti di fare clic su Esegui la procedura guidata di configurazione dell'accesso remoto invece quando ti viene richiesto per la prima volta nella console; in questo modo verrà richiamato il set completo di schermate di configurazione di DirectAccess. La configurazione DA consiste in una serie di quattro diversi passaggi, ciascuno contenente una manciata di schermate attraverso le quali navigherai per scegliere le opzioni di configurazione appropriate. C'è una buona quantità di dettagli su queste schermate, su cosa significa ognuna di esse e quali sono le tue opzioni, quindi non aver paura di immergerti e impostarle nel modo corretto. Se hai già configurato DirectAccess e hai utilizzato la Guida introduttiva, DA potrebbe funzionare per te ma non funzionerà nel modo più efficiente o sicuro possibile. Di seguito è riportato un breve elenco dei motivi per cui la procedura guidata per l'avvio non è nel tuo migliore interesse.

- GSW co-ospita il sito web NLS sul server DA: cattivo
- GSW applica le impostazioni GPO del client DA ai computer del dominio: questa è un'idea terribile
- GSW utilizza certificati autofirmati, un "livello di sicurezza 101" no-no
- GSW disabilita automaticamente Teredo, inefficiente
- GSW non ti guida attraverso nessuna delle opzioni avanzate per DirectAccess, probabilmente perché il modo in cui imposta tutto invalida la tua capacità di utilizzare anche le funzioni avanzate:

Console di gestione dell'accesso remoto

Sei sulla buona strada per fornire agli utenti funzionalità di accesso remoto su questo nuovo server. Come con molti dispositivi di rete, una volta stabilite tutte le configurazioni su un server di accesso remoto, è abbastanza comune che gli amministratori se ne vadano e lo lascino funzionare. Non sono necessarie molte operazioni di manutenzione o modifiche a quella configurazione una volta che è stata eseguita correttamente. Tuttavia, la console di gestione dell'accesso remoto in Windows Server 2019 è utile non solo per la configurazione di parti e componenti di accesso remoto, ma anche per il monitoraggio e il reporting. Quando lavori con DirectAccess, qui trovi praticamente tutto: configurazione, gestione e monitoraggio. Sul lato VPN / AOVPN del set di strumenti di accesso remoto, prenderai molte delle decisioni di configurazione VPN all'interno di RRAS, ma RAMC è il posto dove andare quando si controlla il monitoraggio lato server, il monitoraggio della connessione client e le statistiche di reporting. Sia che utilizzi DA, VPN o una combinazione dei due, RAMC è uno strumento con cui devi sentirti a tuo agio.

Diamo un'occhiata all'interno di questa console in modo da avere familiarità con i diversi schermi con cui interagirai:

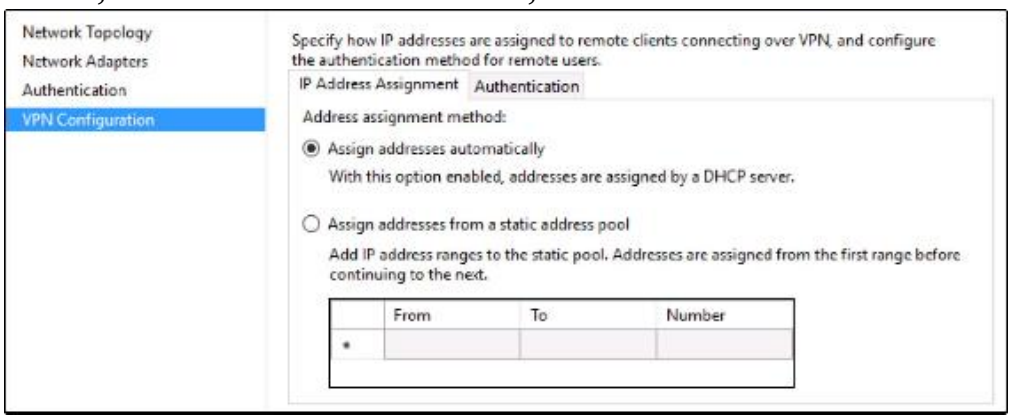


Configurazione

La schermata di configurazione è piuttosto autoesplicativa; qui è dove crei la tua configurazione di accesso remoto iniziale e dove aggiorni le impostazioni in futuro. Come puoi vedere nello screenshot, puoi configurare DirectAccess e VPN, e persino il proxy dell'applicazione Web, direttamente da questa console di gestione dell'accesso remoto.

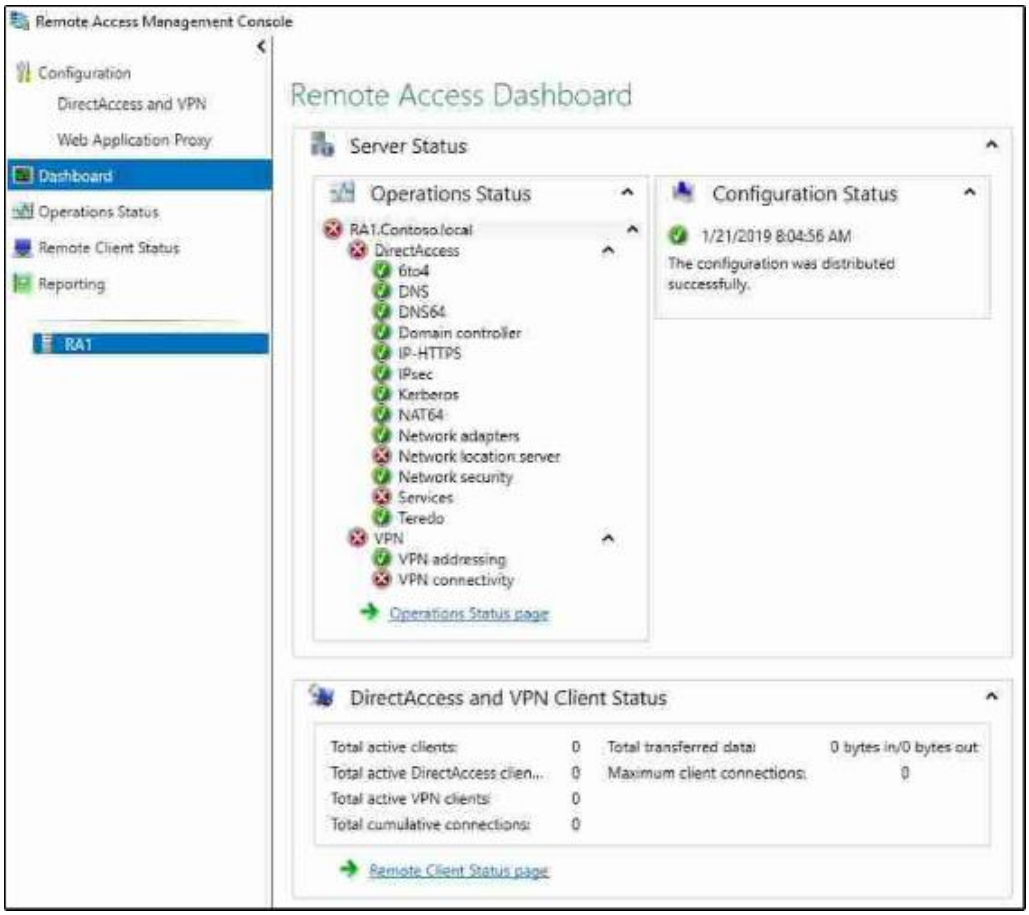
Non seguire il mio esempio con questo screenshot. Ho installato la parte DA / VPN del ruolo di accesso remoto insieme alla parte del proxy dell'applicazione Web dello stesso ruolo, ma non è consigliabile eseguire contemporaneamente DA / VPN e WAP sullo stesso server. L'ho fatto semplicemente allo scopo di creare screenshot nel mio laboratorio di prova.

Non c'è molto da configurare per quanto riguarda la VPN; hai davvero solo una schermata di opzioni in cui definisci quali tipi di indirizzo IP vengono trasmessi ai client VPN che si connettono e come gestire l'autenticazione VPN. Non è immediatamente ovvio dove sia questa schermata, quindi volevo segnalarlo. Nella sezione DirectAccess e configurazione VPN, se fai clic su Modifica ... nel passaggio 2, verrà avviato il mini-wizard del passaggio 2. L'ultima schermata di questa mini-procedura guidata si chiama Configurazione VPN. Questa è la schermata in cui puoi configurare questi indirizzi IP e le impostazioni di autenticazione per le tue connessioni VPN. Il resto delle tue attività di configurazione VPN rientrerà nella tradizionale console di configurazione VPN, chiamata RRAS. Tuttavia,



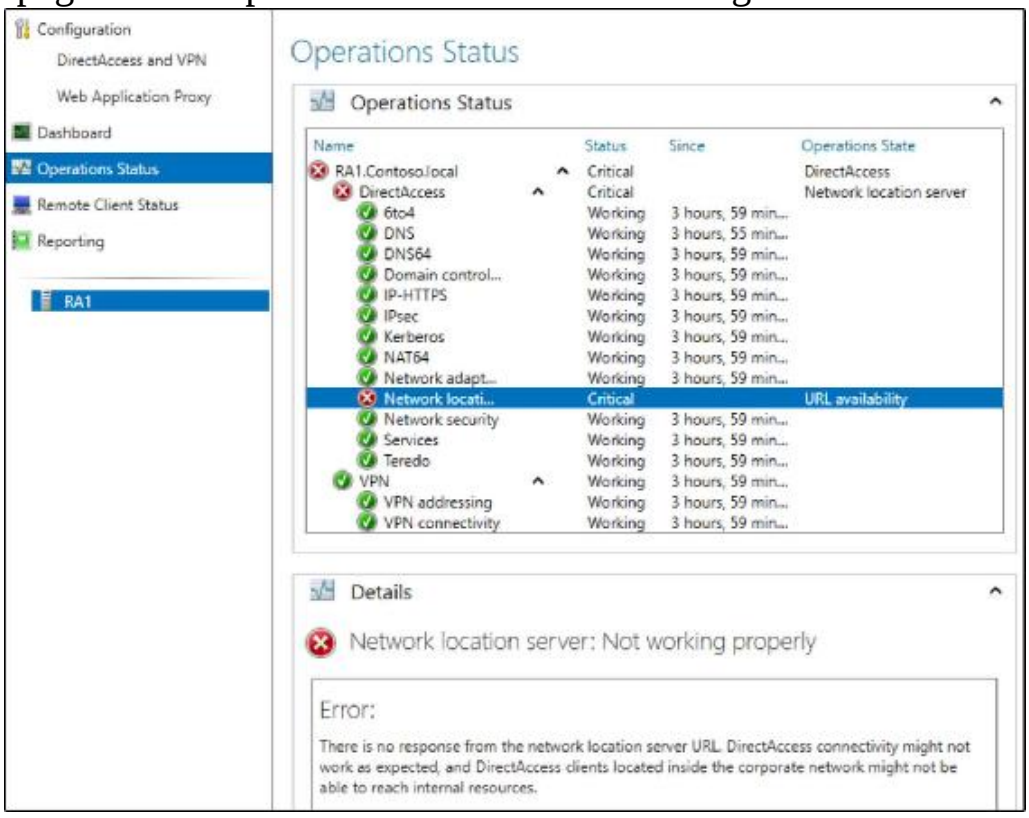
Pannello di controllo

Il dashboard di accesso remoto ti offre una visualizzazione di 30.000 piedi dello stato del server di accesso remoto. È possibile visualizzare rapidamente lo stato dei componenti in esecuzione sul server, indipendentemente dal fatto che le ultime modifiche alla configurazione siano state implementate e alcuni numeri di riepilogo nella parte inferiore del numero di connessioni DirectAccess e VPN in corso:



Stato delle operazioni

Se si desidera approfondire ciò che sta accadendo sul lato server delle connessioni, è di questo che si occupa la pagina Stato delle operazioni. Qui puoi vedere più dettagli su ciascuno dei componenti che sono in esecuzione sotto il cofano per realizzare le tue connessioni DA e VPN. Se qualcuno di loro ha un problema, puoi fare clic sul componente specifico per ottenere ulteriori informazioni. Ad esempio, come test, ho disattivato il server Web NLS nella rete del mio laboratorio e ora posso vedere nella pagina Stato operazioni che NLS è contrassegnato con un errore:



Stato del client remoto

La prossima è la schermata Stato client remoto. Come indicato, questa è la schermata in cui possiamo monitorare i computer client connessi. Ci mostrerà sia DirectAccess che le connessioni VPN qui. Saremo in grado di vedere i nomi dei computer, i nomi utente e persino le risorse che stanno utilizzando durante le loro connessioni. Le informazioni su questa schermata possono essere filtrate semplicemente inserendo qualsiasi criterio nella barra di ricerca nella parte superiore della finestra.

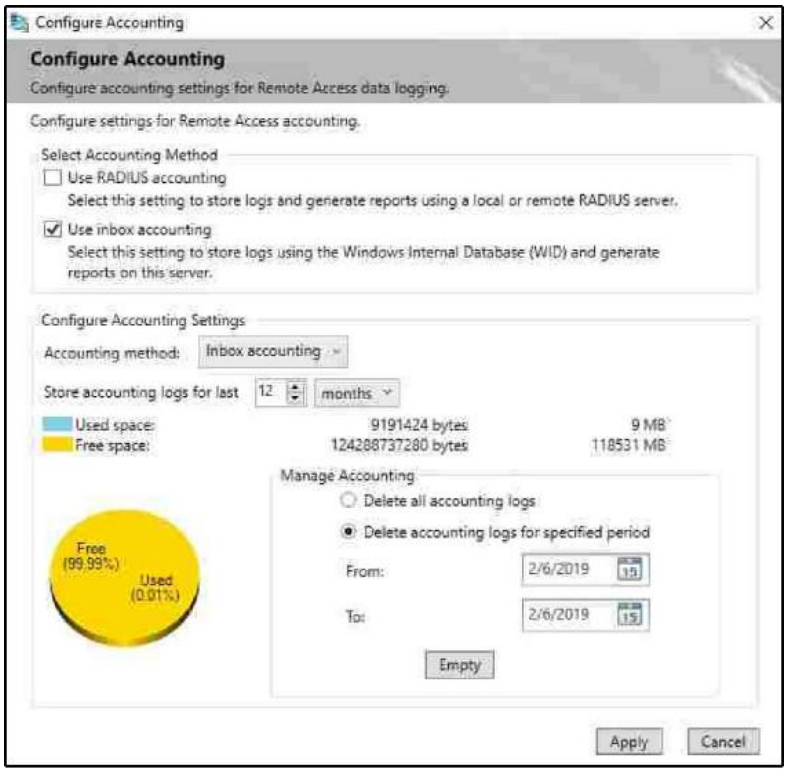
È importante notare che la schermata Stato client remoto mostra solo connessioni attive e attive. Non ci sono informazioni storiche memorizzate qui.

Segnalazione

Hai indovinato: questa è la finestra che devi visitare se vuoi vedere le informazioni storiche di accesso remoto. Questa schermata è quasi identica alla schermata Stato client remoto, tranne per il fatto che hai la possibilità di generare rapporti per i dati storici estratti da intervalli di date di tua scelta. Una volta visualizzati i dati, si hanno le stesse funzionalità di ricerca e filtro che si avevano nella schermata Stato client remoto.

I rapporti sono disabilitati per impostazione predefinita, ma devi semplicemente accedere alla pagina Rapporti e fare clic su Configura contabilità. Una volta abilitato, ti verranno presentate le opzioni per la memorizzazione delle informazioni storiche. È possibile scegliere di archiviare i dati nel WID locale o su un server RADIUS remoto.

Hai anche delle opzioni qui per quanto tempo conservare i dati di registrazione e un meccanismo che può essere utilizzato per cancellare i vecchi dati:



Compiti

L'ultimo riquadro della finestra nella Console di gestione dell'accesso remoto che desidero evidenziare è la barra delle attività sul lato destro dello schermo. Le azioni e le opzioni visualizzate in questa barra delle applicazioni cambiano a seconda di quale parte della console si sta navigando. Assicurati di tenere d'occhio questo lato dello schermo per impostare alcune funzioni più avanzate. Alcuni esempi di attività disponibili sono la creazione di rapporti sull'utilizzo, l'aggiornamento dello schermo, l'abilitazione o la disabilitazione di VPN e la configurazione del bilanciamento del carico di rete o di configurazioni multisito se si eseguono più server di accesso remoto.

DA, VPN o AOVPN? Qual è il migliore?

La VPN esiste da moltissimo tempo, rendendola un'idea abbastanza familiare a chiunque lavori nel settore IT. Always On VPN porta sicuramente la sua parte di nuove funzionalità, ma dietro le quinte ciò che AOVPN sta facendo è lanciare una connessione VPN configurata tradizionalmente, quindi il flusso di connessione è simile a quello che abbiamo sempre saputo. In questo capitolo, abbiamo anche discusso un po 'di DirectAccess per portarti al passo con questo metodo alternativo per connettere automaticamente i tuoi client remoti al data center. Ora che sai che ci sono due fantastiche piattaforme di connettività integrate in Windows Server 2019 per abilitare la tua forza lavoro mobile, qual è la migliore?

Non devi scegliere! Puoi effettivamente eseguire entrambe queste tecnologie fianco a fianco, anche sullo stesso server di accesso remoto. Ogni tecnologia ha i suoi pro e contro e il modo in cui li usi, o entrambi, dipenderà da molte variabili. I tuoi utenti, i tuoi computer client e le esigenze individuali della tua organizzazione dovranno essere presi in considerazione nel tuo processo decisionale. Discutiamo alcune delle differenze tra DirectAccess e VPN in modo da poter prendere decisioni intelligenti su quali piattaforme di connettività si adattano bene alla tua organizzazione.

Appartenenza a un dominio o no?

Uno dei requisiti principali per un computer client DirectAccess è che deve essere aggiunto a un dominio. Sebbene questo requisito di per sé non sembri così importante, ciò che implica può avere enormi implicazioni. Affidarsi a un computer abbastanza da essere unito al tuo dominio più che probabilmente significa che il laptop è di proprietà dell'azienda. Probabilmente significa anche che questo laptop è stato inizialmente costruito e preparato dal team IT. Le aziende che hanno

l'abitudine di consentire ai dipendenti di acquistare i propri computer da utilizzare per scopi di lavoro potrebbero non trovare che DirectAccess sia compatibile con quel modello. DA non è inoltre l'ideale per le situazioni in cui i dipendenti utilizzano i computer di casa esistenti per connettersi al lavoro in remoto.

In questo tipo di situazione, come i computer domestici e di proprietà personale, la VPN potrebbe essere più adatta all'attività. Puoi connetterti a una VPN (inclusa Always On VPN) da un computer Windows 10 non appartenente a un dominio e puoi persino stabilire connessioni VPN (connessioni manuali) da molti dispositivi non Microsoft. iOS, Android, telefoni Windows e Mac: tutte queste piattaforme hanno un client VPN integrato che può essere utilizzato per attingere a un listener VPN su un server di accesso remoto Windows Server 2019. Se la tua unica soluzione di accesso remoto fosse DirectAccess, non saresti in grado di fornire ai dispositivi non aggiunti a un dominio una piattaforma di connettività.

Tieni presente che, sebbene il tunnel utente Always On VPN sia più flessibile di DirectAccess in questo senso, se intendi utilizzare il tunnel dei dispositivi AOVPN, le tue macchine dovranno comunque essere aggiunte a un dominio.

Avvio automatico o manuale

Ci sono molti modi diversi per guardare questo. Quando si discute se DirectAccess o una VPN tradizionale sia migliore, DirectAccess è il chiaro vincitore. Nessuno vuole che i propri utenti aprano una connessione e la avviano manualmente per stabilire la connettività VPN quando è disponibile una piattaforma automatizzata per l'uso.

Always On VPN, tuttavia, porta una connettività automatizzata e senza interruzioni nel mondo VPN. AOVPN è fluido quasi quanto DirectAccess in questo senso. Dico quasi perché, nel momento in cui scrivo, è abbastanza difficile far funzionare bene un Device Tunnel. Ciò significa che la maggior parte delle aziende che lanciano AOVPN utilizza solo il tunnel utente. Nello scenario Tunnel utente, la VPN viene avviata automaticamente, ma non finché l'utente non ha già superato la schermata di accesso. Ciò significa che, in queste situazioni, DirectAccess ha ancora un vantaggio su AOVPN, perché DA si connette perfettamente alla schermata di accesso. Ciò consente la reimpostazione della password e ai nuovi utenti del dominio di accedere alle macchine connesse a DA. La mia speranza è che i miglioramenti futuri consentiranno ai dispositivi AOVPN e ai tunnel utente di coesistere bene, il che fornirà una vera connettività sempre attiva ai client AOVPN.

Software contro built-in

Sono un fan dei mobili Ikea. Fanno un ottimo lavoro nel fornire prodotti di qualità a basso costo, incluso il confezionamento in scatole incredibilmente piccole. Dopo aver pagato il prodotto, estrailo dalla confezione, assemblalo e poi provalo per assicurarti che funzioni: è fantastico. Se non riesci a vedere dove sta andando, ti do un

suggerimento: è un'analogia per le VPN tradizionali di terze parti. Ad esempio, in genere si paga un fornitore per il proprio prodotto VPN, lo si estrae dalla confezione, lo si implementa a una spesa maggiore, quindi si prova il prodotto. Quel software VPN ha quindi il potenziale per rompersi e necessita di reinstallazione o riconfigurazione, e verrà sicuramente fornito con aggiornamenti software che devono essere completati lungo la strada. Manutenzione, manutenzione, manutenzione.

Forse ultimamente ho guardato troppi spettacoli di bricolage, ma sono un fan delle case con built-in. I built-in sono essenzialmente mobili che sono permanenti per la casa, integrati nei muri, negli angoli o ovunque si trovino. Aggiunge valore e si integra nella casa in generale molto meglio dei mobili che sono stati assemblati separatamente e poi attaccati al muro nell'angolo.

DirectAccess e Always On VPN sono come funzionalità integrate. Vivono all'interno del sistema operativo. Non c'è alcun software da installare, nessun software da aggiornare, nessun software da reinstallare quando si rompe. Tutto ciò di cui DA e AOVPN hanno bisogno è già in Windows oggi, semplicemente non lo usi. Oh, ed è gratis! Bene, comunque integrato nel costo della tua licenza di Windows. Non ci sono licenze CAL per utente e nessun costo di licenza in corso relativo all'implementazione di una delle soluzioni di accesso remoto di Microsoft.

Se la tua forza lavoro è composta da macchine Windows 10, Microsoft DirectAccess o Microsoft Always On VPN sono chiari vincitori rispetto a qualsiasi soluzione di connettività VPN di terze parti.

Problemi di password e accesso con le VPN tradizionali

Se hai mai lavorato all'helpdesk per un'azienda che utilizza una VPN, sai di cosa sto parlando. Esistono una serie di chiamate di risoluzione dei problemi comuni che avvengono nel mondo VPN relative alle password. A volte, l'utente dimentica la password. Forse la loro password è scaduta e deve essere cambiata - ugh! Anche la VPN non gestisce molto bene questo scenario. O forse il dipendente ha cambiato la password scaduta sul desktop prima di lasciare il lavoro per la giornata, ma ora sta tentando di accedere in remoto dal proprio laptop e non funziona.

Qual è la soluzione ai problemi di password con VPN? Reimpostare la password dell'utente e quindi far entrare l'utente in ufficio per farlo funzionare sul proprio laptop. Sì, questo tipo di telefonate avviene ancora ogni giorno. Questo è un peccato, ma un vero potenziale problema con le VPN della vecchia scuola.

Qual è la buona notizia? Le nuove soluzioni di accesso remoto Microsoft non hanno questo tipo di problema! Poiché DA e AOVPN fanno parte del sistema operativo, hanno la capacità di essere connessi ogni volta che Windows è online. Ciò include la schermata di accesso! Anche se sono

seduto sulla schermata di accesso o di blocco e il sistema attende che io inserisca il mio nome utente e la password, finché ho accesso a Internet dispongo anche di un tunnel DirectAccess o di un tunnel del dispositivo VPN Always On. Ciò significa che posso svolgere attivamente attività di gestione delle password. Se la mia password scade e devo aggiornarla, funziona. Se ho dimenticato la password e non riesco ad accedere al mio laptop, posso chiamare l'helpdesk e semplicemente chiedere loro di reimpostare la mia password. Posso quindi accedere immediatamente al mio laptop DA o AOVPN con la nuova password, direttamente da casa mia.

Un'altra funzione interessante abilitata da questa fluidità è la possibilità di accedere con nuovi account utente. Hai mai effettuato l'accesso al tuo laptop come un account utente diverso per testare qualcosa? Sì, funziona anche su DA e AOVPN. Ad esempio, sono seduto a casa e ho bisogno di aiutare uno dei venditori a risolvere una sorta di problema di autorizzazione dei file. Sospetto che abbia qualcosa a che fare con il suo account utente, quindi voglio accedere al mio laptop come lui per testarlo. Il problema è che il suo account utente non ha mai effettuato l'accesso al mio laptop prima. Con VPN, nessuna possibilità; questo non funzionerebbe mai. Con DirectAccess, un gioco da ragazzi! Mi disconnetto semplicemente, digito il suo nome utente e password e bingo. Ho effettuato l'accesso, mentre sono ancora seduto a casa in pigiama.

È importante notare che è possibile eseguire entrambe le connessioni DirectAccess e VPN sullo stesso server di accesso remoto di Windows Server 2019. Ciò ti consente di ospitare client che sono connessi tramite DA, tramite AOVPN e anche tramite connessioni VPN tradizionali se disponi di macchine non Win10 che devono connettersi. Se una qualsiasi di queste tecnologie di connettività ha funzionalità di cui potresti trarre

Firewall con limitazioni alle porte

Una delle altre comuni chiamate all'helpdesk relative alla VPN è sempre stata La mia VPN non si connetterà da questo hotel. Sfortunatamente, la maggior parte dei protocolli utilizzati dalle VPN per connettersi non sono compatibili con i firewall. È probabile che il tuo router di casa consenta tutto il traffico in uscita, quindi dalla tua connessione Internet domestica tutto va bene quando ti connetti con un protocollo VPN. Ma porta lo stesso laptop e la stessa connessione in un bar pubblico, in un hotel o in un aeroporto e improvvisamente la VPN non riesce a connettersi, con uno strano errore. Questo di solito è causato dalla connessione Internet pubblica che fa scorrere il suo traffico attraverso un firewall che limita le porte. Questi firewall limitano l'accesso in uscita, spesso bloccando cose come ICMP e UDP, che possono interferire con le connessioni VPN. Nei casi più gravi, questi firewall possono consentire solo due porte in uscita: TCP 80 per HTTP e TCP 443 per il traffico del sito Web HTTPS. Quindi bloccano tutto il resto.

Nel caso in cui ci si trovi dietro un firewall con limitazioni di porte, come gestiscono la connettività queste nuove tecnologie di accesso remoto?

DirectAccess è progettato per gestire questo scenario immediatamente. Ricordi quei tre diversi protocolli che DA può usare per connettersi? L'opzione di fallback si chiama IP-HTTPS e fa scorrere il suo traffico all'interno di TCP 443. Quindi, anche se si trova dietro i firewall più severi, DA si connetterà generalmente automaticamente e senza esitazione.

Always On VPN viene generalmente distribuito (come dovrebbe essere) tenendo a mente le best practice, che includono la priorità IKEv2 come protocollo di connettività VPN. In effetti, alcune aziende implementano AOVPN solo con IKEv2. Per queste persone, un firewall che limita le porte sarebbe dannoso per la connessione VPN di quell'utente, poiché IKEv2 utilizza le porte UDP per connettersi. Non funzionerebbe. Quindi, si spera, il punto principale che prendi da questo è che, quando configuri AOVPN, assicurati di prendere i passaggi necessari per abilitare anche la connettività VPN SSTP come metodo di fallback. SSTP gestisce anche il traffico all'interno di TCP 443, che può quindi ricevere il traffico in uscita, anche attraverso firewall hardcore.

Super importante:

Il tunnel dei dispositivi AOVPN può utilizzare solo IKEv2. Se sei dietro un firewall che limita le porte e ti affidi a un tunnel di dispositivi per la connettività, non funzionerà. Il tunnel utente AOVPN è l'unico in grado di eseguire il fallback SSTP.

In effetti, di recente ho lavorato su questo scenario esatto con qualcuno che stava cercando di decidere se desiderava configurare DirectAccess o Always On VPN per le proprie macchine remote. Si trattava di una società che gestisce i computer per numerosi ospedali e studi medici e non disponeva di collegamenti WAN con tali uffici. Tuttavia, gli uffici avevano accesso a Internet, quindi avevamo bisogno della capacità di mantenere i computer collegati automaticamente al data center principale in ogni momento. Finora nello scenario, DirectAccess o Always On VPN si adatterebbero al conto. Quindi, durante i test, abbiamo scoperto che molte reti ospedaliere limitano l'accesso a Internet in uscita. L'unico modo in cui DA si collegava era tramite IP-HTTPS e l'unico modo in cui AOVPN si connetteva era tramite SSTP. Nessun problema, vero? Tranne che lo era. Vedi, queste postazioni di lavoro remote sono spesso trattate come chioschi, macchine walk-up, dove dozzine di dipendenti diversi possono avvicinarsi in qualsiasi momento e accedervi. Spesso, questo significa che gli utenti accedono a queste macchine che non hanno mai effettuato l'accesso prima, quindi non hanno le credenziali memorizzate nella cache su quei computer.

Se non l'hai già capito, non abbiamo avuto altra scelta che andare con DirectAccess in questo scenario. DA è sempre connesso alla schermata di accesso, anche quando si utilizza il metodo "fallback" IP-HTTPS. Always On VPN, tuttavia, può eseguire IKEv2 solo nella schermata di accesso, poiché il tunnel del dispositivo richiede IKEv2. Questo utilizza UDP ed è stato bloccato dal firewall, quindi l'unico modo in cui AOVPN si connette era utilizzando SSTP, ma non era disponibile fino a quando non è stato possibile avviare il tunnel utente, che era solo dopo che l'utente aveva effettuato l'accesso alla macchina. È stato un caso d'uso nel mondo reale estremamente interessante che ha contribuito a far luce sul processo decisionale che potresti dover adottare per i tuoi ambienti.

Disconnessione manuale

Se non sei già convinto che le VPN tradizionali della vecchia scuola siano le notizie di ieri, ti spieghiamo un altro punto. Quando si utilizzano VPN che richiedono all'utente di avviare manualmente la connessione, ci si affida all'utente stesso per mantenere quella macchina gestita, patchata e aggiornata. Certo, potresti avere sistemi automatizzati che eseguono queste cose per te, come WSUS, SCCM e Criteri di gruppo. Ma quando il laptop è in giro, in roaming lontano dalla LAN, quei sistemi di gestione possono svolgere il proprio lavoro solo quando l'utente decide di stabilire una connessione VPN. È molto probabile che un laptop possa trascorrere settimane completamente al di fuori della rete aziendale, connettendosi a dozzine di hotspot insicuri mentre quel dipendente si fa strada nei Caraibi su una nave da crociera. Dopo settimane di feste e Netflix,

Non così con gli strumenti di accesso remoto di Microsoft! Fornire un'opzione di connettività automatica come Always On VPN o DirectAccess significa che il laptop sarebbe stato connesso e avrebbe ricevuto tutti i suoi criteri di sicurezza e le patch durante l'intera vacanza.

In effetti, per fare un ulteriore passo avanti, su un computer connesso a DirectAccess, l'utente non può disabilitare i propri tunnel DA anche se lo desidera. Hai la possibilità di fornire loro un pulsante Disconnetti, ma questo fondamentalmente falsifica la connessione dal punto di vista dell'utente per fargli sentire come se DA sia offline. In realtà, i tunnel IPsec continuano a scorrere in background, consentendo sempre l'esecuzione di attività in stile gestionale.

Funzionalità native di bilanciamento del carico

Per farla breve, DirectAccess è il vincitore qui. La console di gestione dell'accesso remoto in Windows Server 2019 dispone di funzionalità integrate per la configurazione e la gestione di array di server DA. È possibile impilare più server DA uno sopra l'altro, legarli insieme in array

con bilanciamento del carico e fornire ridondanza e resilienza direttamente dall'interno della console, senza hardware aggiuntivo o considerazioni sul bilanciamento del carico tradizionale. Puoi anche configurare qualcosa chiamato DirectAccess multisito, in cui puoi configurare i server DirectAccess che risiedono in diverse posizioni geografiche insieme in array, offrendo resilienza tra siti. Quasi tutte le aziende che eseguono DirectAccess configurano un ambiente ridondante, fornendo bilanciamento del carico interno al sito o multisito, o talvolta entrambi,

Sfortunatamente, queste funzionalità non sono (non ancora, comunque) trasferite nel mondo VPN di Microsoft. Sia che tu stia collegando i client Windows 7 tramite la connettività VPN tradizionale o convincendo i client Windows 10 a connettersi utilizzando Always On VPN, l'infrastruttura back-end di RRAS VPN è la stessa e non dispone di sistemazioni integrate per più server o siti. È certamente possibile farlo, rendendo ridondante quel sistema VPN, ma ciò richiederebbe di configurarlo da soli utilizzando bilanciatori di carico esterni e, spesso, richiederebbe l'uso di bilanciatori di carico di sito / server globali per rendere quel traffico scorrere correttamente.

Chiunque abbia configurato VPN con bilanciamento del carico di qualsiasi tipo in passato potrebbe essere ben consapevole di questo processo ed essere in grado di configurarlo facilmente, e questo è fantastico. Ma questo è sicuramente un fattore limitante per i clienti di piccole imprese che hanno un numero limitato di server, apparecchiature di rete ed esperienza IT. Tutto sommato, le funzionalità aggiuntive integrate nella console relative a DirectAccess lo rendono un passo avanti rispetto a qualsiasi soluzione VPN in termini di creazione della tua infrastruttura di accesso remoto per resistere ai guasti.

Distribuzione delle configurazioni client

L'ultima considerazione principale da tenere in considerazione quando si decide in quale direzione si desidera andare per l'accesso remoto è il metodo con cui le impostazioni lato client vengono inviate ai rispettivi computer.

- **VPN di terze parti**: Abbiamo già discusso gli svantaggi della gestione delle applicazioni software per fornitori di VPN di terze parti. Se puoi invece usare qualcosa di cotto nel sistema operativo Windows, sembra un gioco da ragazzi.
- **Sempre su VPN**: Il modo consigliato per distribuire le impostazioni AOVPN ai computer client è tramite l'uso di una soluzione MDM, ovvero SCCM o Intune. Se disponi di uno di questi sistemi, distribuire le impostazioni AOVPN alla tua forza

lavoro è un gioco da ragazzi. Se non si dispone di uno di questi sistemi, è ancora possibile, ma non è un processo semplice.

- **Accesso diretto**: Penso che l'approccio di DA alla distribuzione delle impostazioni del client sia sicuramente il più semplice con cui lavorare e il più flessibile. Tieni presente che DirectAccess è solo per i tuoi sistemi aggiunti al dominio. Dato che puoi aspettarti che tutti i client siano aggiunti a un dominio, puoi accedere alle impostazioni di connettività DirectAccess in sequenza tramite Criteri di gruppo, che esistono all'interno di qualsiasi infrastruttura gestita da Microsoft.

Spero sinceramente che in futuro vedremo un'opzione di distribuzione di Criteri di gruppo aggiunta per le implementazioni della configurazione Always On VPN. Se una tale funzionalità fosse introdotta, sono completamente fiducioso che diventerebbe immediatamente il modo più popolare per implementare le impostazioni AOVPN.

Per riassumere l'intero argomento, confrontando DirectAccess con le VPN tradizionali ad avvio manuale, DA si aggiudica chiaramente il primo premio. Non c'è davvero paragone. Ora che abbiamo Always On VPN a nostra disposizione, i vantaggi dell'uno sull'altro (DA o AOVPN) sono piuttosto sfocati. Entrambi realizzano molte delle stesse cose, ma in modi diversi. I fattori decisivi primari per la maggior parte dei clienti finora sembrano essere le capacità di implementazione lato client, indipendentemente dal fatto che abbiano o meno accesso a una soluzione MDM e quanto sia importante per loro la connettività Device Tunnel. L'obiettivo di Microsoft è che AOVPN abbia la parità di funzionalità con DirectAccess e si sta avvicinando. Always On VPN ha anche alcune funzionalità di autenticazione avanzate che DirectAccess non ha, come l'integrazione con Windows Hello for Business o Azure MFA.

Proxy dell'applicazione Web

DirectAccess e VPN sono entrambe ottime tecnologie di accesso remoto e la loro combinazione può fornire una soluzione di accesso remoto completa per la tua organizzazione, senza dover pagare o lavorare con una soluzione di terze parti. Meglio ancora, in Windows Server 2019 è disponibile un altro componente del ruolo Accesso remoto. Questa terza parte della storia dell'accesso remoto è il Web Application Proxy (WAP). Si tratta essenzialmente di un meccanismo di proxy inverso, che offre la possibilità di prendere alcune applicazioni HTTP e HTTPS ospitate all'interno della rete aziendale e pubblicarle in modo sicuro su Internet. Chi di voi ha lavorato con le tecnologie Microsoft nel settore delle reti perimetrali negli ultimi anni riconoscerà probabilmente un prodotto chiamato Forefront Unified Access Gateway (UAG), che ha realizzato funzionalità simili. UAG era una soluzione SSLVPN completa, progettata anche per pubblicare applicazioni interne su Internet tramite SSL. Era notevolmente più potente di un semplice proxy inverso, inclusi componenti come pre-autenticazione, SSTP VPN e gateway RDS; DirectAccess stesso potrebbe anche essere eseguito tramite UAG.

Se tutti i tuoi lavoratori mobili hanno accesso all'avvio di DirectAccess o VPN, probabilmente non utilizzi il WAP. Tuttavia, con la crescente mentalità del cloud, è abbastanza comune per gli utenti aspettarsi di poter aprire un browser Web da qualsiasi computer, ovunque e ottenere l'accesso ad alcune delle loro applicazioni. L'accesso ai documenti è ora spesso fornito da servizi Web come SharePoint. È possibile accedere alla posta elettronica in remoto, da qualsiasi computer, toccando Outlook Web Access.

È possibile accedere a così tante applicazioni e così tanti dati solo tramite un browser Web e ciò consente ai dipendenti di accedere a questi dati senza la necessità di stabilire un tunnel aziendale completo come una VPN. Allora qual è il caso d'uso nel mondo reale per WAP? Computer di casa a cui non vuoi essere connesso tramite VPN. In questo modo, non devi preoccuparti tanto della salute e dello stato dei computer domestici o di proprietà degli utenti, poiché l'unica interazione che hanno con la tua azienda è tramite il browser web. Ciò limita il potenziale flusso di attività sinistre nella tua rete da questi computer. Come puoi vedere, una tecnologia come il WAP ha sicuramente il suo posto nel mercato dell'accesso remoto.

Mi auguro che, nel tempo, il WAP continuerà a essere migliorato e ciò gli consentirà di essere un vero sostituto di UAG. UAG veniva eseguito su Windows Server 2008 R2 e ora è stato ufficialmente interrotto come prodotto Microsoft. La soluzione più vicina che Microsoft ha ora a UAG è il ruolo WAP. Non è ancora così completo, ma stanno lavorando per migliorarlo. Attualmente, il WAP è utile per pubblicare l'accesso a semplici applicazioni web. Puoi anche pubblicare l'accesso a rich client che utilizzano l'autenticazione HTTP di base, come Exchange ActiveSync. È inclusa anche la possibilità di pubblicare dati su client che utilizzano MSOFBA, ad esempio quando gli utenti tentano di estrarre dati aziendali dalle loro applicazioni Word o Excel in esecuzione sul computer locale.

Il WAP può essere utilizzato per eseguire il proxy inverso (pubblicazione) dell'accesso remoto a cose come gli ambienti Exchange e SharePoint. Non è cosa da poco, poiché si tratta di tecnologie che quasi tutti utilizzano, quindi può sicuramente essere vantaggioso per la tua azienda implementare il WAP per pubblicare un accesso sicuro a queste risorse; è sicuramente meglio del NAT direttamente sul tuo server Exchange.

WAP come proxy AD FS

Un altro modo utile in cui è possibile utilizzare un server WAP è quando si configura Active Directory Federation Services (AD FS) nella rete (questo è forse l'uso più comune per WAP in questo momento). AD FS è una tecnologia progettata per abilitare il Single Sign-On per gli utenti e la federazione con altre società, quindi implica il trasferimento del traffico proveniente da Internet nella rete interna. In passato, c'era un componente del ruolo di Windows Server che accompagnava AD FS, chiamato proxy di AD FS. Nelle ultime versioni di AD FS, questo ruolo separato non esiste più ed è stato sostituito dal componente Proxy applicazione Web del ruolo Accesso remoto. Ciò unifica meglio la soluzione di accesso remoto, portando il traffico ADFS in ingresso attraverso il server di accesso remoto ufficiale, anziché richiedere un server proxy AD FS separato.

Requisiti per WAP

Sfortunatamente, la possibilità di utilizzare il proxy dell'applicazione Web viene fornita con un requisito piuttosto scomodo: è necessario che AD FS sia installato nel proprio ambiente per poter utilizzare i, anche per testarlo, perché la configurazione WAP è archiviata all'interno di AD FS. Nessuna delle informazioni di configurazione WAP viene memorizzata sul server di accesso remoto stesso, il che rende un server leggero che può essere facilmente spostato, modificato o aggiunto. Lo svantaggio di questo è che devi avere AD FS in esecuzione nel tuo ambiente in modo che WAP possa avere un posto dove archiviare le informazioni di configurazione.

Sebbene una stretta integrazione con AD FS significhi che abbiamo migliori opzioni di autenticazione e gli utenti possono trarre vantaggio dal Single Sign-On di AD FS per le loro applicazioni pubblicate tramite WAP, finora questo si è dimostrato un ostacolo all'implementazione per piccole imprese. Molte persone non stanno ancora eseguendo AD FS e se l'unico motivo per cui stanno cercando di implementare AD FS è per poter utilizzare WAP per pubblicare alcune applicazioni Web su Internet, potrebbero non scegliere di investire il tempo e gli sforzi solo per fallo accadere.

Una cosa da tenere a mente se si è interessati a utilizzare WAP e si sta quindi esaminando il requisito per AD FS, è che AD FS può certamente essere utilizzato per altre funzioni. In effetti, uno dei suoi usi più comuni attualmente è l'integrazione con Office 365. Se hai intenzione di incorporare Office 365 nel tuo ambiente, ADFS è un ottimo strumento che può migliorare le capacità di autenticazione per quel traffico.

Ultimi miglioramenti al WAP

Il proxy dell'applicazione Web è stato introdotto in Server 2012 R2 e ha avuto molti miglioramenti quando è stato rilasciato Windows Server 2016. Da allora non sono state apportate modifiche importanti, ma è comunque importante sottolineare gli ultimi vantaggi che sono stati introdotti in questa funzione, per dimostrare che sta ancora imparando a fare cose nuove. Di seguito sono riportati alcuni dei miglioramenti che sono stati apportati se non si è dato un'occhiata al WAP dalla sua prima iterazione.

Preautenticazione per HTTP di base

Esistono due modi diversi in cui gli utenti possono autenticarsi nelle applicazioni pubblicate da Web Application Proxy: preautenticazione o autenticazione pass-thru. Quando si pubblica un'applicazione con la preautenticazione, ciò significa che gli utenti dovranno fermarsi dall'interfaccia AD FS per autenticarsi prima di poter accedere all'applicazione Web stessa. Ai miei occhi, la preautenticazione è una componente fondamentale per qualsiasi proxy inverso e dovrei essere bloccato tra l'incudine e l'incudine per pubblicare esternamente un'applicazione che non richiede la preautenticazione. Tuttavia, la seconda opzione è eseguire l'autenticazione pass-thru e lo fa esattamente. Quando si pubblica l'accesso a un'applicazione e si sceglie l'autenticazione pass-thru, tutto ciò che il WAP sta facendo è trasferire i pacchetti da Internet al server delle applicazioni. Gli utenti sono in grado di accedere all'applicazione Web senza autenticazione, quindi in teoria chiunque può visitare il sito Web principale dell'applicazione. Da lì, l'applicazione stessa richiederà probabilmente all'utente di autenticarsi, ma non è prevista alcuna protezione man-in-the-middle; quell'applicazione web è disponibile per la visualizzazione da parte del pubblico. Come puoi vedere, non consiglio di prendere questa strada.

Sappiamo già che il WAP può preautenticare le applicazioni web, ma la versione originale non poteva eseguire alcuna forma di preautenticazione sulle applicazioni HTTP Basic, come quando un'azienda voleva pubblicare l'accesso a Exchange ActiveSync. Questa incapacità lascia ActiveSync un po 'troppo esposto al mondo esterno ed è un rischio per la sicurezza. Per fortuna, questo è cambiato in Windows Server 2016: ora puoi preautenticare i flussi di traffico che utilizzano HTTP Basic.

Reindirizzamento da HTTP a HTTPS

Agli utenti non piace fare di tutto o perdere tempo dovendo ricordare che devono inserire HTTPS: // davanti all'URL quando accedono alle applicazioni. Preferirebbero semplicemente ricordare

email.contoso.com. L'incapacità del WAP di eseguire il reindirizzamento da HTTP a HTTPS era stata un fastidio e un ostacolo all'adozione, ma da allora la situazione è cambiata. Il proxy dell'applicazione Web ora include la capacità del WAP stesso di gestire il reindirizzamento da HTTP a HTTPS, il che significa che gli utenti non devono più digitare HTTPS nella barra degli indirizzi del browser; possono semplicemente digitare il nome DNS del sito e lasciare che il WAP gestisca le traduzioni.

Indirizzi IP client inoltrati alle applicazioni

Nel mondo del proxy inverso e SSLVPN, occasionalmente eseguiamo applicazioni che richiedono la conoscenza dell'indirizzo IP locale del client. Sebbene questo requisito non si verifichi molto spesso ed è tipicamente separato da ciò che chiameremmo applicazioni legacy, continua a verificarsi. Quando l'applicazione di backend deve sapere qual è l'indirizzo IP del client, ciò rappresenta una grande sfida con le soluzioni di proxy inverso. Quando il traffico dell'utente passa attraverso WAP o qualsiasi altro proxy inverso, è simile a un NAT, in cui le informazioni sull'indirizzo IP di origine in questi pacchetti cambiano. Il server delle applicazioni di backend non è in grado di determinare l'indirizzo IP del client e si verificano problemi. Il proxy dell'applicazione Web ora ha la capacità di propagare l'indirizzo IP del lato client attraverso il server delle applicazioni back-end, alleviando questo problema.

Pubblicazione di Gateway Desktop remoto

Uno degli elementi per cui UAG veniva comunemente utilizzato era l'accesso di pubblicazione a Servizi Desktop remoto. UAG era essenzialmente il proprio Gateway Desktop remoto, che ti dava la possibilità di pubblicare l'accesso ai server RDSH, le singole connessioni RDP ai computer desktop, come in un'implementazione VDI, e persino l'accesso alle applicazioni RemoteApp. Sfortunatamente, il WAP non può fare nulla di tutto ciò, anche nella nuova versione, ma il fatto che abbiano aggiunto un po 'di funzionalità qui significa che il movimento nella giusta direzione sta avvenendo.

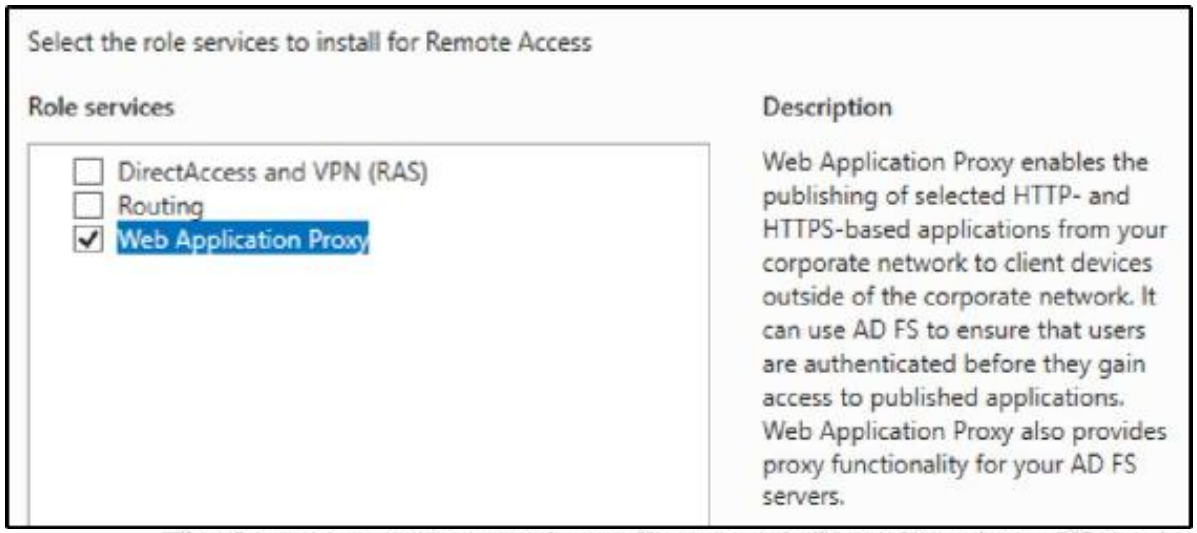
Ciò che è stato migliorato per quanto riguarda WAP e Desktop remoto è che ora è possibile utilizzare WAP per pubblicare l'accesso al server Gateway Desktop remoto stesso. Tradizionalmente,

un Gateway Desktop remoto si trova ai margini della rete e collega gli utenti esterni ai server di Desktop remoto interni. Posizionare il WAP davanti al Gateway Desktop remoto consente una preautenticazione più forte per i servizi di Desktop remoto e crea una separazione maggiore tra le reti interne ed esterne.

Ho tutte le dita incrociate che continueremo a vedere miglioramenti in quest'area e che il WAP può essere espanso per gestire il traffico come Desktop remoto in modo nativo, senza nemmeno bisogno di un Gateway Desktop remoto nel mix.

Console di amministrazione migliorata

La versione originale di WAP all'interno di Windows Server 2012 R2 è stata ottimizzata utilizzando PowerShell per implementarlo. È certamente possibile ancora utilizzare PowerShell per creare le regole di pubblicazione se lo si desidera, ma la console di gestione dell'accesso remoto è stata ora migliorata in termini di relazione con il proxy dell'applicazione Web. Prima di vederlo nella console, è necessario assicurarsi che la casella appropriata sia stata selezionata durante l'installazione del ruolo di accesso remoto. Se non hai selezionato Web Application Proxy quando hai installato per la prima volta quel ruolo, rivisita la funzione aggiungi / rimuovi ruoli all'interno di Server Manager per aggiungere WAP a questo server:



Tieni presente che, sebbene il proxy dell'applicazione Web sia un componente dello stesso ruolo di accesso remoto che ospita DirectAccess e VPN, non è consigliabile eseguire WAP insieme a DA e VPN sullo stesso server. Come già saprai, puoi certamente co-ospitare connessioni DA e VPN insieme, contemporaneamente su un singolo server di accesso remoto. Ma una volta che fai incursione nel WAP, questo dovrebbe essere un componente autonomo. Non eseguire WAP su un server DA / VPN e non eseguire DA / VPN su un server WAP.

Ora che abbiamo aggiunto il proxy dell'applicazione Web al nostro server, puoi aprire la console di gestione dell'accesso remoto e vederlo elencato nella sezione Configurazione. Da qui, si avvia la Configurazione guidata proxy dell'applicazione Web e si inizia a seguire i passaggi per definire il server AD FS, i certificati che si prevede di utilizzare e altri criteri necessari per il ruolo:

Sommario

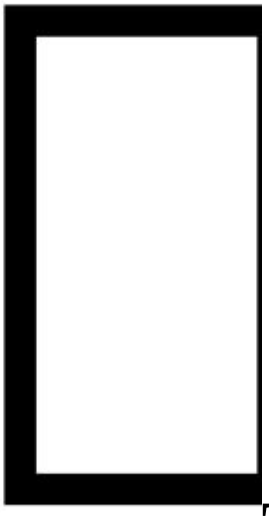
La tecnologia odierna richiede che la maggior parte delle aziende consenta ai propri dipendenti di lavorare ovunque si trovino. Sempre più organizzazioni assumono un lavoro dalla forza lavoro domestica e necessitano di un modo sicuro, stabile ed efficiente per fornire accesso ai dati e alle applicazioni aziendali per questi lavoratori mobili. Il ruolo Accesso remoto in Windows Server 2019 è progettato per fare esattamente questo. Con tre diversi modi per fornire accesso remoto alle risorse aziendali, i reparti IT non hanno mai avuto così tanta tecnologia di accesso remoto a portata di mano, integrata direttamente nel sistema operativo Windows di cui già possiedono. Se stai ancora supportando un sistema VPN di terze parti o legacy, dovresti assolutamente esplorare le nuove funzionalità fornite qui e scoprire quanto potrebbero salvare la tua attività.

DirectAccess e Always On VPN sono opzioni di connettività particolarmente interessanti e convincenti, un nuovo modo di guardare all'accesso remoto. La connettività automatica include macchine sempre attive a cui vengono costantemente applicate patch e aggiornate perché sono sempre connesse ai server di gestione. Puoi migliorare la produttività degli utenti e la sicurezza della rete allo stesso tempo. Queste due cose sono solitamente ossimori nel mondo IT, ma con lo stack di accesso remoto di Microsoft, si tengono per mano e cantano insieme canzoni.

Successivamente, daremo un'occhiata ad alcune delle funzioni di sicurezza integrate nei tuoi sistemi operativi Windows Server 2019 e ad alcuni dei modi in cui i tuoi server possono essere rafforzati per fornire una sicurezza ancora migliore di quella che viene fuori dalla scatola.

Domande

1. Cosa significa AOVPN?
2. Quali sono i due protocolli principali utilizzati per connettere i client AOVPN?
3. In quale versione di Windows 10 è stato rilasciato AOVPN?
4. In quale caso speciale dovrebbe essere necessario unire un client AOVPN al tuo dominio?
5. DirectAccess richiede che la rete interna aziendale esegua IPv6?
6. Qual è il nome del sito Web interno con cui i client DirectAccess effettuano il check-in per determinare quando si trovano all'interno della rete aziendale?
7. Quale ruolo ricopre un server proxy dell'applicazione Web in un ambiente federativo?



Tempra e sicurezza

$ 3,8 milioni di dollari. Per chiunque lo legga con la voce del Dr. Evil, il mio cappello va a te. Per chiunque non abbia idea di cosa sto parlando, potresti aver avuto un'infanzia protetta. A parte gli scherzi, quel numero è significativo per la sicurezza IT. Perché? Perché 3,8 milioni di dollari sono il costo medio per un'azienda quando è vittima di una violazione dei dati. Inizialmente ho sentito questa e altre statistiche spaventose a una conferenza Microsoft a Redmond un paio di anni fa, e i numeri hanno continuato a salire di anno in anno. Che ne dici di guardare un'altra statistica che può essere utilizzata per ottenere l'approvazione per un aumento del budget per la sicurezza? A seconda dello studio che leggi, il numero medio di giorni di permanenza nella rete di un utente malintenzionato (il tempo che trascorre all'interno dei file e dell'infrastruttura prima che vengano rilevati ed eliminati) è di circa 200. Pensateci: 200 giorni! Questa è la parte migliore dell'anno in cui si accampano prima di scoprirli! Cosa stanno facendo in genere durante quei 200 giorni? Sifonando tutti i tuoi dati, un po 'alla volta fuori dalla porta sul retro. Un altro numero è del 76%, come nella percentuale di intrusioni

di rete che si verificano a seguito di credenziali utente compromesse. Inoltre, sta diventando sempre più difficile identificare questi attacchi in primo luogo, perché gli aggressori utilizzano strumenti IT legittimi per afferrare ciò che vogliono, come ad esempio ingegnerizzarsi socialmente nella fiducia di un singolo dipendente, e sfruttare questa fiducia per ottenere uno strumento di connettività di accesso remoto installato sul computer di lavoro dell'utente. Perché usare malware quando puoi usare qualcosa che è affidabile e sta per volare sotto il radar dei sistemi di rilevamento delle intrusioni? È sensato per me.

Sicurezza dei dati, sicurezza della rete, sicurezza delle credenziali: queste cose stanno diventando sempre più difficili da realizzare, ma ci sono sempre nuovi strumenti e tecnologie in uscita che possono aiutarti a combattere i cattivi. Windows Server 2019 è il sistema operativo più sicuro che Microsoft abbia prodotto; in questo capitolo, discutiamo alcune delle funzionalità incluse che rendono vera questa affermazione:

- Protezione avanzata dalle minacce di Windows Defender Firewall di Windows Defender: non importa Tecnologie di crittografia
- Password vietate Advanced Threat Analytics
- Best practice di sicurezza generali

Protezione avanzata dalle minacce di Windows Defender

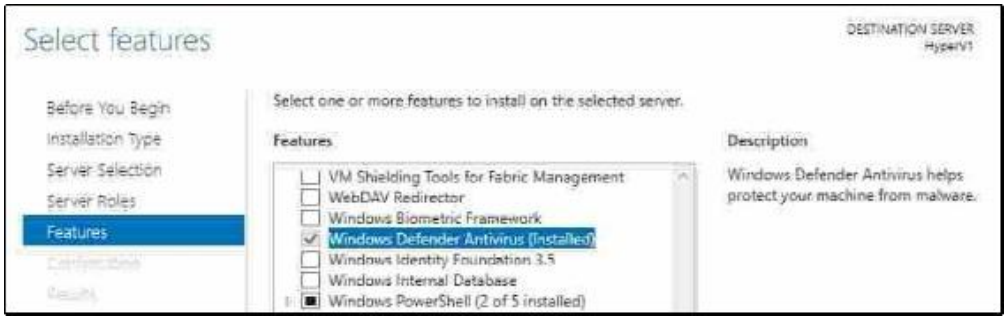
Windows Defender esiste da diversi anni, ma la sua terminologia e le sue capacità si sono davvero sviluppate negli ultimi due rilasci del sistema operativo. Inizialmente, è iniziato nei giorni di Windows 8 come prodotto antivirus gratuito e integrato e all'epoca non è stato preso troppo sul serio. Avanti veloce fino ad oggi, tuttavia, e raramente mi imbatto in un computer Windows 10 con le funzionalità di Defender Antivirus (AV) o firewall disabilitate. Questi strumenti esistono nel sistema operativo e sono abilitati per impostazione predefinita e, di conseguenza, hanno un livello di integrazione e reattività difficile da eguagliare per i fornitori di terze parti. Non posso dirti quante volte ho rintracciato perdite di memoria e riavvii casuali del server su un software antivirus di terze parti mal funzionante, il che è inaccettabile nel mondo dei server di oggi. Alcuni considerano ancora le funzionalità antivirus fornite da Defender poco brillanti, probabilmente solo perché sono gratuite, ma trovo che sia robusto e ben integrato con Windows stesso. Devo ancora vedere un prodotto Windows Defender caricare un client o un server.

Anche il più recente e più specifico Windows Defender Advanced Threat Protection (ATP) è davvero una famiglia di prodotti e sistemi che lavorano insieme per proteggere i tuoi computer Windows. L'antivirus / anti-malware è solo una di queste funzionalità e l'antivirus integrato è in realtà ancora un'idea abbastanza nuova quando si parla della famiglia di sistemi operativi Windows Server. Il primo sistema operativo per server che abbiamo trovato con Defender integrato per antivirus è stato Server 2016. Sospetto che la maggior parte dei server in esecuzione in produzione per aziende di tutto il mondo siano ancora Server 2012 R2 a questo punto, quindi l'esistenza migliorata di Defender set di strumenti in Server 2019 è un altro motivo per iniziare a pianificare la migrazione oggi stesso.

Semplicemente non abbiamo abbastanza spazio nella pagina per immergerci in ogni aspetto di Windows Defender ATP e viene continuamente migliorato. Quello che faremo è esplorare alcune delle interfacce, assicurarci di sapere come utilizzare i componenti più comuni che non richiedono manipolazione a livello di policy e ampliare le tue conoscenze su alcune delle funzionalità più avanzate disponibili per ulteriori approfondimenti e scavare.

Installazione di Windows Defender AV

Hai finito! Windows Defender è installato per impostazione predefinita in Windows Server 2019. Infatti, a meno che tu non l'abbia modificato in qualche modo, non solo Defender AV è installato, ma protegge automaticamente il tuo sistema non appena il sistema operativo viene installato. Ma non credermi sulla parola, se apri Server Manager e scegli Aggiungi ruoli e funzionalità, fai clic sulla pagina Seleziona funzionalità e dovresti trovare una casella di controllo accanto a Windows Defender Antivirus:



Se per qualche motivo non è già stato controllato, allora questo è esattamente il posto da visitare per installarlo e farlo funzionare.

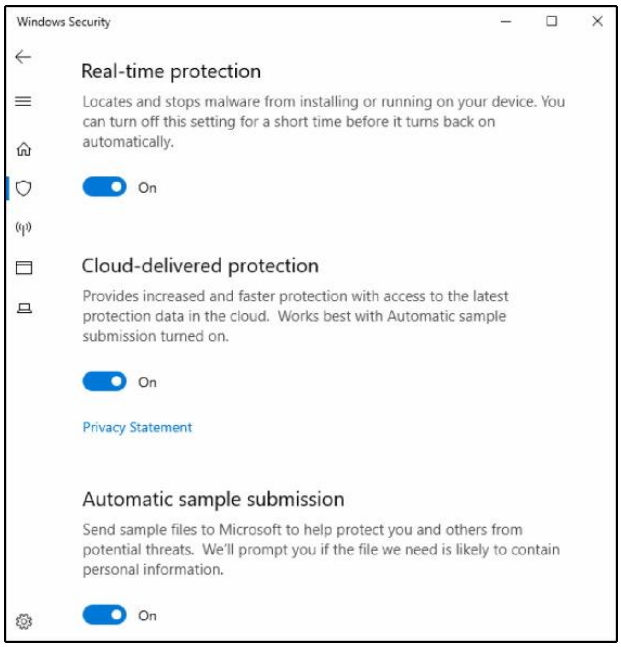
Esplorazione dell'interfaccia utente

L'interfaccia per il set di strumenti di Windows Defender è la stessa delle ultime versioni di Windows 10, ma se non l'hai ancora esplorata, daremo una rapida occhiata qui. Vai avanti e avvia Impostazioni dal menu Start, quindi fai clic su Aggiorna e sicurezza. Una volta all'interno di quella

sezione, vedrai Windows Security elencato a sinistra. Qui ottieni una vista dall'alto dei diversi componenti di Defender che lavorano insieme per proteggere il tuo sistema.

Ricorda, non hai fatto nulla per abilitare nessuna di queste funzionalità; queste sono tutte funzionalità pronte all'uso:

Facendo clic ulteriormente in una qualsiasi di queste aree di protezione, verranno fornite descrizioni più dettagliate di ciascuna funzionalità, nonché molte opzioni per abilitare o disabilitare particolari protezioni esistenti. Ad esempio, se si fa clic su Protezione da virus e minacce, verranno visualizzate informazioni di riepilogo su Defender AV, quando i suoi file di definizione sono stati aggiornati, cosa sta scansionando e così via. Quindi, facendo clic ulteriormente su un collegamento chiamato Gestisci impostazioni, ti verranno fornite le opzioni per disabilitare Defender AV se ne hai bisogno, oltre a numerose altre opzioni che possono essere selezionate o deselezionate. Ecco uno screenshot di alcune delle impostazioni disponibili in Defender AV. Ho scelto di visualizzare questi tre perché sono importanti per un altro argomento che tratteremo a breve, quando discuteremo della parte ATP di Defender ATP:



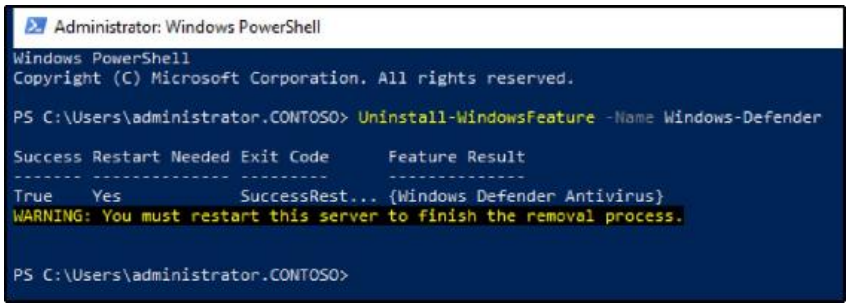
Disattivazione di Windows Defender

Sai già che Defender AV è abilitato per impostazione predefinita, così come molti altri componenti che compongono la famiglia di prodotti Windows Defender. Capovolgendo l'opzione radio mostrata nello screenshot precedente, puoi disabilitare temporaneamente AV. Facendo un ulteriore passo avanti, se sei assolutamente sicuro di non voler utilizzare Defender AV perché hai il tuo software AV che hai già pagato, hai due strade diverse che potrebbero essere prese.

Innanzitutto, Defender AV è progettato per ritirarsi automaticamente nel caso in cui venga installato un altro AV. Molto probabilmente, tutto ciò che devi fare è installare il tuo altro strumento antivirus di terze parti e, al termine del riavvio del server, Defender AV si spegnerà e consentirà l'esecuzione del prodotto di terze parti, in modo che non entrino in conflitto tra loro altro. Questo è importante, perché un fatto di cui anche molti tecnici informatici non si rendono conto è che più programmi AV in esecuzione su un singolo sistema è generalmente un'idea terribile. Spesso causano conflitti tra loro, hanno errori di allocazione della memoria e causano un comportamento altrimenti lento e strano nel sistema.

Se hai intenzione di utilizzare il tuo AV e vuoi assicurarti che Defender sia completamente rimosso, è possibile disinstallare completamente la funzione Defender dal tuo server. Questa operazione viene eseguita più facilmente tramite PowerShell, con il seguente comando:

Disinstalla-WindowsFeature -Nome Windows-Defender



Che cos'è l'ATP, comunque?

È difficile definire cosa significhi esattamente ATP, perché è il culmine di parti, componenti e meccanismi di sicurezza di Windows Defender che lavorano insieme per proteggere client e server da cose dannose: AV, funzionalità di firewall, protezioni hardware e persino resistenza specifica contro ransomware. La combinazione di funzionalità all'interno della sezione Protezione di Windows di Server 2019 lavorano insieme per diventare ATP.

Qualcosa che dovrebbe essere incredibilmente intrigante per tutti noi è il modo intelligente in cui Microsoft utilizza ora la connettività cloud e

l'elaborazione per migliorare Defender AV su base giornaliera. Che ce ne rendiamo conto o meno, la maggior parte delle macchine Windows connesse a Internet nel mondo ora si aiutano continuamente a vicenda segnalando vulnerabilità scoperte di recente e attività dannose fino a Microsoft. Queste informazioni vengono quindi analizzate e analizzate tramite l'apprendimento automatico e le informazioni risultanti possono essere immediatamente utilizzate dal resto delle macchine Windows in tutto il mondo.

Anche se questo suona un piccolo Grande Fratello e pieno di preoccupazioni per la privacy, credo che noi come comunità presto supereremo quella paura e ci renderemo conto che i benefici superano le potenziali paure. Milioni di utenti ora inviano la posta elettronica tramite Office 365; potresti anche non rendertene conto, ma Office 365 gestisce anche questo tipo di gestione dei dati per identificare e bloccare gli exploit. Ad esempio, se un indirizzo di posta elettronica all'interno di un'azienda invia improvvisamente messaggi di posta elettronica a un grande gruppo di persone e tale messaggio di posta elettronica contiene un documento di Word abilitato per le macro, che è qualcosa che l'utente in genere non fa, Office 365 può prendere quel documento molto rapidamente offline in una zona sicura, aprilo (o avvialo se l'allegato è un eseguibile) e scopri se questo file è effettivamente malware di qualche tipo. Se è, Office 365 inizierà immediatamente a bloccare quel file, interrompendo così la diffusione di questo comportamento potenzialmente disastroso. Tutto ciò avviene senza l'input dell'utente o del personale IT dell'azienda. Questo non è nemmeno specifico dell'azienda interna. Se la posta di uno dei miei utenti è la prima a ricevere un nuovo virus ed è identificata da Microsoft, quella scoperta aiuterà a bloccare il nuovo virus per tutti gli altri clienti che ospitano anche la loro posta nel cloud di Microsoft. Questa è roba davvero incredibile! questa scoperta aiuterà a bloccare il nuovo virus per tutti gli altri clienti che ospitano anche la loro posta elettronica nel cloud di Microsoft. Questa è roba davvero incredibile! questa scoperta aiuterà a bloccare il nuovo virus per tutti gli altri clienti che ospitano anche la loro posta elettronica nel cloud di Microsoft. Questa è roba davvero incredibile!

Questa stessa idea vale per Defender AV, quando scegli di consentirgli di comunicare e inviare informazioni alle risorse cloud di Microsoft. In precedenza, ho incollato uno screenshot di alcune funzionalità di Defender AV chiamate protezione fornita dal cloud e invio automatico di campioni: sono questi pezzi di Defender AV che consentono a questa magia basata su cloud di accadere a vantaggio dell'intera popolazione di computer.

Windows Defender ATP Exploit Guard

Ancora una volta, stiamo esaminando quello che sembra essere un titolo lungo per una tecnologia che deve avere uno scopo ben preciso, giusto? No. Il nuovo Exploit Guard non è una nuova funzionalità, ma piuttosto un intero set di nuove funzionalità integrate nella famiglia Windows Defender.

In particolare, queste nuove protezioni sono progettate per aiutare a rilevare e prevenire alcuni dei comportamenti comuni utilizzati negli attuali attacchi di malware. Ecco i quattro componenti principali di Defender ATP Exploit Guard:

- **Riduzione della superficie di attacco** (ASR): ASR è una serie di controlli che possono essere abilitati che bloccano l'esecuzione di determinati tipi di file. Questo può aiutare a mitigare il malware installato dagli utenti che fanno clic sugli allegati di posta elettronica o dall'apertura di determinati tipi di file di Office. Stiamo rapidamente imparando come società di computer che non dovremmo mai fare clic su file in un'e-mail che sembrano essere eseguibili, ma spesso un utente di computer tradizionale non conoscerà la differenza tra un file eseguibile e un file legittimo. ASR può aiutare a bloccare l'esecuzione di qualsiasi file eseguibile o di scripting dall'interno di un'e-mail.

- **Protezione della rete**: Questo abilita Windows Defender SmartScreen, che può impedire a potenziali malware di telefonare a casa, comunicando ai server dell'aggressore per sifonare o trasferire dati aziendali all'esterno della tua azienda. I siti Web su Internet hanno valutazioni di reputazione, che ritengono tali siti o indirizzi IP attendibili o non attendibili, a seconda dei tipi di traffico diretti a quell'indirizzo IP in passato. SmartScreen attinge a quei database di reputazione per impedire al traffico in uscita di raggiungere destinazioni sbagliate.
- **Accesso controllato alle cartelle**: Protezione ransomware! Questo è intrigante perché il ransomware è una delle principali preoccupazioni per qualsiasi professionista della sicurezza IT. Se non hai familiarità con il concetto, il ransomware è un tipo di malware che installa un'applicazione sul tuo computer, che quindi crittografa i file sul tuo computer.
Una volta crittografati, non hai la possibilità di aprire o riparare quei file senza la chiave di crittografia, che gli aggressori (la maggior parte delle volte) ti consegneranno felicemente per un sacco di soldi. Ogni anno, molte aziende finiscono per pagare quel riscatto (e quindi impegnarsi in comportamenti criminali passivi) perché non hanno buone protezioni o buoni backup da cui ripristinare le proprie informazioni. L'accesso controllato alle cartelle aiuta a proteggersi dal ransomware impedendo a processi non attendibili di afferrare aree del disco rigido che sono state ritenute protette.
- **Protezione dagli exploit**: Protezione generalizzata contro molti tipi di exploit che potrebbero verificarsi su un computer. La funzione di protezione dagli exploit di Defender ATP è un raggruppamento di funzionalità da qualcosa chiamato Enhanced Mitigation Experience Toolkit (EMET) che era precedentemente disponibile, ma ha raggiunto la fine del ciclo di vita a metà del 2018. La protezione dagli exploit controlla e protegge i processi di sistema e gli eseguibili delle applicazioni.

Windows Defender Firewall: niente da ridere

Facciamo un gioco di associazione di parole. Dirò qualcosa e tu dici la prima parola che mi viene in mente.

Sicurezza della rete.

Hai detto firewall? Penso che l'avrei fatto. Quando pensiamo di proteggere i nostri dispositivi a livello di rete, pensiamo ai perimetri. Tali perimetri sono definiti e protetti da firewall, principalmente a livello hardware, con dispositivi di rete specializzati realizzati per gestire quel particolare compito nelle nostre reti. Oggi siamo qui per parlare di un altro livello di firewall che puoi e dovresti utilizzare nei tuoi ambienti. Sì, stiamo parlando di Windows Firewall. Smettila di ridere, è maleducato!

È facile prendere in giro Windows Firewall in base alla sua storia. Ai tempi di Windows XP e Server 2003, era piuttosto inutile e causava molti più grattacapi di quanti ne risolvesse. In effetti, queste sensazioni erano così comuni che ancora oggi trovo molte aziende che disabilitano completamente Windows Firewall su tutti i loro sistemi aggiunti a un dominio come una questione di politica predefinita. Se chiedi loro, di solito non c'è una ragione specifica per cui lo stanno facendo: è sempre stato così o è nella nostra politica di sicurezza scritta che sono risposte standard. Questo è un problema, perché Windows Defender Firewall con protezione avanzata (WFAS) che esiste nei sistemi operativi Windows di oggi è molto più robusto e avanzato che mai e può essere assolutamente utilizzato per migliorare la tua architettura di sicurezza.

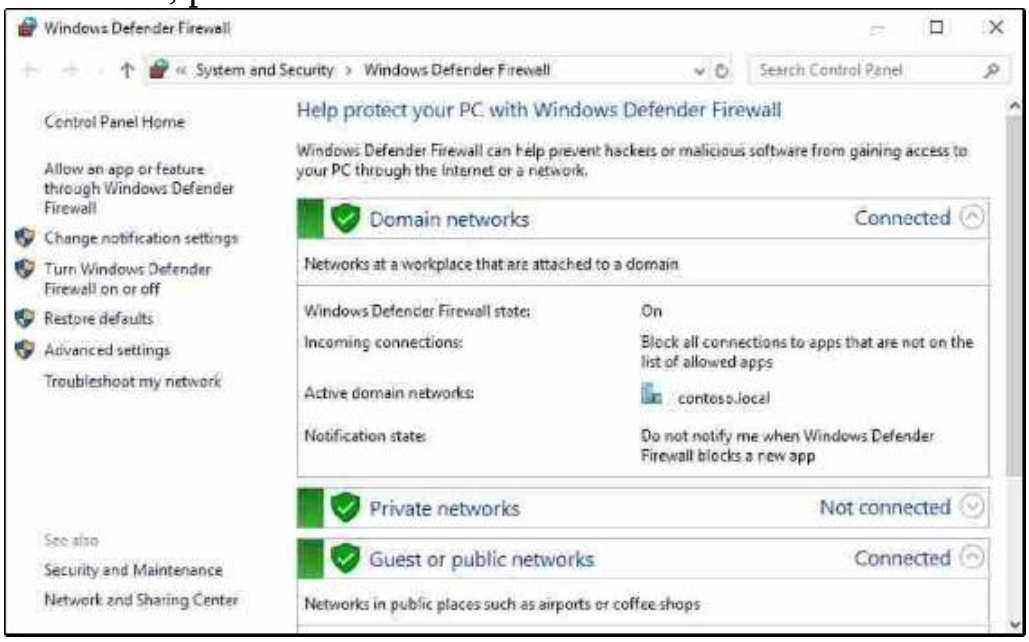
Tre console di amministrazione di Windows Firewall

Innanzitutto, è importante sapere che esistono tre diverse console da cui è possibile configurare le impostazioni di Windows Firewall. Due di queste console sono ridondanti l'una dell'altra e la terza è molto più capace delle altre. Diamo una rapida occhiata a ciascuno di essi.

Windows Defender Firewall (Pannello di controllo)

Quando si tenta di avviare qualsiasi applicazione o impostazione in Windows Server 2019, di solito è più efficiente fare semplicemente clic sul pulsante Start, quindi digitare una parola relativa all'attività che si sta tentando di eseguire. Nel mio caso, ho fatto clic su Start e ho digitato la parola firewall. L'opzione di corrispondenza migliore che è stata fornita per prima nei miei risultati di ricerca è stata Windows Defender Firewall, quindi sono andato avanti e ho fatto clic su di esso.

È interessante notare che questo collegamento apre la console di configurazione di Windows Firewall dall'interno del Pannello di controllo, il modo vecchio stile di eseguire le impostazioni di sistema. Questa console è ancora online e completamente in grado di manipolare le funzioni di firewall di base, come abilitare o disabilitare il firewall di Windows, ma poiché questo strumento risiede all'interno del Pannello di controllo, dobbiamo presumere che questo non sia in realtà lo strumento che Microsoft intende utilizzare . Ricorda, tutte le nuove funzionalità di configurazione sono state migrate nelle schermate Impostazioni di Windows, piuttosto che nel vecchio Pannello di controllo:

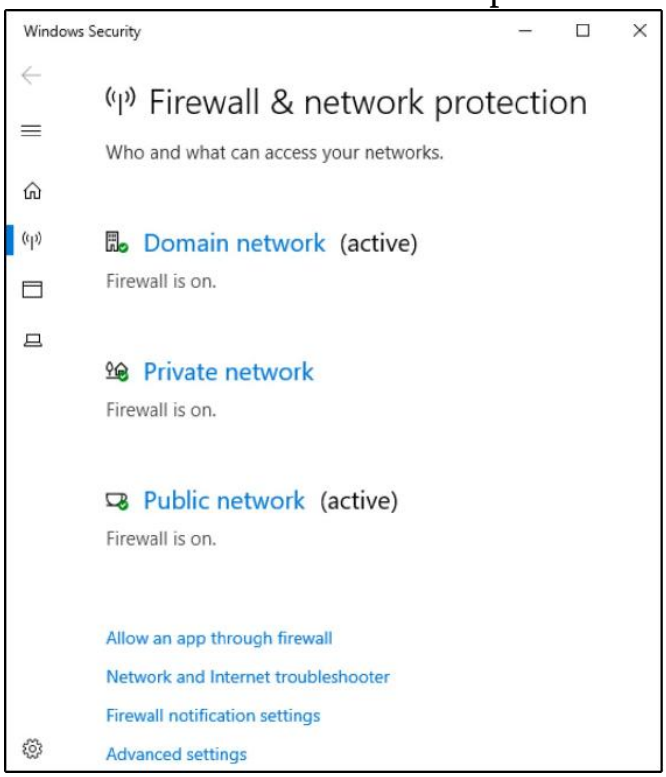


Firewall e protezione della rete (Impostazioni di sicurezza di Windows)

Sebbene gli strumenti basati sul pannello di controllo siano sempre stati il luogo appropriato per apportare queste modifiche nelle versioni precedenti del sistema operativo, sappiamo già che ci sono molte opzioni di Windows Defender memorizzate nelle Impostazioni di Windows. Potrebbe essere che ci siano anche le impostazioni di configurazione di

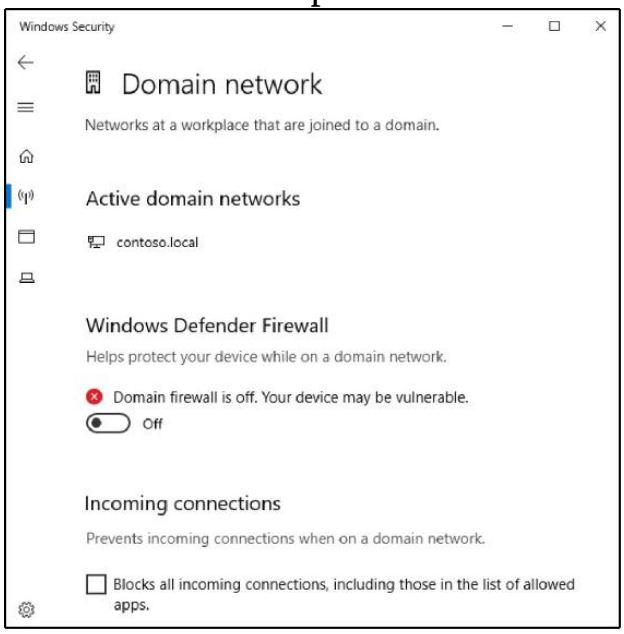
Windows Defender Firewall memorizzate nella sezione Sicurezza di Windows delle Impostazioni?

Sì, sicuramente ci sono. Apri le Impostazioni di Windows e fai clic su Aggiorna e sicurezza, quindi su Sicurezza di Windows. Sei già stato qui: questa è la schermata che fornisce un breve riepilogo dei componenti di Windows Defender. Certo, ce n'è uno qui chiamato Firewall e protezione di rete. Fare clic su quel pulsante e verrai reindirizzato a una nuova piattaforma di configurazione per le funzioni di Windows Firewall che non esistevano nelle versioni precedenti di Windows Server:



Facendo clic su uno dei collegamenti forniti qui si apriranno ulteriori opzioni di configurazione. Ad esempio, se si desidera abilitare o disabilitare rapidamente particolari profili firewall (ne parleremo a breve), è possibile fare clic sul profilo che si desidera configurare, come il profilo di rete del dominio, e da lì disattivare facilmente il firewall per questo profilo di rete. Molte aziende disabilitano il profilo di rete del dominio sulle proprie macchine, in modo che il firewall non protegga il traffico che avviene all'interno di una rete LAN aziendale.

Sebbene disabilitare il firewall sia generalmente una cattiva idea, a volte è necessario per adattarsi al tuo modello di business:



La schermata di configurazione del firewall disponibile nelle Impostazioni di Windows è un buon posto per prendere decisioni semplici e generali sul firewall di Windows Defender, ma questa interfaccia ha funzionalità limitate. Per qualsiasi utilizzo reale della funzionalità o configurazione del firewall ...

Windows Defender Firewall con protezione avanzata (WFAS)

Se sei come me, non sarai soddisfatto di queste informazioni e vorrai vedere cosa sta succedendo sotto il cofano, quindi vorrai un po 'più di informazioni di quelle che i soli strumenti di Windows Firewall possono darti. È possibile fare clic su uno dei collegamenti delle impostazioni avanzate mostrati nelle schermate precedenti o semplicemente aprire il prompt dei comandi o una finestra di dialogo Start | Esegui prompt e digita wf.msc. Entrambe queste funzioni avvieranno la console di amministrazione WFAS completa:

Qui puoi vedere informazioni molto più approfondite sull'attività e le regole in gioco con Windows Firewall e apportare modifiche più acute alle tue indennità e blocchi. È presente anche una sezione Monitoraggio in cui è possibile visualizzare le regole impegnate attivamente, comprese le regole di sicurezza della connessione. Questa è una sezione importante perché evidenzia il fatto che WFAS fa molto di più che bloccare il traffico di rete. Non è solo un firewall, è anche una piattaforma di connettività. Se prevedi di utilizzare IPsec per la crittografia del traffico di rete, sia esso IPsec nativo all'interno della tua rete o tramite la tecnologia di accesso remoto DirectAccess, vedrai le regole popolate in questa sezione che sono le definizioni di quei tunnel IPsec. Windows Firewall è effettivamente responsabile della realizzazione di tali connessioni e tunnel crittografati.

Tre diversi profili firewall

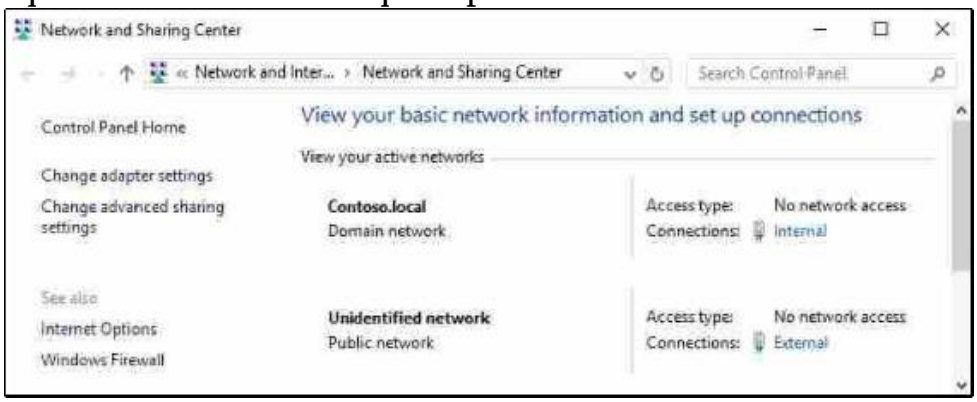
Quando una qualsiasi scheda NIC su un computer o un server è connessa a una rete, Windows Firewall assegnerà a quella connessione uno dei tre diversi profili. Probabilmente ti sei già interfacciato con questo processo decisionale senza nemmeno rendertene conto. Quando colleghi il tuo laptop al Wi-Fi nella tua caffetteria locale, Windows ti ha chiesto se ti stavi connettendo a una rete domestica, lavorativa o pubblica? Questo è il tuo Windows Firewall che ti chiede quale profilo desideri assegnare alla nuova connessione di rete. Il motivo per cui è possibile assegnare NIC e connessioni di rete a diversi profili firewall è che è possibile assegnare regole e criteri di accesso diversi per ciò che è o non è consentito su quei diversi profili. In effetti, ti sta chiedendo quanto ti fidi di questa rete? Per esempio, quando il tuo laptop è connesso alla rete aziendale potresti essere un po 'più rilassato rispetto a quando lo stesso laptop è connesso in un hotel in tutto il paese. Assegnando regole firewall più intense al profilo che è attivo quando sei in hotel, costruisci muri più grandi che gli aggressori devono affrontare quando sei fuori a lavorare su quella rete Internet pubblica. Diamo un'occhiata ai tre diversi tipi di profili disponibili, con una rapida descrizione di ciascuno:

- **Profilo di dominio**: Questo è l'unico che non puoi scegliere di assegnare. Il profilo di dominio è attivo solo quando ci si trova su un computer aggiunto a un dominio attualmente connesso a una rete in cui è accessibile un controller di dominio per il proprio dominio. Quindi, per qualsiasi macchina aziendale all'interno della rete aziendale, puoi aspettarti che il profilo di dominio sia attivo.
- **Profilo privato**: Quando ti connetti a una nuova rete e ti viene chiesto di scegliere dove sei connesso, se scegli Casa o Lavoro, a quella connessione verrà assegnato il Profilo privato.
- **Profilo pubblico**: Quando richiesto, se scegli Pubblico, ovviamente ti viene assegnato il profilo del firewall pubblico. Inoltre, se per qualche motivo non ti viene richiesto, o se non scegli affatto un'opzione e chiudi semplicemente la finestra che ti chiede cosa assegnare alla tua nuova connessione, questo profilo

pubblico sarà il profilo predefinito assegnato a eventuali connessioni che non hanno un profilo diverso già assegnato. Nelle versioni più recenti di Windows (in particolare in Win10), di solito non viene visualizzato il prompt che chiede che tipo di rete sia; invece viene visualizzato un messaggio che chiede se si desidera o meno consentire al computer di comunicare con altri dispositivi sulla nuova rete. In effetti, questo è sempre lo stesso prompt e la decisione che prendi a quel prompt assegnerà la tua connessione al profilo del firewall pubblico o privato.

Ad ogni connessione di rete viene assegnata la propria definizione di profilo, si potrebbe certamente avere più di un profilo firewall attivo contemporaneamente sullo stesso sistema. Ad esempio, il mio server RA1 è connesso sia alla rete aziendale che a Internet pubblico. All'interno di WFAS, puoi vedere che sia il profilo di dominio che il profilo pubblico sono attivi:

In alternativa, se apri Centro connessioni di rete e condivisione su questo server, possiamo anche vedere i profili elencati qui e puoi facilmente dire quale NIC sta usando quale profilo:



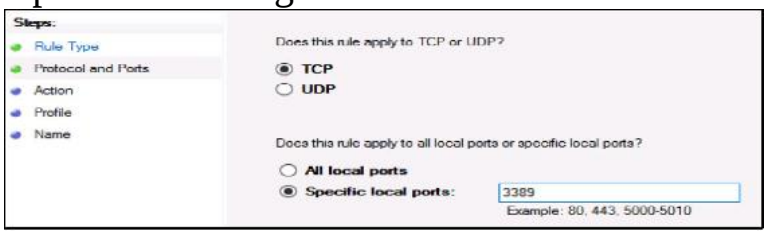
Creazione di una nuova regola del firewall in entrata

Ora sappiamo che la vera carne e le patate di Windows Firewall sono all'interno della console WFAS, quindi usiamo WFAS per costruirci una nuova regola. Su questo server RA1, ho abilitato l'accesso RDP in modo da poter gestire più facilmente questo server dalla mia scrivania. Tuttavia, attivando RDP ora ho consentito l'accesso RDP da tutte le reti su questo server.
Ciò significa che posso RDP in RA1 dall'interno della rete, ma posso anche RDP in RA1 da Internet, poiché questo è un server di accesso remoto e sembra essere connesso direttamente a Internet. Questo è un grosso problema, perché ora qualsiasi yahoo su Internet potrebbe potenzialmente trovare il mio server, trovare il prompt di accesso RDP e provare a far entrare la forza bruta in RA1.

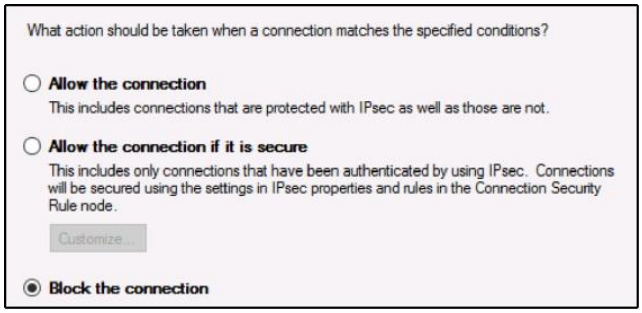
Per alleviare questo problema, voglio schiacciare RDP solo sul mio NIC esterno. Voglio che rimanga attivo all'interno in modo da poter continuare ad accedere al server dalla mia scrivania, ma esiste un modo semplice all'interno di WFAS per creare una regola firewall che blocchi l'accesso RDP solo dall'esterno? Sì, certamente c'è.

Apri wf.msc in ordine per avviare Windows Defender Firewall con sicurezza avanzata e accedere alla sezione Regole in entrata e vedrai tutte le regole del firewall in entrata esistenti che esistono su questo server (ci sono molte regole elencate qui anche se non hai mai visitato questa console prima, queste regole vengono installate con il sistema operativo). Fare clic con il pulsante destro del mouse su Regole in entrata e sceglie**Nuova regola.** Questo avvia una procedura guidata da cui creeremo
la nostra nuova regola del firewall. La prima schermata è dove identifichiamo il tipo di regola che vogliamo creare. È possibile creare una regola che modifica il traffico per un particolare programma oppure consultare un elenco di protocolli predefiniti. Tuttavia, mi piace sapere esattamente cosa sta facendo la mia regola a causa del modo in cui l'ho definita, non a causa di una definizione di protocollo preesistente, e so che

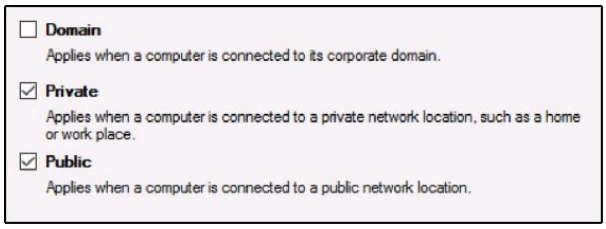
RDP funziona sulla porta TCP 3389. Quindi, sceglierò la porta su questa schermata, e dopo aver fatto clic su Avanti, definirò 3389 come la porta specifica che voglio modificare:



Il nostro terzo passo è decidere se vogliamo consentire o bloccare questa particolare porta. C'è una terza opzione elencata per consentire la connessione solo se è autenticata da IPsec, che è un'opzione potente, ma richiede che IPsec sia già stabilito nella nostra rete.
A causa di questo requisito, questa opzione non si applica alla maggior parte delle persone. Per il nostro esempio, abbiamo già RDP funzionante, ma vogliamo bloccarlo su una delle NIC, quindi sceglierò Blocca la connessione:



Tuttavia, non vogliamo bloccare RDP per tutti i NIC, quindi questa schermata successiva è molto importante. Qui dobbiamo fare riferimento alle nostre conoscenze sui profili firewall di cui abbiamo parlato. Ricorda che alle schede NIC interne connesse alla nostra rete di dominio verrà assegnato il profilo di dominio. Tuttavia, qualsiasi scheda NIC non connessa a una rete interna in cui risiede un controller di dominio avrà profili pubblici o privati attivi. Questa è la conoscenza che dobbiamo impiegare su questo schermo. Se si desidera disabilitare RDP solo sulla scheda NIC esterna, è necessario che questa regola sia attiva solo per il profilo privato e il profilo pubblico. Infatti, guardando indietro agli screenshot che abbiamo già acquisito, possiamo vedere che alla scheda NIC esterna è assegnato specificamente il profilo pubblico, e quindi potremmo selezionare solo la casella di controllo Pubblica qui e RDP verrebbe quindi bloccato sulla NIC esterna. Ma nel caso in cui in futuro aggiungeremo più NIC a questo server su cui vogliamo assicurarci che l'accesso RDP non sia possibile, lasceremo sia Pubblico che Privato selezionati, per garantire una migliore sicurezza per il futuro. Assicurati di deselezionare il profilo di dominio! Altrimenti bloccherai completamente l'accesso RDP e se stai attualmente utilizzando RDP per connetterti a questo server, ti espellerai e non sarai in grado di riconnetterti:


Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.

E ora creiamo semplicemente un nome per la nostra nuova regola, e abbiamo finito! La nostra capacità di eseguire l'RDP in questo server da Internet è stata immediatamente disabilitata e stanotte possiamo riposare molto più facilmente.

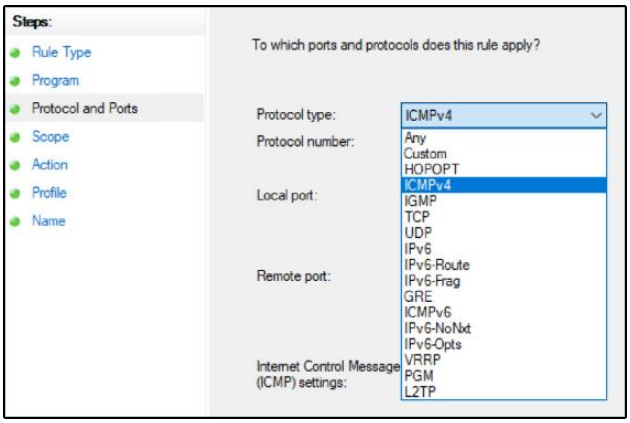
Creazione di una regola per consentire i ping (ICMP)

Molto spesso mi trovo a dover creare una regola di autorizzazione o di blocco per ICMP. In altre parole, mi trovo spesso a dover regolare il firewall sui server per abilitare o disabilitare la loro capacità di rispondere alle richieste di ping. Probabilmente hai notato con i sistemi operativi server più recenti che è abbastanza normale che il firewall blocchi automaticamente i ping (ICMP) immediatamente. Questo è un problema per gli ambienti in cui il ping è il metodo standard per verificare se un indirizzo IP viene utilizzato o disponibile. Potreste ridere, ma, credetemi, ci sono ancora molti amministratori IT là fuori che non tengono traccia di quali indirizzi IP hanno utilizzato all'interno delle loro reti, e quando si trovano di fronte alla necessità di configurare un nuovo server e decidono quale indirizzo IP dargli, iniziano semplicemente a eseguire il ping degli indirizzi IP nella loro rete fino a quando non ne trovano uno che scade! L'ho visto così tante volte. Anche se questo non è ovviamente un buon modo per gestire gli indirizzi IP, succede. Sfortunatamente, questo metodo incontra grossi problemi, perché la maggior parte delle nuove installazioni di Windows sono progettate per bloccare le risposte ICMP immediatamente, il che significa che potresti eseguire il ping di un indirizzo IP e ricevere un timeout, ma potrebbe effettivamente esserci un server in esecuzione su quell'indirizzo IP .

Quindi, tornando al punto. Potrebbe essere necessario abilitare ICMP sul nuovo server, in modo che risponda quando qualcuno tenta di eseguirne il ping. Quando dobbiamo creare una nuova regola che consenta l'esecuzione dei ping, impostiamo una regola proprio come abbiamo fatto per RDP, ma c'è un grosso problema. Nella primissima schermata Tipo di

regola quando si crea la nuova regola in cui è necessario identificare il tipo di regola che si sta creando, non ci sono opzioni o predefinizioni per ICMP. Lo trovo strano perché questo è un tipo di regola molto comune da mettere in atto, ma purtroppo scegliere ICMP dall'elenco a discesa sarebbe troppo facile. Invece, quello che devi fare è creare una nuova regola in entrata proprio come abbiamo fatto per RDP, ma nella primissima schermata per Tipo di regola, assicurati di selezionare l'opzione che dice Personalizzato.

Quindi, lascia l'opzione selezionata per definire questa regola per Tutti i programmi. Fai di nuovo clic su Avanti e ora hai una casella a discesa chiamata Tipo di protocollo. Questo è il menu in cui puoi scegliere la nuova regola per manipolare il traffico ICMP. Come puoi vedere nello screenshot seguente, puoi scegliere ICMPv4 o ICMPv6, a seconda di come appare il tuo traffico di rete. Il mio laboratorio di prova è solo IPv4, quindi sceglierò ICMPv4:

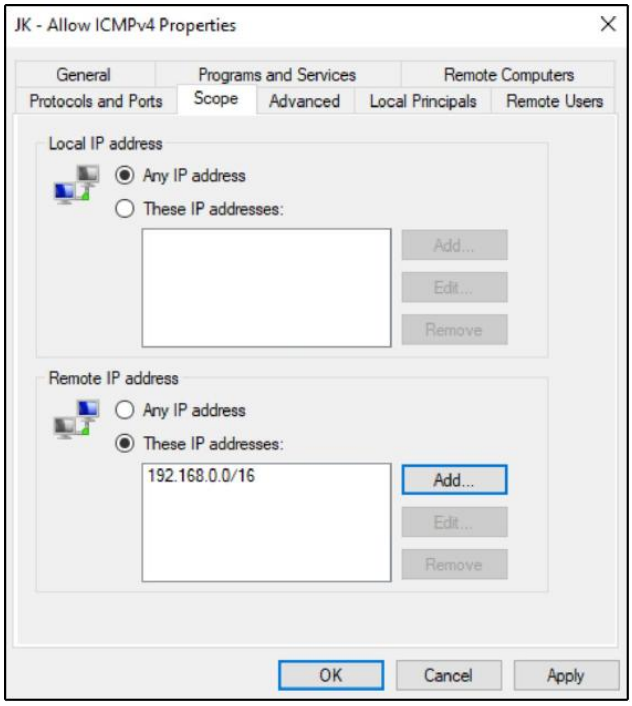


Per il resto della creazione della regola ICMP, segui le stesse procedure descritte quando abbiamo creato la regola RDP, scegliendo di consentire o bloccare questo traffico e per quali profili firewall. Una volta terminato, la tua nuova regola ICMPv4 viene immediatamente applicata e, se hai configurato una regola Consenti, il tuo nuovo server ora risponderà correttamente alle richieste di ping:

```
PS C:\Users\administrator.CONTOSO> ping ra1

Pinging ra1.contoso.local [10.10.10.13] with 32 bytes of data:
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
```

Se mai hai bisogno di modificare una regola o scavare in proprietà più avanzate di una regola firewall, torna alla schermata Regole in entrata puoi fare clic con il tasto destro su qualsiasi regola firewall individuale e andare in Proprietà. All'interno di queste schede, hai la possibilità di modificare qualsiasi criterio sulla regola. Ad esempio, è possibile ospitare porte aggiuntive, modificare i profili firewall a cui si applica o persino limitare gli indirizzi IP specifici a cui si applica questa regola utilizzando la scheda Ambito.

Ciò consente di applicare la regola del firewall solo al traffico in entrata o in uscita da una parte specifica della rete o da un determinato sottoinsieme di macchine. Ad esempio, qui ho modificato la mia scheda Ambito per riflettere che desidero applicare questa regola del firewall solo al traffico in arrivo dalla sottorete 192.168.0.0/16:



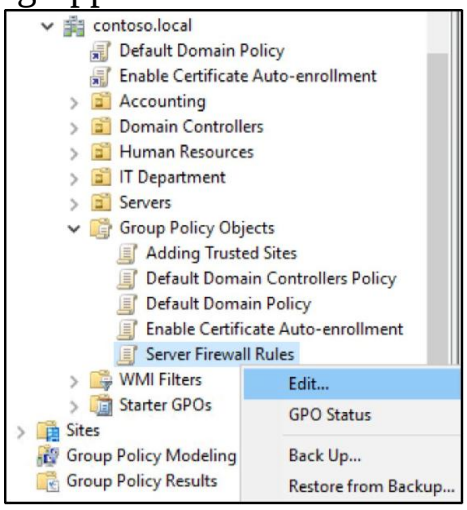
Gestione di WFAS con Criteri di gruppo

La gestione delle regole del firewall sui tuoi server e client può essere un enorme passo avanti verso un ambiente più sicuro per la tua azienda. La parte migliore? Questa tecnologia è di classe enterprise e può essere utilizzata gratuitamente poiché è già integrata nei sistemi operativi che utilizzi. L'unico costo associato al firewall a questo livello è il tempo necessario per mettere in atto tutte queste regole, il che sarebbe un incubo amministrativo se dovessi implementare l'intero elenco di autorizzazioni e blocchi su ogni macchina individualmente.

Grazie al cielo per l'oggetto Criteri di gruppo (GPO). Come con la maggior parte delle impostazioni e delle funzioni all'interno della piattaforma Microsoft Windows, la configurazione di un criterio firewall che si applica a tutti è un gioco da ragazzi per le macchine che fanno parte del dominio. Puoi persino suddividerlo in più set di criteri, creando un GPO che applica le regole del firewall ai tuoi client e un GPO separato che applica le regole del firewall ai tuoi server, come ritieni opportuno. Il punto è che puoi raggruppare più macchine in categorie, creare un set di regole GPO per ogni categoria e applicarlo automaticamente a ogni macchina utilizzando le potenti capacità di distribuzione del GPO.

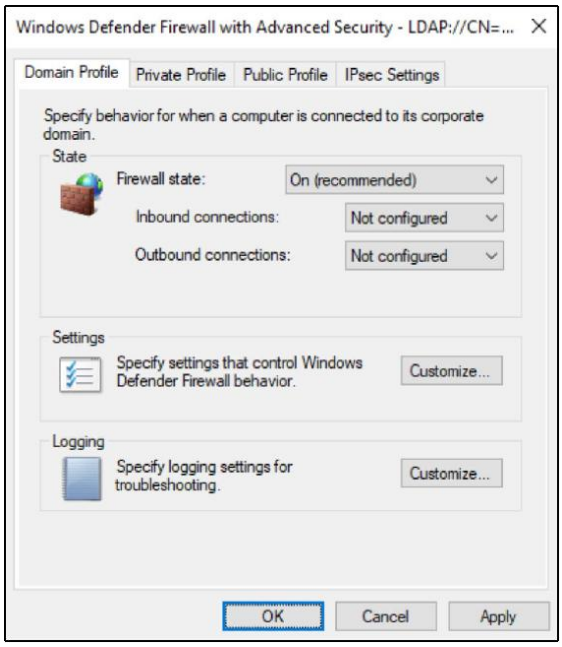
Hai già familiarità con la creazione di oggetti Criteri di gruppo, quindi vai avanti e creane uno ora che conterrà alcune impostazioni del firewall con cui possiamo giocare. Collega e filtra l'oggetto Criteri di gruppo di conseguenza in modo che solo le macchine per le quali desideri avere le impostazioni le ottengano effettivamente. Forse un buon punto di partenza è un test di unità organizzativa, in modo che tu possa assicurarti che tutte le regole che stai per inserire all'interno dell'oggetto Criteri di gruppo funzionino bene insieme e con tutte le altre tue politiche esistenti, prima di distribuire la nuova politica alla tua forza lavoro di produzione .

Una volta creato il nuovo oggetto Criteri di gruppo, fare clic con il tasto destro su di esso dall'interno della Console di gestione dei criteri di gruppo e fare clic su Modifica ...:



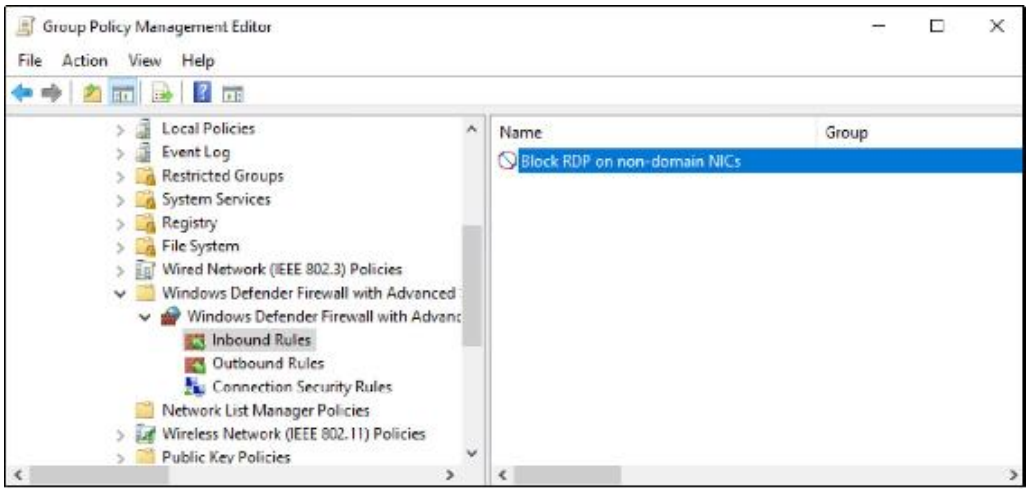
Ora che stiamo esaminando l'interno di questo nuovo oggetto Criteri di gruppo, dobbiamo solo capire dove si trova la posizione corretta per poter creare alcune nuove regole del firewall. Quando si esaminano le regole sulla macchina locale stessa, tutto è elencato sotto un'intestazione Windows Defender Firewall con protezione avanzata e si trova in Configurazione computer | Politiche | Impostazioni di Windows | Impostazioni di sicurezza | Windows Defender Firewall con protezione avanzata | Windows Defender Firewall con sicurezza avanzata:

Come puoi vedere, questo è anche il posto dove andare quando vuoi assicurarti che determinati profili del firewall, o il Windows Firewall nel suo insieme, siano specificamente attivati o disattivati. Quindi, questo è lo stesso posto in cui andresti se volessi disabilitare Windows Firewall per tutti. Facendo clic sulle proprietà di Windows Defender Firewall, collegamento mostrato in precedenza, è possibile determinare individualmente lo stato di ciascun profilo firewall:



Una volta terminato di impostare i profili in base alle proprie esigenze, fare clic su OK e ci si ritrova nella parte WFAS dell'oggetto Criteri di gruppo. Proprio come nella console WFAS locale, hai categorie per Regole in entrata e Regole in uscita. È sufficiente fare clic con il pulsante destro del mouse su Regole in entrata e fare clic su Nuova regola ... per iniziare a creare una regola direttamente in questo GPO. Segui la stessa procedura guidata con cui hai già familiarità con la creazione di una regola nella console WFAS locale e, al termine, la nuova regola del firewall in ingresso viene visualizzata all'interno dell'oggetto Criteri di gruppo.

Questa regola firewall si sta già diffondendo in Active Directory e si installa su quei computer e server che hai definito nei collegamenti e nei criteri di filtro:



Tecnologie di crittografia

Un'idea che ha fatto un rapido passo da qualcosa con cui le grandi organizzazioni stanno giocando a tutti quelli di cui hanno bisogno è l'uso della crittografia. La maggior parte di noi crittografa il traffico del nostro sito Web per molti anni utilizzando siti Web HTTPS, ma anche in quel campo ci sono eccezioni sorprendenti, con molte società di web hosting a basso costo che forniscono ancora pagine di accesso che trasmettono il traffico in chiaro. Questo è terribile, perché con qualsiasi cosa che invii su Internet ora utilizzando il normale HTTP o un'e-mail non crittografata devi presumere che venga letta da qualcun altro. È probabile che tu sia paranoico e nessuno stia effettivamente intercettando e leggendo il tuo traffico, ma devi sapere che se stai accedendo a un sito Web che dice HTTP nella barra degli indirizzi o se stai inviando un'e-mail da uno qualsiasi dei servizi di posta elettronica gratuiti ,
quell'email può essere facilmente rubata da qualcuno dall'altra parte del mondo. La crittografia dei dati è un requisito assoluto in questi giorni per le informazioni aziendali che devono attraversare Internet; sebbene allo stesso tempo lo dica, il retro della mia mente mi dice che la stragrande maggioranza delle aziende non utilizza ancora alcun tipo di tecnologia di crittografia sul proprio sistema di posta elettronica, e quindi è ancora un potenziale disastro in attesa di accadere per la maggior parte .

Sebbene stiamo migliorando sempre di più nella protezione del traffico del browser Internet, tradizionalmente ancora non prestiamo molta attenzione ai dati che sono al sicuro all'interno delle mura della nostra organizzazione. I cattivi non sono stupidi, però, e hanno una cassetta degli attrezzi molto ampia di trucchi per ingegnerizzare socialmente la loro strada nelle nostre reti. Una volta dentro, cosa trovano? Nella maggior parte dei casi, è un grande free-for-all. Ottieni un account utente o un computer e hai le chiavi per gran parte del regno. Fortunatamente, ci sono diverse tecnologie integrate in Windows Server 2019 progettate per combattere queste intrusioni e proteggere i tuoi dati anche quando si trovano all'interno delle quattro mura del tuo data center. Permettere'

BitLocker e il TPM virtuale

BitLocker è una tecnologia che è diventata abbastanza familiare da vedere sui nostri sistemi client all'interno delle reti aziendali. È una tecnologia di crittografia dell'intera unità, che ci offre il vantaggio di assicurarci che i nostri dati siano completamente protetti su laptop o computer che potrebbero essere rubati. Se un ladro mette le mani su un laptop aziendale, estrae il disco rigido e lo collega al computer ... scusa, Charlie, nessun accesso. L'intero volume è crittografato. Ciò ha molto senso per l'hardware mobile che potrebbe essere facilmente perso o rubato, ma nelle fasi iniziali di questa tecnologia non è mai stata presa in considerazione l'utilizzo di BitLocker per proteggere i nostri server.

Con l'adozione crescente delle risorse di cloud computing, improvvisamente ha molto più senso volere BitLocker sui nostri server. Più in particolare quando parliamo di cloud, ciò che vogliamo veramente è BitLocker sulle nostre macchine virtuali, siano esse sistemi operativi client o server. Sia che tu stia archiviando le tue macchine virtuali (VM) in un vero ambiente cloud fornito da un provider di servizi di cloud pubblico o che tu stia ospitando il tuo cloud privato dove i tenant raggiungono per creare e gestire le proprie VM, senza la possibilità di crittografare quei dischi rigidi virtuali —I file VHD e VHDX — i tuoi dati non sono assolutamente protetti. Perché no? Perché chiunque abbia

diritti amministrativi sulla piattaforma host di virtualizzazione può facilmente accedere a tutti i dati che si trovano sui dischi rigidi del tuo server, anche senza alcun tipo di accesso alla tua rete o account utente sul tuo dominio. Tutto quello che devono fare è prendere una copia del tuo file VHDX (l'intero contenuto del disco rigido del tuo server), copiarlo su una chiavetta USB, portarlo a casa, montare questo disco rigido virtuale sul proprio sistema e bingo: hanno l'accesso al disco rigido del tuo server e ai tuoi dati. Questo è un grosso problema per la conformità alla sicurezza dei dati.

Perché storicamente non è stato possibile crittografare le VM? Perché BitLocker viene fornito con un requisito interessante. Il disco rigido è crittografato, il che significa che non può avviarsi senza che la crittografia sia sbloccata. Come sblocciamo il disco rigido in modo che la nostra macchina possa avviarsi? Uno dei due modi. Il metodo migliore è memorizzare le chiavi di sblocco all'interno di un Trusted Platform Module (TPM). Si tratta di un microchip fisico integrato nella maggior parte dei computer che acquisti oggi. Memorizzare la chiave di sblocco di BitLocker su questo chip significa che non devi collegare nulla fisicamente al tuo computer per farlo avviare, devi semplicemente inserire un pin per accedere al TPM, quindi il TPM sblocca BitLocker. D'altra parte, se scegli di distribuire BitLocker senza la presenza di un TPM, per sbloccare un volume BitLocker e renderlo avviabile, è necessario collegare una chiavetta USB fisica che contenga le chiavi di sblocco di BitLocker. Vedi il problema con uno di questi percorsi di installazione in uno scenario di macchina virtuale? Le VM non possono non avere un chip TPM fisico e non hai nemmeno un modo semplice per collegare una chiavetta USB! Quindi, come crittografiamo quelle VM in modo che gli occhi indiscreti della società di cloud hosting non possano vedere tutte le mie cose?

Immettere il TPM virtuale. Questa capacità ci è arrivata completamente nuova in Windows Server 2016; ora abbiamo la capacità di fornire ai nostri server virtuali un TPM virtuale che può essere utilizzato per archiviare queste chiavi! Questa è una notizia incredibile e significa che possiamo finalmente crittografare i nostri server, sia che siano ospitati su server Hyper-V fisici nel nostro data center o che si trovino nel cloud di Azure.

VM schermate

L'utilizzo di BitLocker e dei TPM virtuali per crittografare e proteggere i file del disco rigido virtuale produce qualcosa chiamato VM schermate. Le macchine virtuali schermate erano una funzionalità introdotta per la prima volta in Windows Server 2016 e sono state migliorate in Server

2019. So che questo è solo un piccolo assaggio e un'anteprima di questa straordinaria nuova tecnologia, ma volevo menzionarlo qui perché si riferisce sicuramente al stato di sicurezza generale dei nostri ambienti server.

Tratteremo molti più dettagli sulle VM schermate in Capitolo 12, Virtualizzazione del data center con Hyper-V.

Reti virtuali crittografate

Non sarebbe fantastico se potessimo configurare, controllare e governare le nostre reti da un'interfaccia amministrativa grafica, piuttosto che guardare i router a CLI tutto il giorno? Non trarremmo vantaggio dalla flessibilità di rete per spostare server e carichi di lavoro da una sottorete all'altra, senza dover modificare l'indirizzo IP o il routing su quei server? Non potremmo trovare un modo per crittografare automaticamente tutto il traffico che scorre tra i nostri server, senza dover configurare tale crittografia sui server stessi?

Sì sì sì! Attraverso l'uso di Software Defined Networking (SDN) e una nuova funzionalità chiamata reti virtuali crittografate, possiamo realizzare tutte queste cose. Questa sezione di testo è in realtà solo un punto di riferimento, un luogo verso cui riportarti indietroCapitolo 5, Collegamento in rete con Windows Server 2019, se lo hai saltato e invece sei atterrato qui. Abbiamo già discusso di SDN e della sua nuova capacità di creare e crittografare automaticamente le reti virtuali che fluiscono tra VM Hyper-V e server host Hyper-V, quindi se questa idea ti intriga, assicurati di tornare indietro e rivisitare quel capitolo.

Crittografia del file system

Encrypting File System (EFS) è un componente di Microsoft Windows che esiste da molti anni su sistemi operativi sia client che server. Mentre BitLocker è responsabile della protezione di un intero volume o disco, EFS è un po 'più particolare. Quando vuoi crittografare solo documenti o cartelle particolari, questo è il posto a cui ti rivolgi. Quando si sceglie di crittografare i file utilizzando EFS, è importante comprendere che Windows deve utilizzare un certificato utente come parte del processo di crittografia / decrittografia, quindi la disponibilità di una PKI interna è la chiave per una corretta distribuzione. È anche importante notare che le chiavi di autenticazione sono legate alla password dell'utente, quindi un account utente completamente compromesso potrebbe annullare i vantaggi forniti da EFS.

Penso che molte aziende non impieghino EFS perché lasci all'utente la decisione su quali documenti crittografare. Ciò significa anche che dipendi da loro per ricordarti di eseguire la crittografia in primo luogo, il che significa che dovranno comprenderne l'importanza per renderlo degno del loro tempo. Volevo menzionare EFS perché è ancora attivo ed è ancora una piattaforma valida per la quale è possibile crittografare i dati, ma la maggior parte degli amministratori approda a BitLocker come soluzione migliore. La mancanza di responsabilità da parte dell'utente e una buona piattaforma di gestione centralizzata fanno di BitLocker un solido passo avanti rispetto a EFS. Entrambe le tecnologie potrebbero

certamente coesistere, tuttavia, mantenendo i dati al sicuro su due livelli diversi invece di fare affidamento su una sola delle tecnologie di crittografia dei dati a tua disposizione.

IPsec

Gran parte della tecnologia di crittografia integrata nei sistemi operativi ruota attorno ai dati inattivi. Ma per quanto riguarda i nostri dati in movimento? Abbiamo parlato dell'utilizzo di SSL sui siti Web HTTPS come metodo per crittografare i dati del browser Web in movimento su Internet, ma per quanto riguarda i dati che non fluiscono attraverso un browser Web?

E se non fossi nemmeno preoccupato per Internet? e se fossi interessato a proteggere il traffico che potrebbe anche fluire da un punto all'altro all'interno della mia rete aziendale? C'è qualcosa che può aiutare con questo tipo di requisiti? Certamente.

IPsec è una suite di protocolli che può essere utilizzata per autenticare e crittografare i pacchetti che avvengono durante una comunicazione di rete. IPsec non è una tecnologia specifica del mondo Microsoft, ma in Windows Server 2019 ci sono vari modi in cui IPsec può essere utilizzato per proteggere i dati che stai spostando avanti e indietro tra le macchine.

Il luogo più comune in cui viene visualizzata l'interazione IPsec su un server Windows è quando si utilizza il ruolo di accesso remoto. Quando configuri la VPN sul tuo server RA, avrai a disposizione diversi protocolli di connessione che i client VPN possono utilizzare per connettersi al server VPN. In questo elenco di possibili piattaforme di connessione sono inclusi i tunnel IPsec (IKEv2). La seconda tecnologia di accesso remoto che utilizza IPsec è DirectAccess. Quando si stabilisce DirectAccess nella rete, ogni volta che un computer client crea un tunnel DirectAccess su Internet al server DirectAccess, quel tunnel è protetto da IPsec.
Per fortuna la console di gestione dell'accesso remoto che usi per distribuire sia VPN che DirectAccess è abbastanza intelligente da sapere tutto ciò che è necessario per far funzionare l'autenticazione e la crittografia IPsec, e non è necessario sapere una sola cosa su IPsec per renderli le tecnologie di accesso remoto lavorano per te!

Il grande fattore mancante con IPsec fornito dal ruolo di accesso remoto è il traffico all'interno della rete. Quando parli di VPN o DirectAccess, parli di traffico che si muove su Internet. Ma cosa succede se si desidera semplicemente crittografare il traffico che si sposta tra due server diversi all'interno della stessa rete? O il traffico che fluisce dai computer client all'interno dell'ufficio ai loro server locali, anch'essi situati in ufficio? È qui che una certa conoscenza delle impostazioni dei criteri IPsec è utile, perché possiamo specificare che vogliamo che il traffico in movimento all'interno delle nostre reti aziendali venga crittografato utilizzando IPsec. Realizzare ciò significa mettere in atto le politiche giuste.

Configurazione di IPsec

Esistono due posizioni diverse in cui è possibile configurare le impostazioni IPsec in un ambiente Microsoft Windows. Sia i vecchi che i nuovi sistemi possono essere forniti con configurazioni IPsec tramite il tradizionale snap-in IPsec Security Policy. Se stai eseguendo tutti i sistemi più recenti, come Windows 7 e Server 2008 e versioni successive, puoi in alternativa utilizzare Windows Defender Firewall con sicurezza avanzata per impostare i tuoi criteri IPsec.
WFAS è la soluzione più flessibile, ma non è sempre un'opzione a seconda dello stato dei sistemi legacy nel tuo ambiente.

Per prima cosa, diamo un'occhiata alla vecchia console dei criteri IPsec. Inizieremo da qui perché le diverse opzioni disponibili ci aiuteranno a costruire una linea di base per iniziare a comprendere il modo in cui funziona l'interazione IPsec tra due endpoint. Esistono tre diverse classificazioni di criteri IPsec che possono essere assegnati alle macchine che incontreremo in questa console. Dedichiamo un minuto per spiegare ciascuno di essi, perché i nomi delle politiche possono essere un po 'fuorvianti. La comprensione di queste opzioni ti consentirà di fare un passo avanti per capire come funzionano anche le impostazioni all'interno di WFAS.

Criterio del server

La politica del server dovrebbe probabilmente essere rinominata in politica del richiedente, perché questo è davvero ciò che fa questo. Quando un computer o un server invia una richiesta di rete in uscita a un altro computer o server, richiede di stabilire una connessione di rete. Su questi computer richiedenti, quelli che avviano il traffico, è qui che diciamo di applicare il criterio del server IPsec. Una volta applicato, il criterio del server indica a quel computer o server di richiedere la crittografia IPsec per la sessione di comunicazione tra la macchina che ha avviato e il computer remoto. Se il sistema remoto supporta IPsec, viene creato il tunnel IPsec per proteggere il traffico che scorre tra le due macchine. La politica del server è tuttavia piuttosto indulgente e se il computer remoto non supporta IPsec, la connessione di rete ha ancora successo, ma rimane non crittografata.

Criterio del server sicuro

La differenza qui è che il criterio del server sicuro richiede la crittografia IPsec per consentire la comunicazione di rete. La normale politica del server di cui abbiamo parlato in precedenza verrà crittografata con IPsec quando possibile, ma se non è possibile continuerà a fluire il traffico non crittografato. Il criterio del server

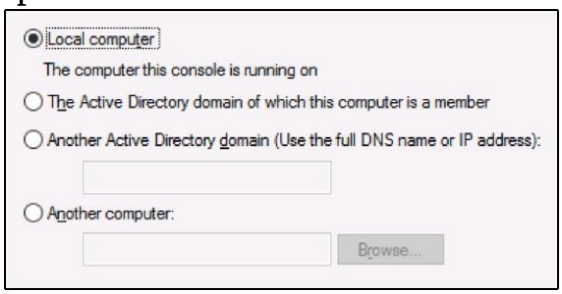
sicuro, d'altra parte, non riuscirà a stabilire la connessione se IPsec non può essere negoziato tra le due macchine.

Politica del cliente

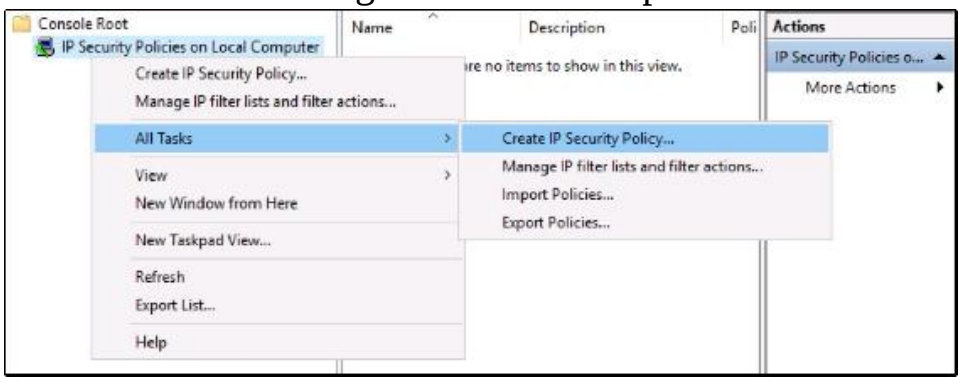
La politica del client deve essere rinominata in politica di risposta, perché questa si trova all'altra estremità della connessione. La politica del client non si preoccupa di richiedere una sessione IPsec, si preoccupa solo di riceverne una. Quando un computer effettua una richiesta di rete a un server e quel computer ha il criterio Server o Secure Server quindi richiede IPsec, il server dovrebbe avere il criterio Client assegnato per accettare e costruire quel tunnel IPsec. La politica del client risponde consentendo la crittografia in quella sessione.

Snap-in Criterio di sicurezza IPsec

La console originale per la manipolazione delle impostazioni IPsec è accessibile tramite MMC. Aprilo e aggiungi lo snap-in Gestione criteri di sicurezza IP. È interessante notare che, quando si aggiunge questo snap-in, si noterà che è possibile visualizzare il criterio IPsec locale della macchina, a cui si è attualmente connessi, oppure è possibile aprire il criterio IPsec per il dominio stesso. Se sei interessato a configurare un'implementazione IPsec a livello di dominio, questa sarebbe la tua zona di destinazione per lavorare su tali impostazioni. Ma allo scopo di mettere la nostra testa qui per curiosare un po ', puoi scegliere il computer locale per dare un'occhiata alla console:

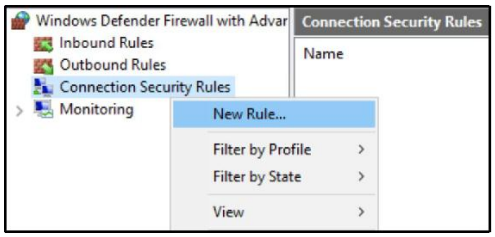


Una volta all'interno, è possibile visualizzare eventuali criteri IPsec esistenti che potrebbero essere in atto, oppure è possibile iniziare a crearne uno personalizzato utilizzando l'azione Crea criterio di protezione IP ... disponibile facendo clic con il pulsante destro del mouse su Criteri di protezione IP. In questo modo verrà richiamata una procedura guidata che illustrerà la configurazione del tuo particolare criterio IPsec:

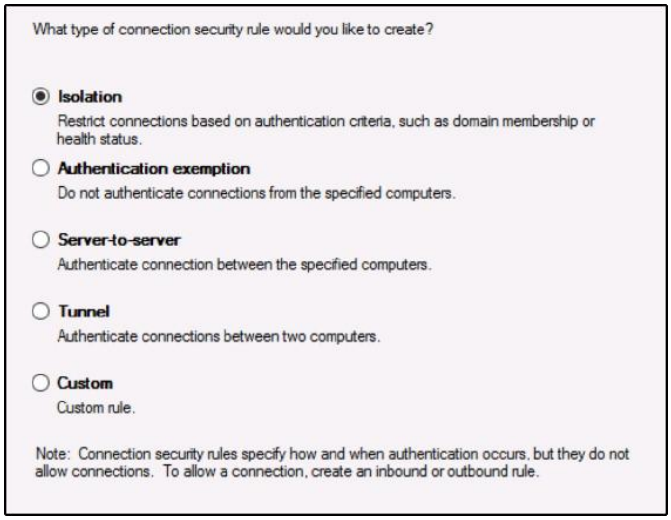


Utilizzando invece WFAS

La piattaforma più recente utilizzata per stabilire le regole di connessione IPsec è Windows Defender Firewall con sicurezza avanzata. Vai avanti e aprilo, come hai già familiarità con il fare. Una volta dentro, vai alla sezione Regole di sicurezza della connessione, che è elencata immediatamente sotto Regole in entrata e Regole in uscita. Regole di sicurezza della connessione, è dove si definiscono le regole di connessione IPsec. Se fai clic con il pulsante destro del mouse su Regole di sicurezza della connessione e scegli Nuova regola ... seguirai una procedura guidata simile a quella per la creazione di una regola del firewall:



Una volta all'interno della procedura guidata per creare la nuova regola, inizi a vedere che le opzioni a tua disposizione sono abbastanza diverse da quelle mostrate durante la creazione di una nuova regola firewall. Questa è la piattaforma dalla quale stabilirai le regole di sicurezza della connessione IPsec che definiscono l'aspetto dei tunnel IPsec e su quali macchine o indirizzi IP devono essere attivi:



Non abbiamo spazio qui per coprire tutte le opzioni disponibili in questa procedura guidata, ma consiglio vivamente di riprendere da qui e di fare un ulteriore passo avanti con alcune conoscenze aggiuntive su TechNet, come indicato qui: https: //documenti.microsoft.com /en-noi/precedente- versioni /finestre/esso-pro /finestre-server-2012-R2-e-2012 /hh831807 (v =ws.11).

Password vietate

Se sei un cliente di Azure Active Directory, hai già accesso a questa nuova funzione chiamata password vietate. L'idea è questa: Microsoft mantiene un elenco continuo globale di password comunemente errate (come la parola password) e blocca automaticamente tutte le varianti di password come P @ ssword, Password123 e così via. Ognuna di queste potenziali password verrebbe bloccata del tutto se un utente provasse a crearne una come propria password. Hai anche la possibilità di aggiungere le tue password vietate personalizzate all'interno dell'interfaccia di Azure Active Directory. Dopo aver escluso le password attive e in esecuzione in Azure, questa funzionalità può essere trasferita anche nell'ambiente Active Directory locale, implementando il servizio proxy di protezione password di Azure Active Directory (accidenti, è un boccone). Questo proxy si interfaccia tra i controller di dominio locali e Azure Active Directory, assicurando che le password che gli utenti tentano di inserire nei controller di dominio locali si adattino alle regole definite dagli algoritmi delle password vietate di Azure.

Per poter utilizzare questa tecnologia, devi ovviamente utilizzare Azure Active Directory, quindi non è per tutti. Tuttavia, se si dispone e si sincronizza con Azure Active Directory, questa funzionalità viene persino trasferita nelle versioni precedenti dei controller di dominio locali.
Questi server possono essere vecchi quanto Windows Server 2012.

Di seguito è riportato un collegamento a ulteriori informazioni sulle password vietate: https: //documenti.microsoft.com /en-noi/azzurro/attivo-directory /autenticazione/concetto-parola d'ordine-bandire-male-su- premesse.

Analisi avanzata delle minacce

A mio parere, una delle funzionalità di sicurezza più interessanti emerse da Microsoft negli ultimi anni è l'Advanced Threat Analytics (ATA), eppure non sento quasi nessuno parlarne. Non è una caratteristica o una funzione integrata nel sistema operativo Windows Server, non ancora comunque, ma è un software locale che funziona su Windows per produrre alcune funzionalità sorprendenti. In sostanza, ciò che ATA fa è monitorare tutto il tuo traffico Active Directory e ti avverte di comportamenti pericolosi o insoliti in tempo reale, non appena si verificano.

L'idea di ATA è piuttosto semplice da capire e ha così tanto senso comune che è qualcosa che ci chiederemo tutti perché ci è voluto così tanto tempo per metterla in atto. La ragione di ciò, tuttavia, è perché sotto il cofano l'elaborazione e l'apprendimento che ATA sta facendo è molto avanzato. Sì, ho detto imparare. Questa è la parte più interessante di ATA. Configurare la rete in modo che tutto il traffico in entrata o in uscita dai controller di dominio arrivi anche al sistema ATA. Il modo più sicuro per ottenere ciò è a livello di rete, stabilendo il mirroring delle porte in modo che anche tutti i pacchetti del controller di dominio raggiungano ATA, ma a un livello che un utente malintenzionato non sarebbe in grado di vedere. In questo modo, anche se qualcuno di malvagio è all'interno della tua rete ed è alla ricerca di un qualche tipo di protezione che funzioni contro di loro, ATA rimane invisibile ai loro occhi indiscreti. Tuttavia, il port mirroring di quel traffico è qualcosa che le aziende più piccole potrebbero non essere in grado di fare o potrebbe essere troppo complesso per una configurazione iniziale, quindi esiste una seconda opzione per installare un agente leggero ATA direttamente sui controller di dominio stessi. Questo agente invia quindi le informazioni necessarie ai server di elaborazione ATA.

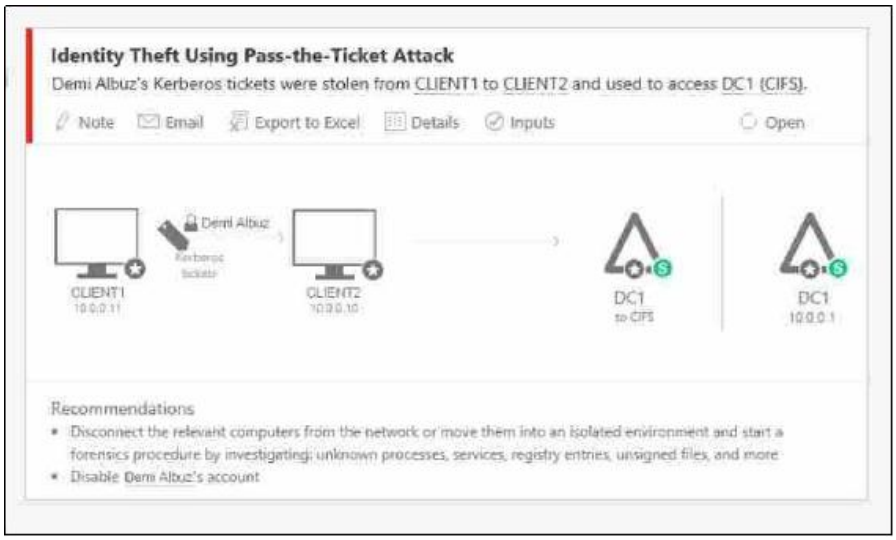
In entrambi i casi, quei server di elaborazione ATA ricevono tutti questi dati e iniziano a trovare modelli. Se Betty utilizza un computer desktop chiamato BETTY-PC e un tablet chiamato BETTY-TABLET, ATA vedrà quel modello e assocerà il suo account utente a quei dispositivi. Controlla anche i suoi normali schemi di traffico. Betty di solito accede intorno alle 8 del mattino e il suo traffico di solito si interrompe da qualche parte intorno alle 17:00. In genere accede ad alcuni file server ea un server SharePoint. Dopo circa una settimana di raccolta e monitoraggio dei dati, ATA ha un'idea abbastanza chiara del MO standard di Betty.

Adesso, una notte, succede qualcosa. ATA rileva una serie di errori di password sull'account di Betty. Questo di per sé potrebbe non essere qualcosa di cui entusiasmarsi, ma all'improvviso Betty accede a un server terminal a cui in genere non accede. Da lì, le sue credenziali vengono utilizzate per accedere a un controller di dominio. Uh oh, questo chiaramente suona come un attacco per me. Con gli strumenti integrati in

Active Directory che attualmente abbiamo a nostra disposizione, cosa sappiamo? Niente. Potremmo vedere errori di password se scaviamo nei registri degli eventi e, in base a ciò, potremmo provare a frugare nei registri degli eventi di altri server per scoprire a cosa accede quell'account, ma non avremmo davvero alcun motivo di sospettare nulla. Questo potrebbe essere l'inizio di una breccia molto grande e non lo vedremmo mai. Per fortuna,

L'interfaccia di gestione di ATA è come un feed di social media, aggiornato quasi in tempo reale. Durante gli eventi che ho appena esposto, se avessimo guardato il feed multimediale di ATA, avremmo visto tutti questi elementi, che ho sottolineato accadere, così come sono accaduti, e sarebbe immediatamente ovvio che qualcuno ha compromesso l'account di Betty e utilizzato per ottenere l'accesso a un controller di dominio. Non c'è mai stata una tecnologia che controlla il traffico di Active Directory così intensamente, e non c'è certamente mai stato nulla che apprenda schemi e deviazioni comportamentali come questo. È davvero una tecnologia straordinaria, e non lo dico solo perché mi capita di conoscere i ragazzi che l'hanno costruita. Ma visto che lo faccio, posso dirti che sono geniali, il che è già abbastanza ovvio da quando Microsoft li ha raccolti.

A questo punto, ATA è ancora abbastanza nuovo che la maggior parte della comunità IT non ha avuto alcuna interazione con esso e ti incoraggio vivamente a cambiarlo. Un giorno potrebbe salvarti la pancetta. Quello che segue è uno screenshot dell'interfaccia web di ATA in modo da poter ottenere una visuale su quel feed in stile social media. Questo screenshot è stato preso da una demo Microsoft in cui hanno rubato intenzionalmente il ticket Kerberos da un utente e poi lo hanno utilizzato su un altro computer per accedere ad alcuni file riservati a cui solo Demi Albuz avrebbe dovuto essere in grado di accedere. Sebbene ATA non abbia interrotto questa attività, è stato immediatamente, e intendo in pochi secondi, avvisato all'interno di questo feed per mostrare l'attacco pass-the-ticket:



Ecco un altro esempio in cui un utente di nome Almeta Whitfield accede improvvisamente a 16 computer a cui di solito non accede, un'altra grande bandiera rossa che qualcosa sta succedendo con il suo account utente:

Per ulteriori informazioni o per iniziare a utilizzare ATA, assicurati di controllare il seguente collegamento: https: //documenti.microsoft.com /en-noi/Avanzate-minaccia-analisi /che cosa-è -ata.

Best practice di sicurezza generali

A volte dobbiamo fare affidamento solo su noi stessi, e non necessariamente sulle funzionalità fornite dal sistema operativo, per proteggere i nostri sistemi. Ci sono molti approcci di buon senso all'amministrazione (se questa è una parola) che sono facili da realizzare ma sono usati raramente sul campo. Di seguito sono riportati alcuni suggerimenti e trucchi che ho imparato nel corso degli anni e che ho aiutato le aziende a implementare. Si spera che tu come lettore abbia ancora di più da aggiungere a questo elenco su ciò che funziona bene per te, ma se non altro questa sezione ha lo scopo di spingere il tuo pensiero a trovare modi creativi con cui limitare la capacità amministrativa e la vulnerabilità all'interno della tua rete .

Liberarsi degli amministratori perpetui

Tutto il personale IT dispone dei diritti di amministratore di dominio il giorno in cui viene assunto? Qualcuno del tuo personale IT ha accesso alla password dell'account amministratore di dominio incorporata? Hai utenti regolari i cui accessi hanno privilegi amministrativi sui propri computer? Sai dove sto andando con questo - queste sono tutte idee terribili!

Sfortunatamente, questo è stato lo status quo per molti anni in quasi tutte le reti e la tendenza continua ancora oggi. Continuo a osservare regolarmente i tecnici che utilizzano l'account di dominio dell'amministratore per molte attività quando configuriamo nuovi server. Ciò significa che non solo hanno accesso all'account potenzialmente più importante della tua rete e lo stanno utilizzando per le attività quotidiane, ma significa anche che qualsiasi cosa venga impostata con questo account utente non è responsabile. Cosa intendo dire? Quando imposto un nuovo server o apporto modifiche a un server esistente utilizzando l'account amministratore generale, e finisco per causare una sorta di grosso problema, nessuno può dimostrare che l'ho fatto. L'utilizzo di account utente generalizzati è un modo sicuro per contrastare la responsabilità nel caso in cui qualcosa vada storto. Non sto cercando di insinuare che tu sia sempre alla ricerca di chi l'ha fatto ?, ma se incasino qualcosa su un server delle applicazioni che normalmente non amministro, sarebbe bello se i ragazzi che cercano di risolverlo potessero facilmente capire che ero io e venissero a chiedermi cosa ho fatto in modo che possano invertirlo . Ci sono molte ragioni per cui l'utilizzo dell'account amministratore integrato dovrebbe essere vietato per tutti noi.

Per affrontare il lato client, i tuoi utenti hanno davvero bisogno di diritti amministrativi sui loro computer? Veramente? Penso che potresti probabilmente trovare dei modi per aggirarlo. Ridurre gli utenti normali ai diritti di utente o utente avanzato sui loro sistemi può avere un enorme impatto sulla sicurezza di quei computer. Dà ai virus un tempo molto più difficile installarsi da soli se l'utente deve eseguire un prompt che richiede i privilegi di amministratore prima di poter procedere con l'installazione. Mantiene inoltre tutte le vostre macchine in un modello comportamentale molto più coerente, senza che le applicazioni e le impostazioni nuove e sconosciute vengano introdotte dall'utente.

Utilizzo di account distinti per l'accesso amministrativo

Questa idea fa da traino all'ultima ed è qualcosa che ho iniziato a utilizzare anche su tutti i computer di casa che installo per amici e familiari. Si riduce davvero a questo: utilizza due diversi account utente. Uno con accesso amministrativo e uno senza. Quando sei connesso per attività e faccende quotidiane, assicurati di aver effettuato l'accesso con il tuo account utente normale che non dispone di privilegi amministrativi, né sul computer locale né sul dominio. In questo modo, se tenti di installare qualcosa, o se qualcosa tenta di installarsi da solo, ti verrà richiesto dalla casella Controllo account utente (UAC), chiedendoti di inserire un nome utente e una password amministrativi prima che l'installatore possa fare qualsiasi cosa. Posso dirti che funziona poiché ho impedito a una serie di virus sul mio computer di installarsi da soli mentre navigo in Internet cercando di fare ricerche per un progetto o per un altro. Se ricevo un prompt UAC che mi chiede una password amministratore e non ho fatto clic su un file di installazione, so che è qualcosa che non voglio. Tutto quello che devo fare è fare clic su No e il programma di installazione non si impadronirà del mio computer. D'altra parte, se è qualcosa che intendo installare, è un piccolo inconveniente inserire semplicemente la password del mio account amministrativo e consentire al programma di installazione di continuare. Tutto quello che devo fare è fare clic su No e il programma di installazione non si impadronirà del mio computer. D'altra parte, se è qualcosa che intendo installare, è un piccolo inconveniente inserire semplicemente la password del mio account amministrativo e consentire al programma di installazione di continuare. Tutto quello che devo fare è fare clic su No e il programma di installazione non si impadronirà del mio computer. D'altra parte, se è qualcosa che intendo installare, è un piccolo inconveniente inserire semplicemente la password del mio account amministrativo e consentire al programma di installazione di continuare.

Mantenere due account separati ti consente di affrontare la maggior parte delle attività quotidiane mettendo a tuo agio il fatto che non hai il diritto di fare inavvertitamente qualcosa di male al tuo sistema. Questa mentalità limita anche la quantità di attività che qualsiasi account amministrativo deve svolgere su un computer o in rete e rende più facile tenere traccia di tali account amministrativi quando gli amministratori apportano modifiche nell'ambiente.

Utilizzo di un computer diverso per eseguire attività amministrative

Se si desidera progredire ulteriormente nell'idea di account utente separati, è possibile rendere la propria esperienza di elaborazione ancora più sicura utilizzando un computer completamente separato quando si eseguono attività a livello amministrativo. Un computer per le normali attività di knowledge worker e un altro computer per l'amministrazione. Ciò contribuirebbe sicuramente a mantenere sicuro il tuo sistema amministrativo, così come i sistemi remoti a cui ha accesso. E anche se sembra complicato avere due computer fisici alla tua scrivania, ricorda che con la maggior parte degli SKU in Windows 10 abbiamo la possibilità di eseguire Hyper-V direttamente sui nostri computer desktop. In realtà lo faccio esattamente con il mio computer. Ho il mio computer che esegue Windows 10, e poi all'interno di quel computer sto eseguendo una macchina virtuale tramite Hyper-V da cui eseguo tutte le attività amministrative sui server sensibili. In questo modo un compromesso del mio sistema operativo quotidiano non richiede un compromesso dell'intero ambiente.

Sia che tu scelga di suddividere l'accesso amministrativo a livello di account utente oa livello di computer, ricorda questa semplice regola: non amministrare mai Active Directory dallo stesso posto in cui navighi su Facebook. Penso che questo riassuma abbastanza bene questo.

Non navigare mai in Internet dai server

Sembra un gioco da ragazzi, ma lo fanno tutti. Passiamo tutto il giorno a lavorare sui server e molto spesso dobbiamo raggiungere e controllare qualcosa da un browser web. Poiché Internet Explorer esiste sui server Windows, a volte è più semplice e veloce controllare qualunque cosa sia necessario controllare dalla console del server su cui stiamo lavorando, piuttosto che tornare alla nostra scrivania. Resisti alla tentazione! È così facile rilevare cose brutte da Internet, specialmente sui server perché se qualche macchina nella nostra rete funziona senza protezione antivirus, probabilmente è sul lato server. Lo stesso vale per i filtri Internet. Ci assicuriamo sempre che il traffico del client passi attraverso il nostro proxy aziendale (se ne abbiamo uno), ma non ci interessa sempre se il traffico del server si sposta o meno verso l'esterno nello stesso modo.

Non farlo nemmeno per i siti Web di cui ti fidi. Un attacco man-in-the-middle o una compromissione del sito Web stesso possono facilmente danneggiare il tuo server. È molto più facile ricostruire un computer client che non un server.

Controllo degli accessi basato sui ruoli (RBAC)

La frase Controllo di accesso basato sui ruoli (RBAC) non è limitata agli ambienti Microsoft. Inoltre, non è una tecnologia particolare che può essere utilizzata all'interno di Windows Server 2019, ma piuttosto è un'ideologia incentrata sulla separazione dei ruoli e delle mansioni lavorative. Quando pensiamo di separare i ruoli lavorativi dei nostri dipendenti da una prospettiva IT, tradizionalmente pensiamo in termini di gruppi di Active Directory. Sebbene l'aggiunta di account utente ai gruppi risolva molti problemi relativi alla suddivisione dei livelli di autorizzazioni e accesso, può essere complicato crescere in questa mentalità e, in definitiva, i gruppi AD consentono ancora agli amministratori di avere pieno accesso ai gruppi stessi. Le tecnologie RBAC dividono i ruoli a un livello diverso, occupandosi di più delle autorizzazioni. RBAC si concentra più sulle descrizioni delle mansioni dei dipendenti che sulle restrizioni di accesso.

Just Enough Administration (JEA)

Un ottimo esempio di una tecnologia RBAC inclusa in Windows Server 2019 è Just Enough Administration (JEA), che fa parte di PowerShell. JEA fornisce un modo per garantire un accesso privilegiato speciale per le persone, senza la necessità di concedere loro diritti amministrativi, che sarebbero stati necessari per svolgere gli stessi compiti in passato. La necessità di aggiungere qualcuno al gruppo di amministratori su un server in modo che possano svolgere il proprio lavoro è abbastanza comune, ma JEA è un primo passo per allontanarsi da tale necessità.

Nel nostro vecchio modo di pensare, potrebbe essere facile pensare a JEA come a qualcosa come consentire agli utenti di avere accesso amministrativo all'interno di PowerShell anche quando non hanno accesso amministrativo al sistema operativo stesso, ma è ancora più potente di così. Il design di JEA è tale da consentire agli utenti di avere accesso solo per eseguire determinati comandi e cmdlet di PowerShell a livello amministrativo, lasciando gli altri comandi a cui non devono accedere nell'oscurità.

Infatti, se un utente sta lavorando in un contesto JEA di PowerShell e tenta di richiamare un cmdlet che non fa parte dei cmdlet consentiti, PowerShell finge di non riconoscere nemmeno quel cmdlet. Non dice, scusa, non puoi farlo - ignora semplicemente il comando! Questo sicuramente aiuta a tenere le dita indiscreti fuori dal barattolo dei biscotti, a meno che tu non voglia lasciarle entrare.

Facciamo un ulteriore passo avanti. Forse sei un amministratore DNS e potrebbe essere necessario riavviare occasionalmente i servizi DNS. Dal momento che stiamo adottando la mentalità JEA / RBAC, non avrai diritti amministrativi sul sistema operativo di quel server DNS, ma avrai diritti basati su JEA all'interno di PowerShell in modo da poter eseguire gli strumenti di cui hai bisogno per farlo il vostro lavoro. Il riavvio del servizio DNS richiede l'accesso per utilizzare il cmdlet Restart-Service, giusto? Ma questo non significa che sarei in grado di riavviare qualsiasi servizio su quel server e potrei potenzialmente fare ogni sorta di cose che non ho bisogno di fare? JEA è anche abbastanza potente per affrontare questo scenario. Quando si imposta il livello di accesso che l'utente deve ottenere, è anche possibile immergersi in particolari cmdlet e suddividere le autorizzazioni. Nel nostro esempio, è possibile fornire all'utente l'accesso al cmdlet Restart-Service, ma concedere solo le autorizzazioni per riavviare servizi particolari, come quelli relativi al DNS. Se l'utente tentasse di riavviare il servizio su WINrm, verrebbe negato.

Sommario

Il punto all'ordine del giorno numero uno per molti CIO quest'anno è la sicurezza. Sicurezza per le tue macchine client, sicurezza per le tue reti, sicurezza per le tue risorse cloud e, soprattutto, sicurezza per i tuoi dati. Non esiste un'unica soluzione per proteggere la tua infrastruttura, richiede molte parti mobili e molte tecnologie diverse che lavorano insieme per garantire la sicurezza delle tue risorse. Lo scopo di questo capitolo era fornire esempi di misure e tecnologie di sicurezza che possono essere utilizzate negli ambienti di chiunque, nonché ridefinire l'importanza che la sicurezza ha nel mondo IT di oggi. Le preoccupazioni relative alla privacy e alla sicurezza devono essere discusse per ogni soluzione tecnologica che mettiamo in atto. Troppe volte trovo che nuove applicazioni vengano implementate all'interno delle organizzazioni senza alcun riguardo per quanto sia sicura quella piattaforma applicativa. Le applicazioni che trasmettono o archiviano dati non crittografati devono essere modificate o scaricate. La protezione delle informazioni è essenziale per la longevità delle nostre attività.

Non possiamo completare una discussione sulla sicurezza in Windows Server 2019 senza discutere l'opzione di installazione del sistema operativo predefinita che abbiamo finora ignorato in questo libro. Voltiamo pagina e tuffiamoci in Server Core, la nostra versione headless e meno vulnerabile di Windows Server.

Domande

1. Qual è il nome del prodotto anti-malware integrato in Windows Server 2019?
2. Quando un computer aggiunto a un dominio si trova all'interno della LAN aziendale, quale profilo di Windows Defender Firewall deve essere attivo?
3. Oltre al profilo di dominio, quali sono gli altri due possibili profili firewall all'interno di Windows Defender Firewall?
4. Quando si crea una regola firewall per consentire risposte ping IPv4, quale tipo di protocollo è necessario specificare all'interno della regola in entrata?
5. Qual è il modo più semplice per inviare regole standardizzate di Windows Defender Firewall a tutta la tua forza lavoro?
6. Una macchina virtuale il cui file del disco rigido virtuale è crittografato è chiamata ...?
7. Qual è il nome della tecnologia Microsoft che analizza le informazioni del controller di dominio per identificare gli attacchi pass-the-hash e pass-the-ticket?

Server Core

Tesoro, ho ridotto il server! Un altro capitolo, un altro riferimento al film obsoleto. Negli ultimi 20 anni circa, non abbiamo visto altro che una crescita dei sistemi operativi Microsoft. La crescita può essere buona; nuove funzionalità e miglioramenti semplificano la nostra vita.
La crescita può anche essere negativa, come strutture di file gonfie e interfacce grafiche che divorano la memoria. Se dovessi rappresentare cronologicamente i sistemi operativi Windows e Windows Server in termini di footprint, in base a fattori come il consumo di spazio su disco e i requisiti di memoria, mostrerebbe una costante pendenza verso l'alto. Ogni nuova versione richiede solo un po 'più di potenza di elaborazione e solo un po' più di spazio sul disco rigido rispetto alla versione precedente. Questo è stato il caso fino a quando, immagino un po 'di stima qui, forse Windows 8 e Server 2012. Abbiamo visto alcuni passaggi sorprendenti compiuti con l'abbassamento di questi numeri di soglia, un cambiamento positivo. Ma il cambiamento non è stato troppo drammatico. Voglio dire,

cosa puoi trarre dal fatto che una nuova scatola di Windows Server 2019 contiene tutti i tipi di elementi principali ancora in esecuzione in C: \ Windows \ System32? Noi' Non parlerai nemmeno di cosa c'è nel registro. Chiaramente, ci sono ancora tagli che potrebbero essere fatti e, a un certo livello, nuovi sistemi operativi sono ancora in fase di costruzione e patch su quelli vecchi.

Fino ad ora, forse. Qui parleremo di un modo alternativo per utilizzare Windows Server 2019 su una scala molto, molto più piccola. Server Core è in circolazione da un po 'di tempo ormai, ma mi è difficile trovare persone che lo utilizzino effettivamente. Questa versione miniaturizzata di Server 2019 è stata creata per fornire una piattaforma server più piccola, più efficiente e più sicura.

n questo capitolo tratteremo i seguenti

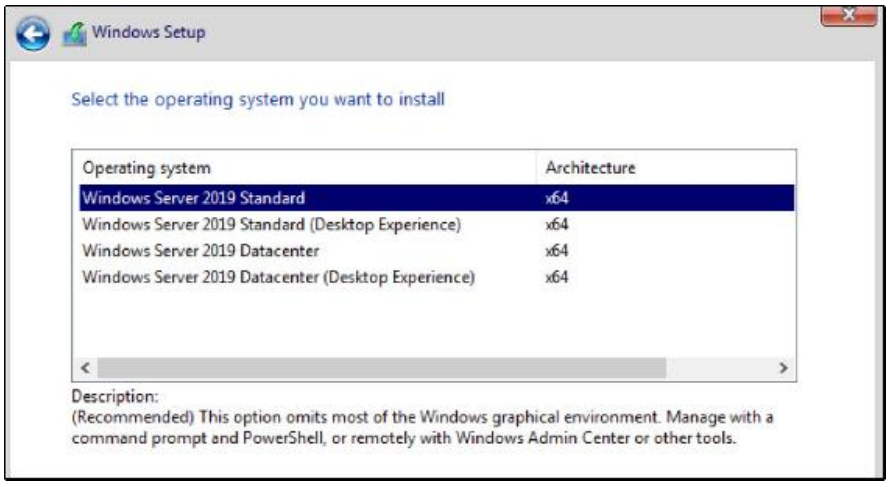
argomenti: Perché utilizzare Server Core?

- Interfacciamento con Server Core
- Windows Admin Center per la gestione di Server Core L'utilità Sconfig
- Ruoli disponibili in Server Core Cosa è successo a Nano Server?

Perché utilizzare Server Core?

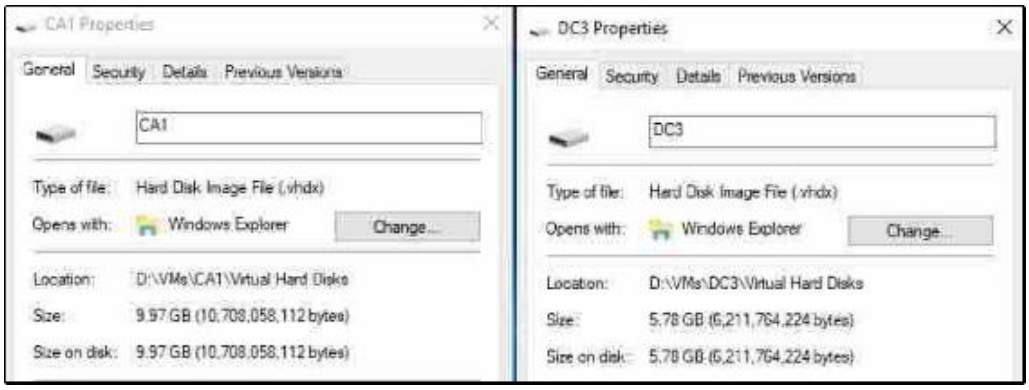
Perché parlo anche di Server Core? Non esiste dal 2008? Sì, è proprio per questo che ne parlo. La variante Server Core del sistema operativo Windows Server è in circolazione da un po 'di tempo, ma sembra che molti amministratori abbiano paura di fidarsi di essa. Lavoro con molte aziende diverse di molti settori diversi. Hanno tutti una grande cosa in comune: usano molti server Windows e tutti questi server Windows eseguono la GUI (esperienza desktop) completa. Hanno sentito parlare di Server Core? Sicuro. L'hanno testato in un laboratorio? A volte. Tutti sembrano avere un livello di esperienza leggermente diverso con Core, ma è abbastanza raro trovarne uno in produzione.
Forse sto solo parlando con le persone sbagliate, ma devo presumere che la maggior parte di noi là fuori, me compreso, ha bisogno di iniziare a utilizzare Server Core in modo più regolare.

Perché dobbiamo iniziare a utilizzare Server Core? Perché i server senza GUI sono il futuro, afferma Microsoft. Ci credereste che all'inizio delle anteprime per Windows Server 2016, l'opzione Esperienza desktop non esistesse nemmeno? Se lo si desidera, non è possibile eseguire una shell desktop con GUI completa su un Server 2016, ad eccezione di una quasi mini shell che potrebbe essere posizionata sopra Server Core. Microsoft ha ricevuto così tante critiche al riguardo che l'esperienza desktop completa è stata aggiunta di nuovo durante uno dei rollout dell'anteprima tecnica. Anche così, da quel momento, probabilmente avrai notato che Server Core è l'opzione predefinita durante l'installazione di qualsiasi sistema operativo Windows Server. Ricordi, all'inizio del nostro libro, dove abbiamo fatto una rapida revisione dell'effettiva installazione di Server 2019? L'opzione predefinita per l'installazione non è Esperienza desktop; piuttosto,


Windows Setup
Select the operating system you want to install
Operating system
Architecture
Windows Server 2019 Standard
x64
Windows Server 2019 Standard (Desktop Experience)
x64
Windows Server 2019 Datacenter
x64
Windows Server 2019 Datacenter (Desktop Experience)
x64
Description:
(Recommended) This option omits most of the Windows graphical environment. Manage with a command prompt and PowerShell, or remotely with Windows Admin Center or other tools.

Uno dei motivi per allontanarsi dall'interfaccia grafica è l'aumento delle capacità di automazione e scalabilità. Quando tutti i nostri server sono costruiti in modo simile, significa che possiamo eseguire più funzioni simili al cloud con loro. Rotazione automatica su e giù delle risorse quando sono necessarie, implementazione di dozzine di server con un clic di un interruttore: questo tipo di automazione e dimensionamento è possibile nel cloud, ma è possibile solo perché l'infrastruttura è configurata in modo tale è così standardizzato. Le risorse hardware del cloud devono essere così semplificate che le operazioni e gli strumenti di automazione possano far sì che facciano ciò che è necessario, senza doversi preoccupare di tutte le variabili che sarebbero presenti in un'interfaccia grafica ottimizzata dall'utente.

Ci sono altri ovvi vantaggi nell'esecuzione di tutti i tuoi server come questa versione limitata e limitata. Server Core vanta uno spazio su disco rigido ridotto, un consumo di memoria ridotto e una superficie di attacco ridotta rispetto a un'esperienza server tradizionale e completa.
Ora puoi capire perché un minuto fa ho fatto le dichiarazioni pesanti su come dobbiamo iniziare a diventare più a nostro agio con Server Core! In effetti, diamo un'occhiata a quell'impronta ridotta. Un Server 2019 Standard di base che esegue Desktop Experience consuma circa 10 GB di spazio su disco rigido; L'ho appena verificato dando un'occhiata alle proprietà del mio file del disco rigido virtuale utilizzato dal mio server CA1. CA1 è un Windows Server 2019 standard che esegue l'esperienza desktop completa. Ora, ho appena finito di eseguire l'installazione per il mio primo sistema operativo Server Core e possiamo vedere nello screenshot seguente che il file VHDX utilizzato da questa nuova macchina virtuale è di soli 5,8 GB, una riduzione dello spazio del 40%:


CA1 Properties
General
Security
Details
Previous Versions
CA1
Type of file: Hard Disk Image File (.vhdx)
Opens with: Windows Explorer
Change...
Location: D:\VMs\CA1\Virtual Hard Disks
Size: 9.97 GB (10,708,058,112 bytes)
Size on disk: 9.97 GB (10,708,058,112 bytes)
DC3 Properties
General
Security
Details
Previous Versions
DC3
Type of file: Hard Disk Image File (.vhdx)
Opens with: Windows Explorer
Change...
Location: D:\VMs\DC3\Virtual Hard Disks
Size: 5.78 GB (6,211,764,224 bytes)
Size on disk: 5.78 GB (6,211,764,224 bytes)

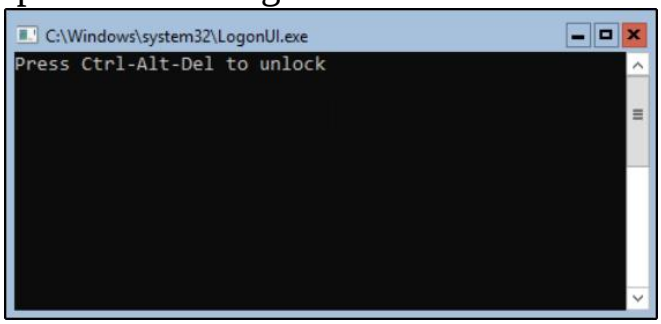
Non più passare avanti e indietro

C'è una nota molto importante che volevo fare qui: quelli di voi che hanno lavorato con Server Core in Windows Server 2012 R2 sanno che avevamo la possibilità di cambiare un server al volo. Quello che voglio dire è che se hai creato un nuovo server come esperienza desktop completa, potresti successivamente cambiarlo in Server Core. L'approccio opposto era ugualmente possibile; potresti prendere un Server Core e capovolgerlo in un'esperienza desktop completa.

Non più! Questa capacità di spostare i server avanti e indietro tra le piattaforme è stata rimossa. Ripeto, questo non è più possibile. Quindi pianifica attentamente da qui in avanti quando installi questi sistemi operativi. Se implementi un server come Server Core, quel ragazzo rimarrà un Server Core per tutta la sua vita.

Interfacciamento con Server Core

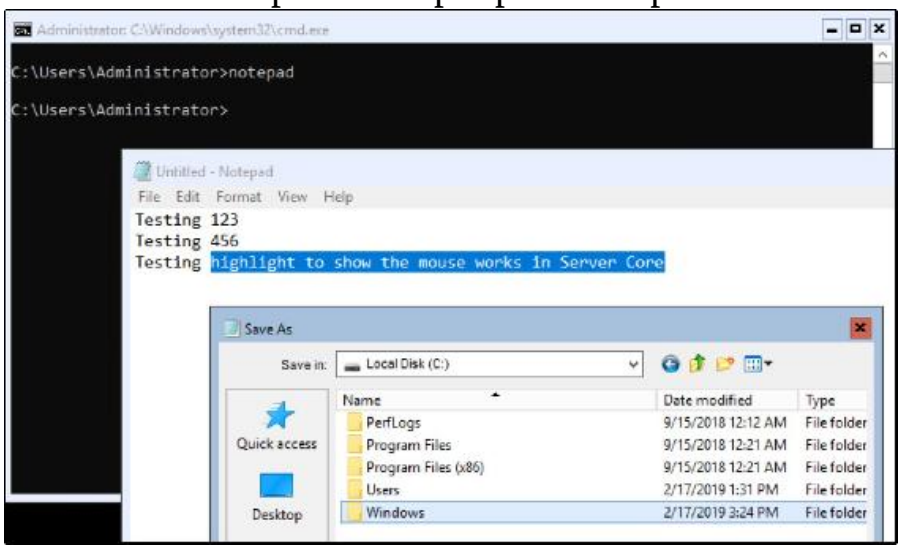
Dopo aver eseguito la prima installazione di Server Core, ti verrà presentata la seguente schermata di blocco:



È davvero una finestra del prompt dei comandi che dice Premi Ctrl-Alt-Canc per sbloccare? Si si lo è. Questo di solito fa qualche risatina quando un amministratore lo vede per la prima volta. So che ha funzionato per me, comunque. Mi ha ricordato un po 'di quando codificavamo i giochi if / then sulle nostre calcolatrici TI-83 durante le lezioni di matematica delle scuole superiori. Premi Ctrl + Alt + Canc e ti verrà chiesto di cambiare la tua password di amministratore per la prima volta, che è la stessa attività che deve essere sempre eseguita per prima nelle versioni GUI di Windows Server. Tranne, ovviamente, che fai tutto dalla finestra del prompt dei comandi usando solo la tastiera. Una volta effettuato l'accesso ufficiale al server, ti ritroverai seduto al tradizionale prompt C: \ Windows \ system32 \ cmd.exe, con un cursore lampeggiante in attesa di istruzioni:

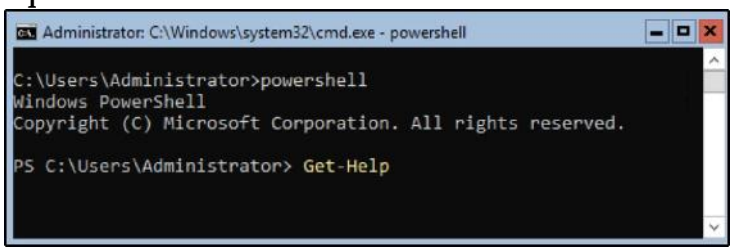
È interessante notare che la finestra del prompt dei comandi non utilizza lo schermo intero; è chiaro che c'è uno sfondo nero su cui sta cavalcando cmd.exe. Lo trovo interessante solo perché puoi dire che il sistema operativo Core stesso è qualcosa di diverso dal prompt dei comandi e che cmd.exe è solo un'applicazione che si avvia automaticamente all'accesso. Puoi anche utilizzare il mouse qui e ridimensionare o spostare la finestra del prompt dei comandi. Mi chiedo se e quando verrà sostituito con un prompt di PowerShell come interfaccia predefinita.

Ancora più interessante e buono a sapersi è che puoi avviare alcune applicazioni simili a GUI da questo prompt. Ad esempio, puoi aprire Blocco note e utilizzarlo sia con la tastiera che con il mouse, proprio come faresti con qualsiasi versione di Windows. Se hai il Blocco note aperto, crea una nota e poi salvala; puoi vedere che esiste in effetti una struttura di file reale e un insieme di cartelle di sistema dall'aspetto relativamente normale. Quindi, piuttosto che una qualche forma di magia nera, Server Core è in realtà il vero sistema operativo Windows Server, racchiuso in un pacchetto più piccolo e più sicuro:



PowerShell

Quindi, per quanto riguarda la gestione di un Server Core, puoi ovviamente lavorare direttamente dalla console e utilizzare il prompt dei comandi, che sembra essere l'interfaccia predefinita presentata dal sistema operativo. In realtà, però, i comandi e le funzioni disponibili all'interno del prompt dei comandi saranno limitati. Se stai lavorando dalla console di una scatola di Windows Server Core, ha molto più senso usare il prompt dei comandi per un solo scopo: richiamare PowerShell e quindi usarlo per eseguire tutte le attività che devi fare su quel server.
Il modo più rapido che conosco per passare a PowerShell dal prompt dei comandi di base è semplicemente digitare il powershell e premere Invio. Ciò porterà le funzionalità di PowerShell direttamente nella finestra del prompt dei comandi esistente, in modo da poter iniziare a interfacciarsi con i comandi ei cmdlet di PowerShell necessari per manipolare davvero questo server:



Qual è la prima cosa che di solito facciamo sui nuovi server? Dare loro gli indirizzi IP, ovviamente. Senza connettività di rete, non c'è molto che possiamo fare su questo server. Puoi assegnare le informazioni sull'indirizzo IP alle schede NIC utilizzando PowerShell su qualsiasi Windows Server più recente, ma la maggior parte di noi non ha l'abitudine di farlo. Dal momento che non possiamo semplicemente aprire il Pannello di controllo e accedere al Centro connessioni di rete e condivisione come possiamo dall'interno della GUI di Desktop Experience di Windows Server, da dove iniziamo con la connettività di rete su questo nuovo Server Core?

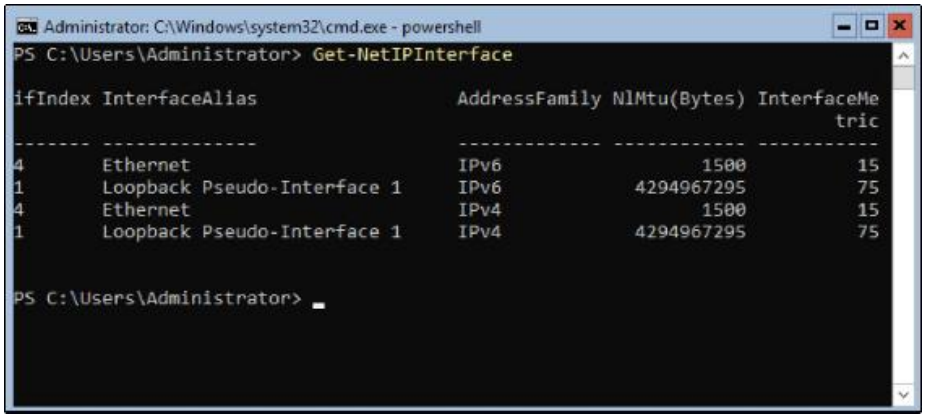
Utilizzo dei cmdlet per gestire gli indirizzi IP

Di seguito sono riportati i cmdlet che è possibile utilizzare per visualizzare e modificare le impostazioni dell'indirizzo IP da PowerShell. Anche in questo caso, questi stessi cmdlet possono essere usati nella versione GUI completa di Windows Server o da Server Core.

Attualmente, lavorando da Server Core in cui abbiamo a disposizione solo l'interfaccia della riga di comando, questi cmdlet sono essenziali per ottenere la connettività di rete che scorre sul nostro nuovo server:

- Get-NetIPConfiguration : Visualizza la configurazione di rete corrente.
- Get-NetIPAddress : Visualizza gli indirizzi IP correnti.
- Get-NetIPInterface: mostra un elenco di NIC e dei loro numeri ID di interfaccia. Questo numero sar à importante quando si imposta un indirizzo IP, perch é vogliamo essere sicuri di dire a PowerShell di configurare l'IP corretto sulla scheda NIC corretta.
- New-NetIPAddress : Viene utilizzato per configurare un nuovo indirizzo IP.
- Set-DNSClientServerAddress : Viene utilizzato per configurare le impostazioni del server DNS nelle proprietà NIC.

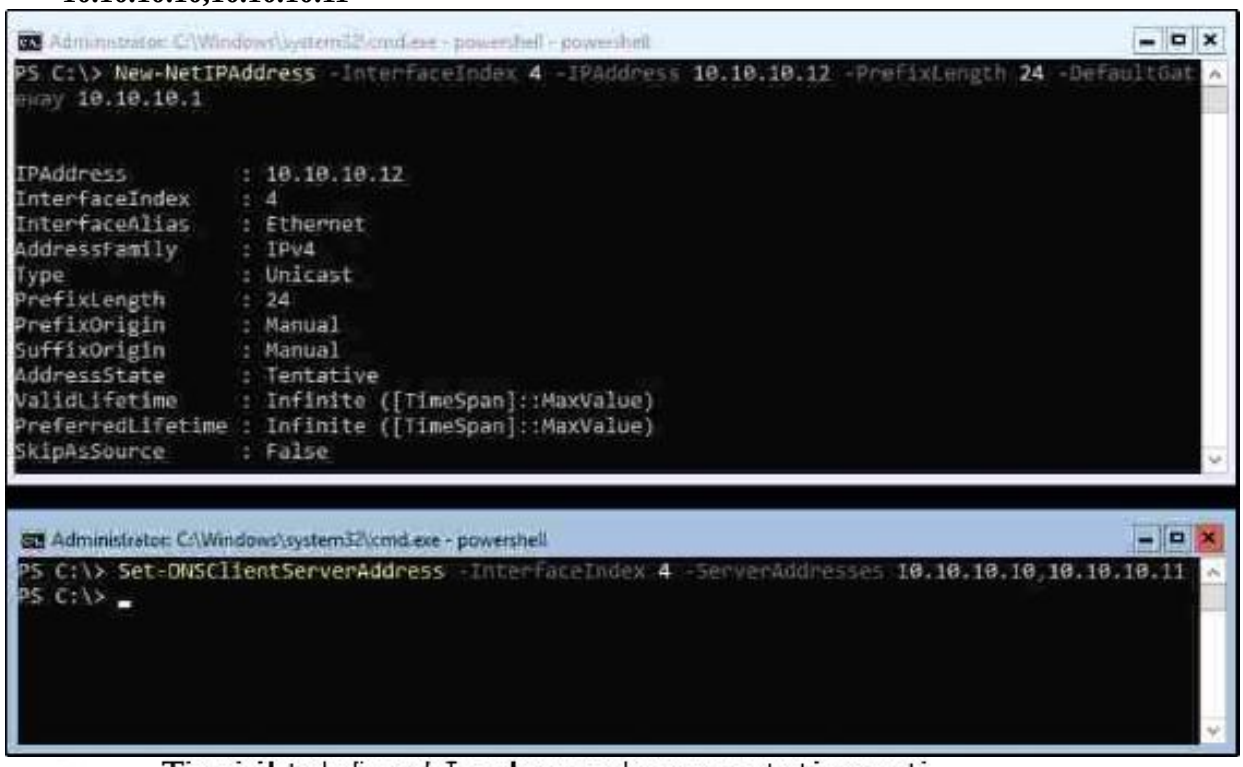
Passiamo rapidamente alla configurazione di un indirizzo IP statico su una nuova istanza di Server Core per assicurarci che tutto abbia senso. Voglio assegnare l'indirizzo IP 10.10.10.12 a questo nuovo server, ma prima dobbiamo scoprire a quale numero ID dell'interfaccia NIC deve essere assegnato. L'output di Get-NetIPInterface ci dice che l'ifIndex che mi interessa è il numero 4:



Ora che conosciamo il numero dell'interfaccia, creiamo i comandi che assegneranno le nuove impostazioni dell'indirizzo IP alla NIC. Userò un comando per assegnare l'indirizzo IP, il prefisso della subnet mask e il gateway predefinito. Userò un secondo comando per assegnare gli indirizzi del server DNS:

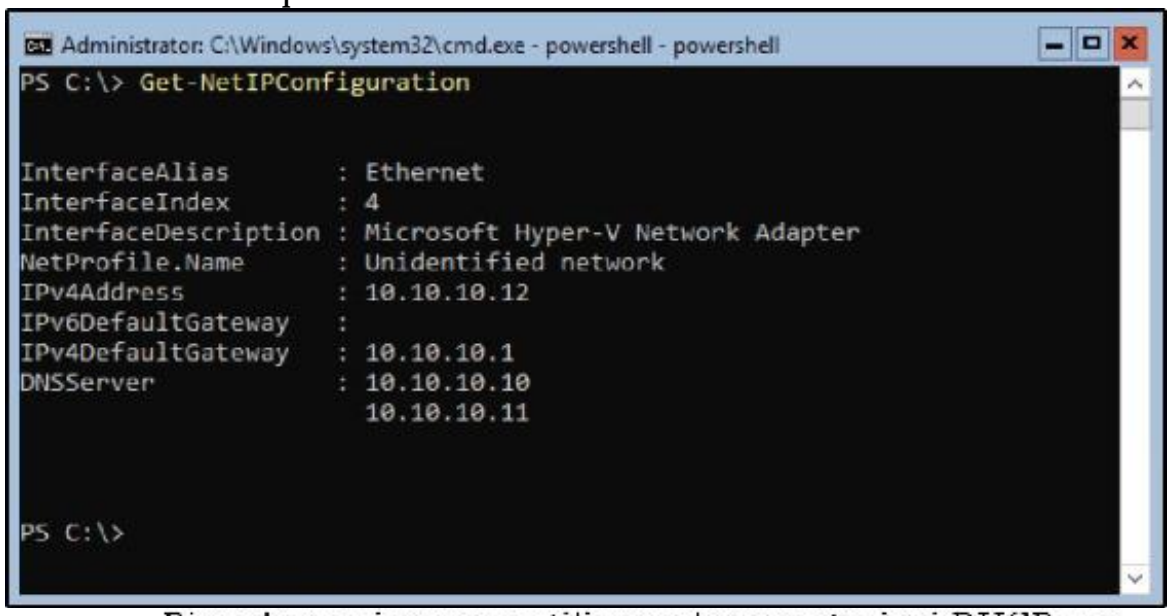
New-NetIPAddress -InterfaceIndex 4 -IPAddress 10.10.10.12 -PrefixLength 24 -DefaultGateway 10.10.10.1

Set-DNSClientServerAddress -InterfaceIndex 4 -ServerAddresses 10.10.10.10,10.10.10.11



Tieni il telefono! In che modo sono stati aperti contemporaneamente due prompt di PowerShell nell'interfaccia Server Core? Assicurati di leggere la sezione Chiusura accidentale del prompt dei comandi più avanti in questo capitolo per scoprire come avviare più finestre e

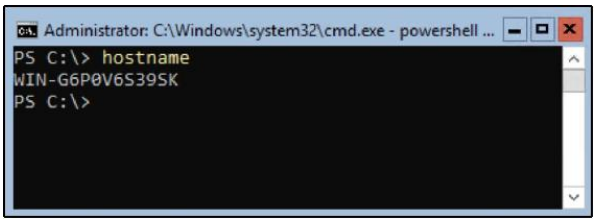
Ora tutte queste impostazioni IP dovrebbero essere presenti sulla scheda NIC. Controlliamolo due volte con un comando Get-NetIPConfiguration, visto nello screenshot seguente. In alternativa, potresti usare il buon vecchio ipconfig per controllare queste impostazioni, ma dov'è il divertimento in questo?



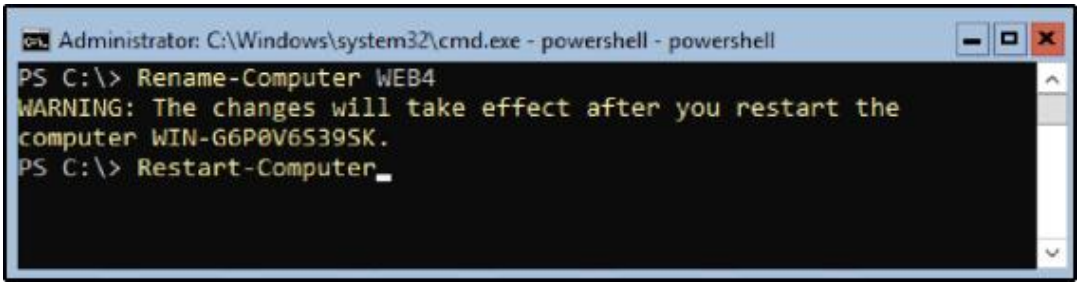
Ricorda, puoi sempre utilizzare le prenotazioni DHCP per renderlo un po 'più semplice. Se dovessi eseguire un semplice filcipconfig / all dal tuo server Core e annota l'indirizzo MAC della tua NIC, puoi usare questo indirizzo per creare una prenotazione in DHCP e assegnare un indirizzo IP specifico al nuovo server in questo modo.

Impostazione del nome host del server

Ora che abbiamo la connettività di rete, un buon passo successivo è impostare il nome host del nostro server e unirlo al dominio. Per prima cosa, vediamo qual è il nome corrente del server e cambiamolo in qualcosa che si adatti ai nostri standard. Quando installi di recente Windows, assegna automaticamente un nome host casuale al server. È possibile visualizzare il nome host corrente semplicemente digitando hostname e premendo Invio:


Administrator: C:\Windows\system32\cmd.exe - powershell ...
PS C:\> hostname
WIN-G6P0V6S39SK
PS C:\>

Per cambiare il nome host del tuo server, dobbiamo usare PowerShell. Passa a un prompt di PowerShell se non è già presente e tutto ciò che dobbiamo fare è utilizzare il cmdlet Rename-Computer per impostare il nostro nuovo nome host. Ho deciso di chiamare il mio nuovo server WEB4, perché in seguito installeremo il ruolo Web Services su di esso e ospiteremo un sito web. Ricorda, dopo aver rinominato il tuo computer proprio come nella versione GUI di Windows Server, è necessario un riavvio del sistema per mettere in atto la modifica. Quindi, seguendo il comando Rename-Computer, puoi emettere un Restart-Computer per riavviare la scatola:

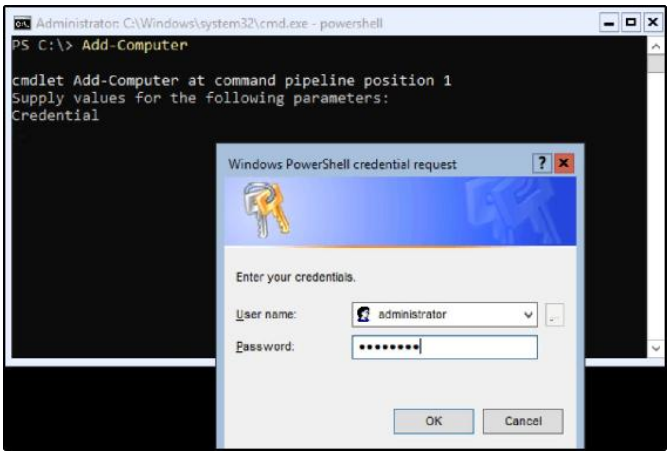


Rinomina computer WEB4

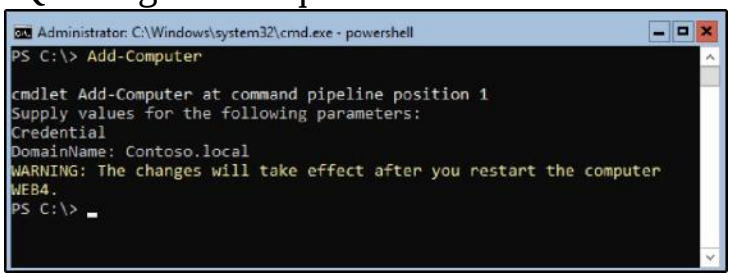
Riavvia computer

Entrare a far parte del tuo dominio

Il passaggio logico successivo è, ovviamente, entrare a far parte del tuo dominio. Queste sono le funzioni standard che eseguiremmo su qualsiasi nuovo server nel nostro ambiente, ma in un modo che potresti non aver mai incontrato prima, dal momento che stiamo facendo tutto questo rigorosamente dal prompt dei comandi e dalle interfacce di PowerShell. Per aggiungere un Server Core al tuo dominio, accedi a PowerShell e quindi usa il cmdlet Add-Computer. Ti verrà chiesto di specificare sia il nome di dominio che le tue credenziali per l'adesione al dominio, le stesse informazioni che dovresti specificare se ti unissi a un Windows Server 2019 in modalità Esperienza desktop a un dominio. Innanzitutto, è necessario specificare le credenziali necessarie per eseguire questa aggiunta al dominio:



Quindi gli dici a quale dominio vorresti unirti:



In alternativa, è possibile utilizzare il parametro -DomainName in combinazione con il cmdlet Add-Computer originale per specificare il nome del dominio come parte del comando originale. E, naturalmente, dopo esserti unito al dominio, devi riavviare il computer ancora una volta per finalizzare questa modifica.

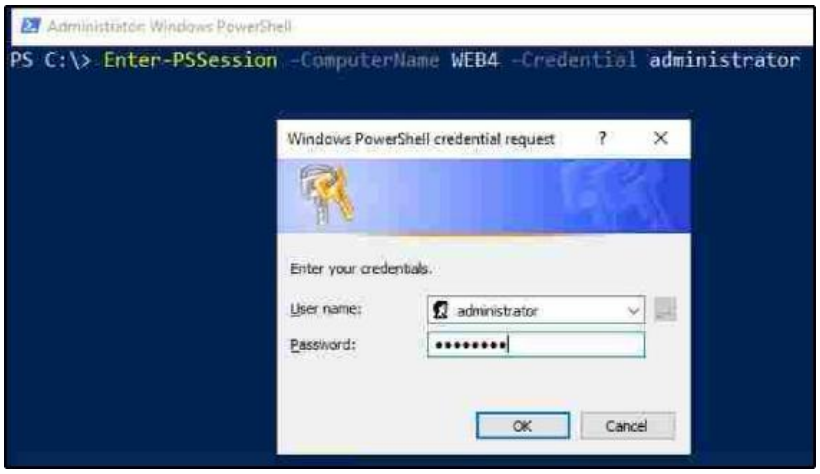
PowerShell remoto

Una volta che il nuovo server è indirizzato, denominato e aggiunto a un dominio, possiamo iniziare a fare una vera amministrazione su questa nuova istanza di Server Core. Potresti sicuramente continuare ad accedere e interfacciarti direttamente con la console, ma come con la gestione di qualsiasi altro server nel tuo ambiente, ci devono essere modi per gestirlo da remoto, giusto? Uno dei modi in cui è possibile manipolare Server Core senza doversi sedere di fronte è usare una connessione PowerShell remota.

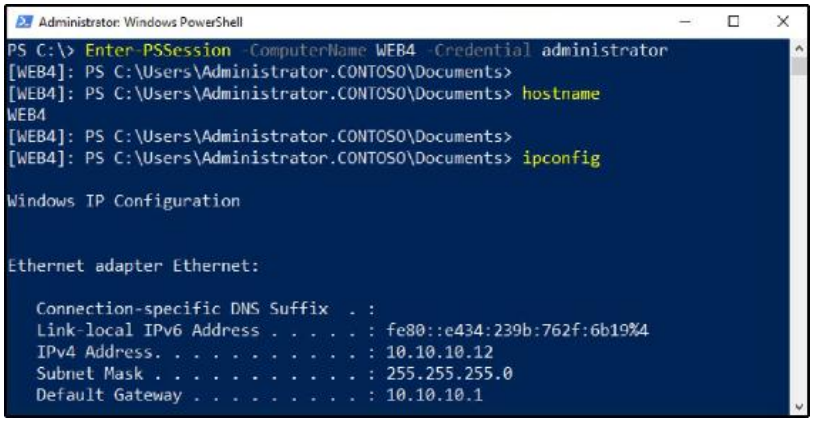
Tratteremo il processo per l'utilizzo di PowerShell remoto per manipolare i server (sia GUI che headless) in modo più dettagliato in Capitolo 10, PowerShell, ma ecco un assaggio dei comandi necessari e delle funzionalità presenti quando si è in grado di ottenere una sessione remota da un prompt di PowerShell su una workstation all'interno di un ambiente aggiunto a un dominio.

Apri PowerShell da un altro sistema: può essere un server o persino un sistema operativo client. Questa finestra di PowerShell è ovviamente aperta nel contesto di qualsiasi macchina a cui sei attualmente connesso e qualsiasi comando emesso tramite PowerShell darà una risposta illecita dal sistema locale. Per inserire PowerShell nell'istanza WEB4 Server Core, emetterò il seguente comando. Dopo aver eseguito questo, mi viene richiesta una password corrispondente all'account amministratore, quindi sarò in grado di emettere comandi PowerShell remoti contro il nostro Server Core:

Enter-PSSession -ComputerName WEB4 -Amministratore delle credenziali


Administrator: Windows PowerShell
PS C:\> Enter-PSSession -ComputerName WEB4 -Credential administrator
Windows PowerShell credential request
Enter your credentials.
User name:
administrator
Password:
OK
Cancel

Adesso siamo seduti al prompt di PowerShell, connesso in remoto al box WEB4 Server Core. Puoi vederlo dall'elenco (WEB4) a sinistra del nostro prompt. Forse non ti fidi di quel piccolo identificatore e vuoi assicurarti che questa finestra di PowerShell stia ora accedendo e manipolando il server WEB4 remoto? Emettiamo un paio di comandi rapidi, come hostname e ipconfig, per dimostrare che le informazioni che ci vengono fornite in questa sessione di PowerShell provengono davvero dal nuovo server WEB4:



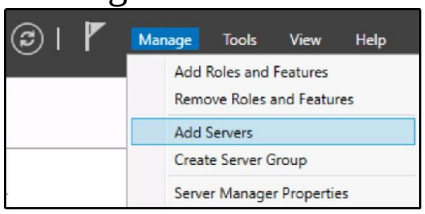
Ora che abbiamo una connessione PowerShell remota a questo nuovo Server Core, possiamo fare praticamente tutto ciò che vogliamo a quel server, direttamente da questa console.

Server Manager

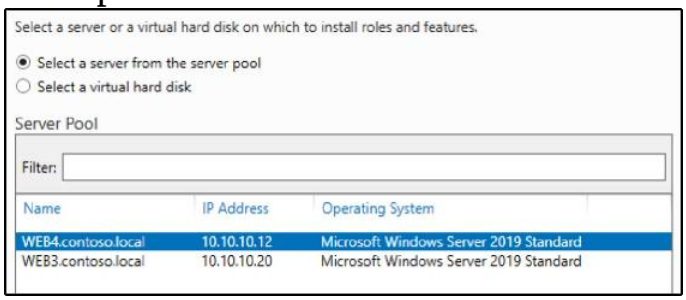
Mentre la configurazione iniziale del tuo server sarà in qualche modo gestita dalle interfacce della riga di comando disponibili sulla console, una volta che il tuo server è stato stabilito sulla rete, sarà probabilmente più vantaggioso per te espandere un po 'i tuoi orizzonti. Probabilmente potresti trovare cmdlet di PowerShell che ti consentono di gestire e manipolare qualsiasi cosa nel tuo nuovo server, ma questa è ancora una mentalità piuttosto nuova per la maggior parte di noi: siamo generalmente più abituati a utilizzare strumenti grafici come Server Manager. Tu già
sappi che Server Manager può essere utilizzato per gestire più server, locali e remoti, ed è un pezzo del puzzle della gestione centralizzata di

Microsoft. Questa funzionalità di gestione remota in Server Manager che abbiamo esplorato in precedenza nel libro consente di attingere non solo ai server Windows basati su GUI, ma anche alle istanze Server Core.

Voglio installare un ruolo nel mio nuovo server WEB4. Potrei farlo con PowerShell direttamente sulla console del server, ma invece proviamo ad aggiungere WEB4 in Server Manager che è in esecuzione su un altro dei miei server. Accedo a WEB3 e da lì utilizzo Server Manager. Proprio come abbiamo già visto, posso aggiungere un nuovo server in Server Manager utilizzando il menu Gestisci e scegliendo Aggiungi server:



Aggiungi il nuovo Il server WEB4 nel nostro elenco di macchine gestite ed è ora gestibile dall'interno di questa istanza di Server Manager. Tornando alle mie intenzioni originali, voglio installare il ruolo di Web Server (IIS) su WEB4. Se utilizzo la funzione Aggiungi ruoli e funzionalit à all'interno di Server Manager, ora posso scegliere di manipolare il server WEB4:

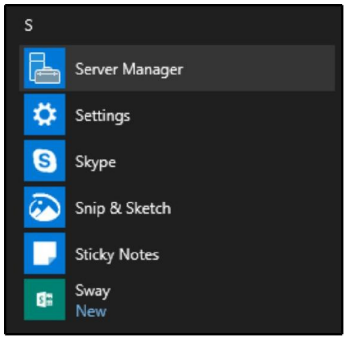


Proprio come con qualsiasi server che esegue la versione completa dell'esperienza desktop di Windows Server, ora possiamo completare la procedura guidata di installazione del ruolo e il ruolo del server Web verrà installato su WEB4.

Strumenti di amministrazione remota del server

È anche vero il fatto che è possibile gestire le istanze Server Core con gli strumenti di amministrazione remota del server (RSAT) in Windows 10. RSAT è essenzialmente solo una copia di Server Manager progettata per essere eseguita sul sistema operativo client. Nel nostro caso, ho già una macchina Windows 10 su cui ho installato RSAT in precedenza nel libro, quindi proverò accedendo a quel ragazzo e aggiungendo WEB4 all'interfaccia. Ho appena finito di installare il ruolo IIS su WEB4 nella nostra attività precedente, quindi dovrei essere in grado di vedere quello elencato all'interno di RSAT quando lo collego a WEB4.

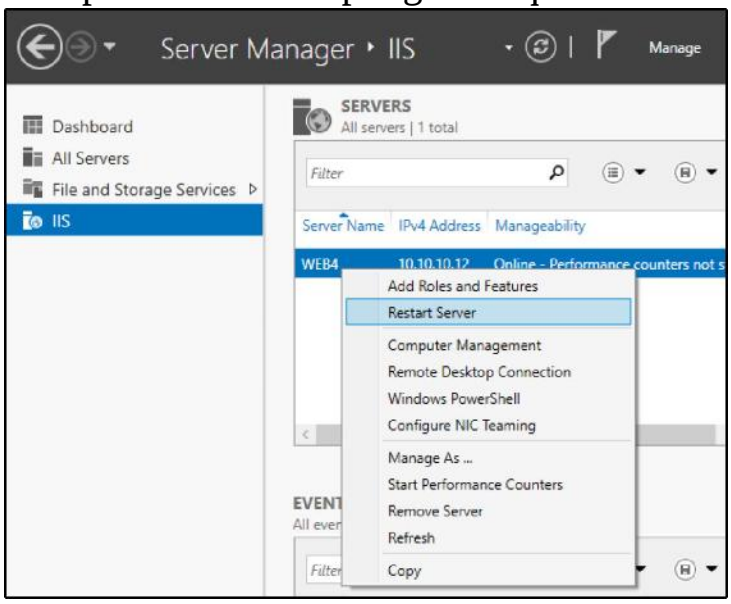
Se non hai mai utilizzato RSAT prima e non hai letto quella sezione del nostro testo, è importante sapere che non esiste un'applicazione chiamata Strumenti di amministrazione remota del server. Invece, dopo che l'installazione di RSAT è stata completata, dai un'occhiata all'interno del menu Start per l'applicazione chiamata Server Manager. Ecco come utilizzi un client Windows 10 per gestire in remoto le istanze di Windows Server 2019:



Esattamente come faresti da un'interfaccia Server Manager di Windows Server 2019, vai avanti e segui la procedura guidata per aggiungere altri server da gestire. Dopo aver aggiunto WEB4 come server gestito nel Server Manager di Win10, posso vedere IIS elencato nel mio dashboard. Ciò indica che il mio servizio IIS in esecuzione su WEB4 è visibile, accessibile e configurabile direttamente dal mio computer desktop Windows 10. Per la maggior parte delle attività che devo

eseguire su WEB4, non dovrò mai preoccuparmi di accedere alla console di quel server.

Se Faccio clic con il pulsante destro del mouse sul nome del server WEB4 da questa console RSAT, puoi vedere che ho molte funzionalità disponibili che posso utilizzare per gestire questa istanza Server Core remota:



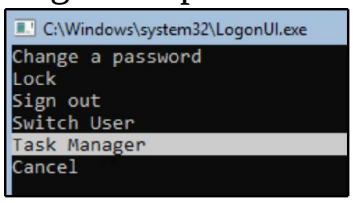
Quindi puoi vedere che ci sono modi per utilizzare gli strumenti della GUI per gestire le nostre istanze senza GUI di Windows Server. È solo questione di mettere la tua mente in un posto in cui pensi ai server come senza testa e che strumenti come PowerShell o Server Manager non si preoccupano affatto se il server che stanno cambiando è locale o remoto. I processi e gli strumenti sono gli stessi in entrambi i casi. Puoi vedere nello screenshot precedente che potrei anche fare clic da qui per avviare una connessione PowerShell remota a WEB4.
Facendo clic su questo pulsante si avvia immediatamente un prompt di PowerShell che è collegato in remoto al server WEB4, anche se al momento sono connesso solo alla mia workstation Windows 10. Ciò è ancora più semplice rispetto all'emissione del cmdlet Enter-PSSession dall'interno di PowerShell.

Chiusura accidentale del prompt dei comandi

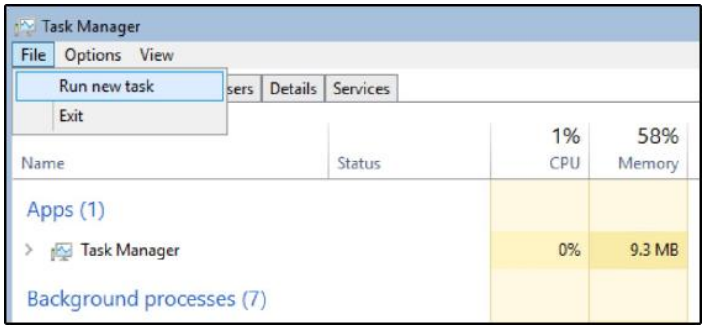
Diamo un'occhiata a un'altra cosa direttamente dalla console Server Core; questo è un ostacolo comune da superare se non hai utilizzato molto Server Core. È nostra tendenza chiudere le finestre e le applicazioni che non vengono più utilizzate, quindi potresti chiudere inconsciamente la finestra del prompt dei comandi che serve l'intera esistenza amministrativa all'interno di una sessione della console Server Core. Ora sei seduto su un grande schermo vuoto, apparentemente senza interfaccia e nessun posto dove andare da qui.

Come torni a lavorare su questo server? Dobbiamo spegnere e riaccendere il server per resettarlo? Ciò interromperebbe qualsiasi ruolo o traffico che questo server potrebbe servire agli utenti, quindi ovviamente non è l'approccio ideale.

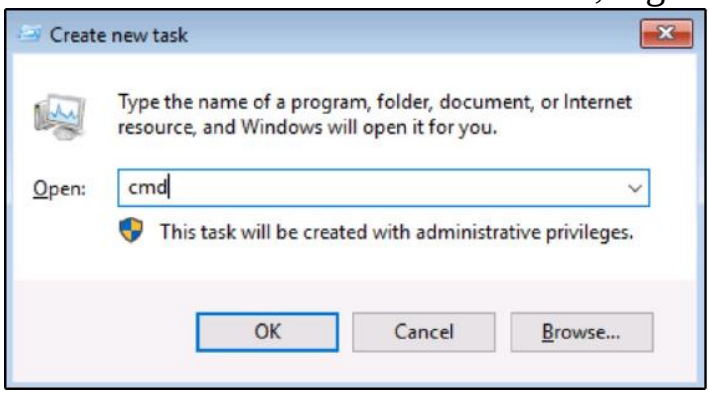
C'è un modo semplice per recuperare il prompt dei comandi, utilizzando Task Manager per avviare una nuova istanza del prompt dei comandi. Dopo aver chiuso erroneamente la finestra del prompt dei comandi corrente, quando sei seduto sulla schermata nera vuota di una console Server Core, puoi premere Ctrl + Alt + Canc e ti verranno presentate le seguenti opzioni:



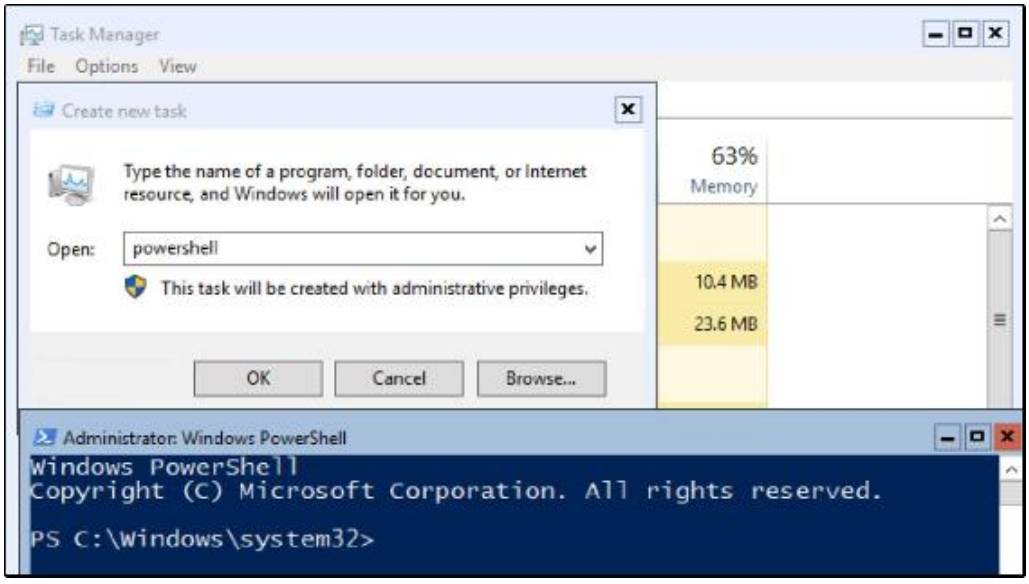
In realtà ci sono alcune funzioni diverse che puoi eseguire qui, il che è abbastanza carino. Ma per riavere la nostra finestra del prompt dei comandi, scorri verso il basso su Task Manager e premi Invio. Questo avvierà l'applicazione Task Manager che tutti conosciamo. Ora fai clic su Maggiori dettagli per espandere le schermate di Task Manager. Apri il menu File e fai clic su Esegui nuova attività:


Task Manager
File
Options
View
Run new task
Exit
sers
Details
Services
1%
CPU
58%
Memory
Name
Status
Apps (1)
Task Manager
0%
9.3 MB
Background processes (7)

Nel nella casella Crea nuova attività, digitare cmd e quindi fare clic su OK:



In alternativa, è possibile specificare di avviare qualsiasi applicazione direttamente da questo prompt Crea nuova attività. Se fossi interessato a passare direttamente a PowerShell, invece di digitare cmd, potresti invece semplicemente digitare powershell in quel prompt e si aprirà direttamente:



Windows Admin Center per la gestione di Server Core

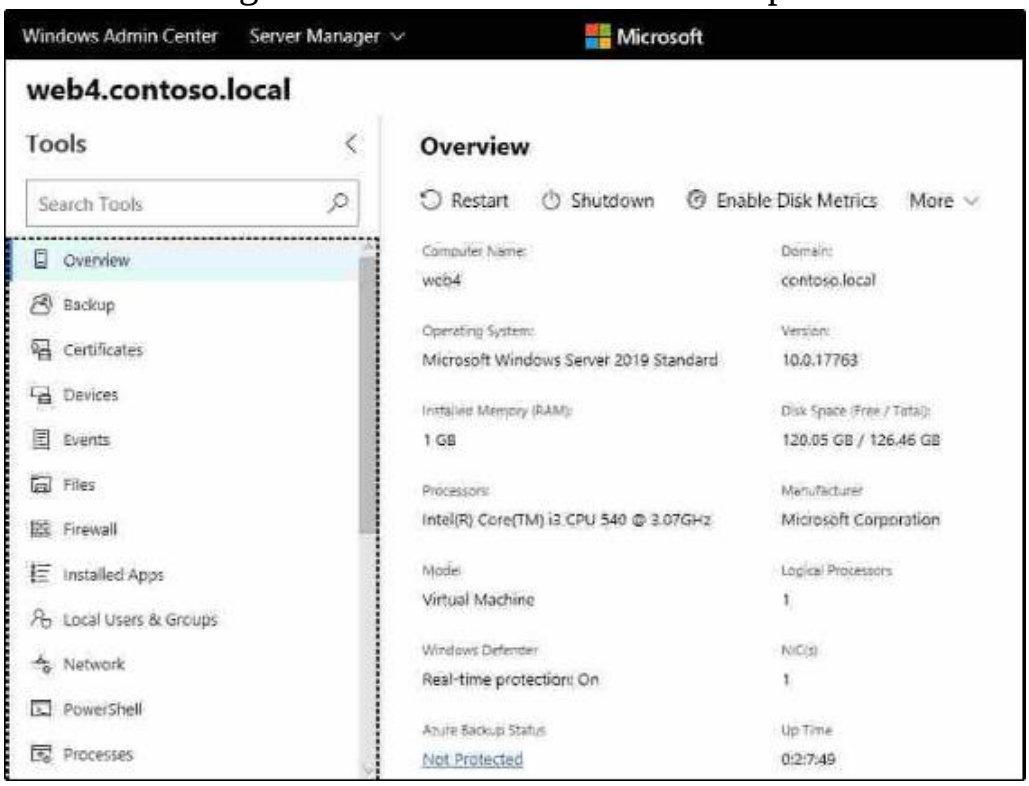
Sebbene il prompt dei comandi dalla console, le connessioni remote di PowerShell, l'amministrazione remota di Server Manager e persino gli strumenti RSAT in esecuzione su una workstation Windows 10 siano tutti strumenti validi e potenti per l'amministrazione delle nostre istanze Server Core, ora sono stati tutti rimpiazzati dal rilascio di Windows Admin Center. Hai già appreso cosa può fare Windows Admin Center per la gestione centralizzata dell'intera infrastruttura server, ma ciò che dobbiamo sottolineare qui è che WAC può essere utilizzato per server con e senza interfacce grafiche.

Ho parlato con molti amministratori di Windows Server sull'argomento Server Core e uno dei maggiori ostacoli all'implementazione di queste piattaforme server più efficienti e sicure è il timore che, una volta configurato, l'amministrazione e la manutenzione continua di questi server sarà più difficile maniglia. Gli amministratori che hanno familiarità e si sentono a proprio agio nel lavorare all'interno dell'esperienza desktop di Windows Server sanno esattamente cosa è necessario fare per svolgere le loro attività quotidiane, ma rimuovono quell'interfaccia punta e clicca e improvvisamente la giornata lavorativa diventa molto più complicata.

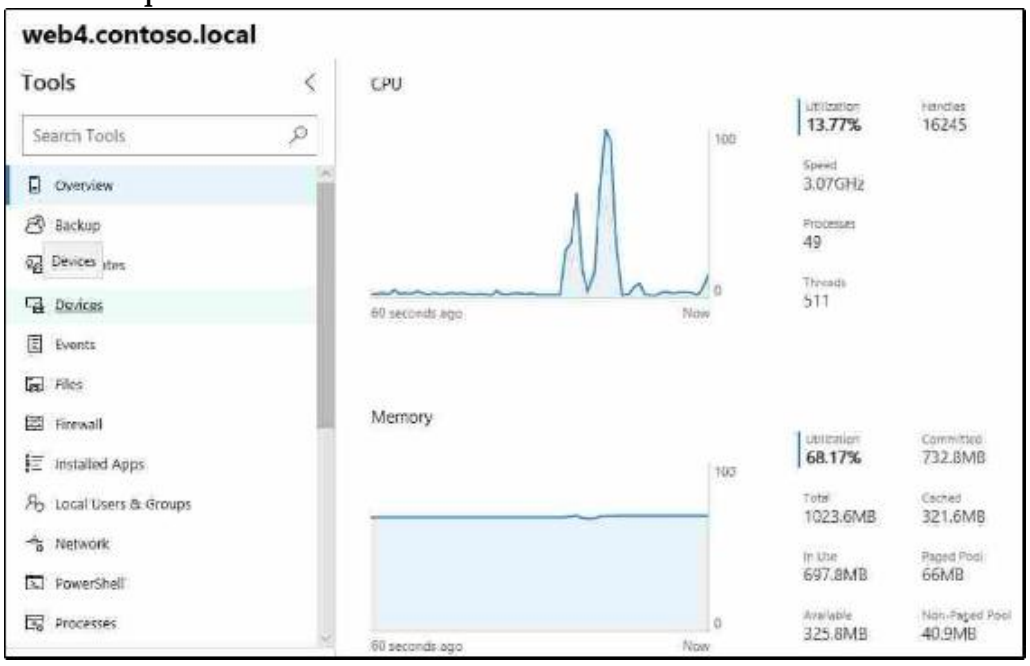
Per fortuna, non è necessario memorizzare il manuale di PowerShell per utilizzare Server Core! Windows Admin Center tratta le istanze Server Core nello stesso modo in cui gestisce un server che esegue Esperienza desktop. Funziona e basta!

Abbiamo già WAC installato su un server nel nostro laboratorio di test, quindi apriamolo e aggiungiamo il mio nuovo server WEB4 da amministrare, e diamo un'occhiata a quali opzioni sono disponibili per la manutenzione continua di questo server.

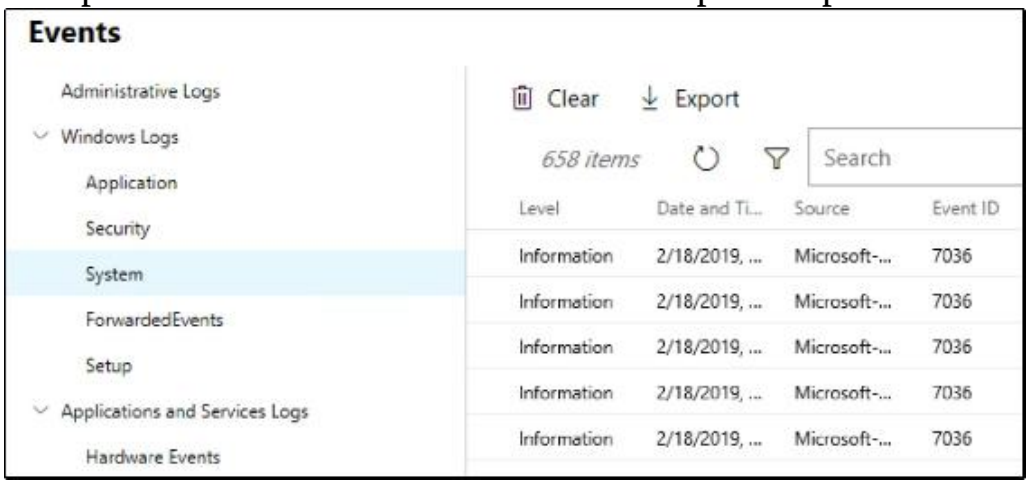
quando per prima cosa ci colleghiamo a WEB4 tramite la console WAC, in realtà non c'è nulla qui che indichi che si tratta di un'istanza Server Core, abbiamo tutti gli strumenti e le utilità WAC disponibili su cui fare clic:



Proviamo un paio di cose da Windows Admin Center. Ovviamente hai i controlli di alimentazione proprio nella parte superiore dello schermo, da cui potresti facilmente spegnere o riavviare il server. È molto più semplice e veloce che dover stabilire una connessione PowerShell remota per emettere comandi per eseguire le stesse azioni. Ci sono anche metriche delle prestazioni nella schermata principale (se scorri verso il basso), che mostrano le risorse di CPU, memoria e rete consumate. Senza WAC, dovresti accedere a WEB4 e avviare Task Manager per vedere queste statistiche:

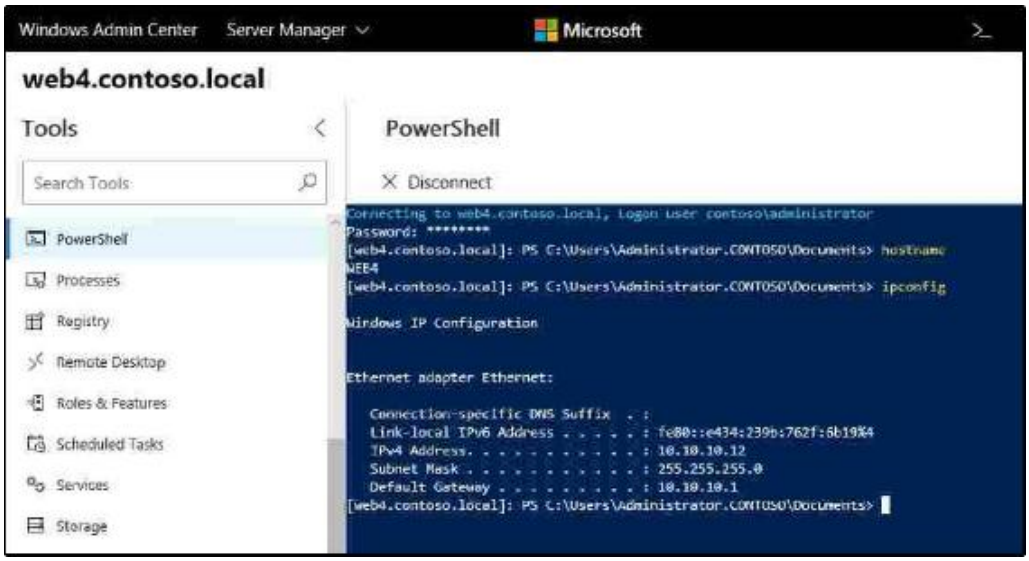


Allontanandoti dalla schermata principale, per quanto utile, prova a fare clic su uno degli strumenti elencati lungo il lato sinistro dello schermo, ad esempio Eventi. Senza WAC, se volessi risolvere un problema su un Server Core, avrebbe senso esaminare i registri eventi di Windows su quel server, ma come faresti a farlo da un'interfaccia della riga di comando? Suppongo che avresti potuto accedere alla console Server Core e utilizzare Task Manager per avviare EventVwr, ma aprire WAC e semplicemente fare clic su Eventi è molto più semplice:



Altri esempi di funzioni utili all'interno di WAC, in particolare quando si lavora con un'istanza Server Core, sarebbero l'utilizzo di File per navigare nella struttura di file e cartelle del disco rigido di WEB4 o l'utilizzo della funzione Firewall qui per creare o rimuovere le regole di Windows Firewall su WEB4 . C'è anche uno strumento di rete, da cui è possibile manipolare le configurazioni degli indirizzi IP.

Sebbene esistano molti altri strumenti all'interno del Windows Admin Center, l'ultimo che voglio sottolineare è che, ancora una volta, abbiamo un'opzione PowerShell (simile a quello che possiamo avviare da Server Manager). Questo pulsante di PowerShell richiamerà e visualizzerà per noi una connessione PowerShell remota all'istanza WEB4 Server Core, se mai non riusciamo a trovare una funzione necessaria all'interno di WAC e dobbiamo immergerci un po 'più sotto il cofano per ottenere qualcosa da un'interfaccia di comando. E la parte migliore è che non hai mai dovuto avviare PowerShell! Tutto questo sta ancora accadendo dalla finestra del tuo browser Internet:



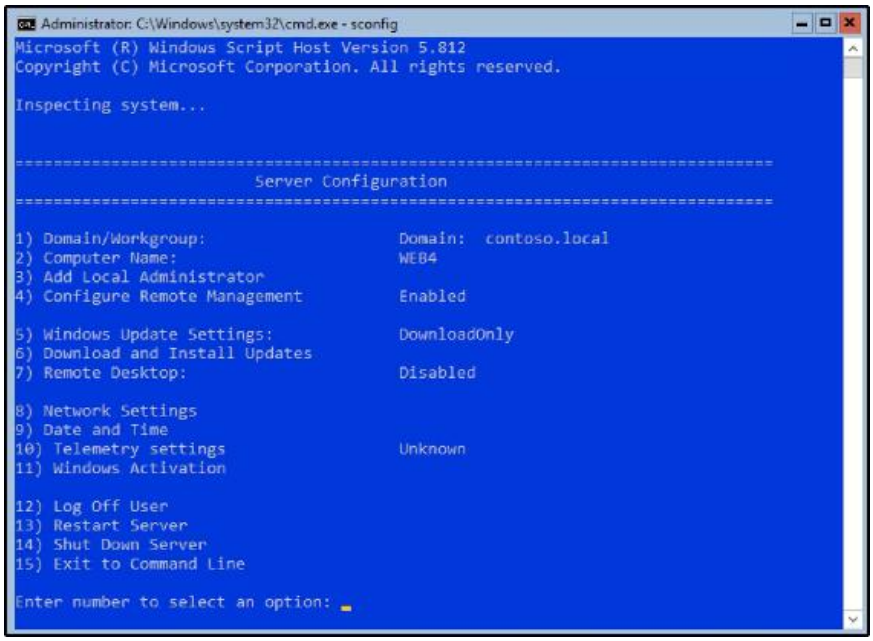
È possibile ottenere molto di più dall'interfaccia di amministrazione di Windows. Modifica del registro, aggiunta di ruoli e funzionalità, controllo dello stato dei servizi, persino interfacciamento con Windows Update. Se non stai già utilizzando WAC, ti manca la barca!

L'utilità Sconfig

Ora faremo un passo indietro e verificheremo uno strumento disponibile all'interno di Server Core, ma generalmente utile solo quando si lavora sulla console del proprio server. Come hai visto, ogni volta che avvii un Server Core, entri in una finestra del prompt dei comandi da cui puoi passare a PowerShell e quindi utilizzare i tradizionali cmdlet di Windows per configurare la tua nuova istanza Server Core.

In alternativa, puoi utilizzare l'utility Sconfig. Questo è un insieme di strumenti, una specie di scorciatoie da riga di comando, per implementare gli elementi di base necessari per portare il tuo nuovo server online e collegarlo alla rete. Lo scopo di Sconfig è quello di essere il passaggio 1 dopo l'installazione del sistema operativo, occupandosi delle configurazioni iniziali sul nuovo server in modo da poter poi saltare per iniziare a utilizzare una delle interfacce amministrative più robuste, come Server Manager o Windows Admin Centro.

Immediatamente dopo aver avviato una nuova istanza Server Core, ti trovi al prompt dei comandi, che è in attesa di input. All'interno di questa schermata, digita semplicemente Sconfig e premi Invio; dovresti sperimentare un rapido passaggio dal nero al blu e vedere la seguente schermata:

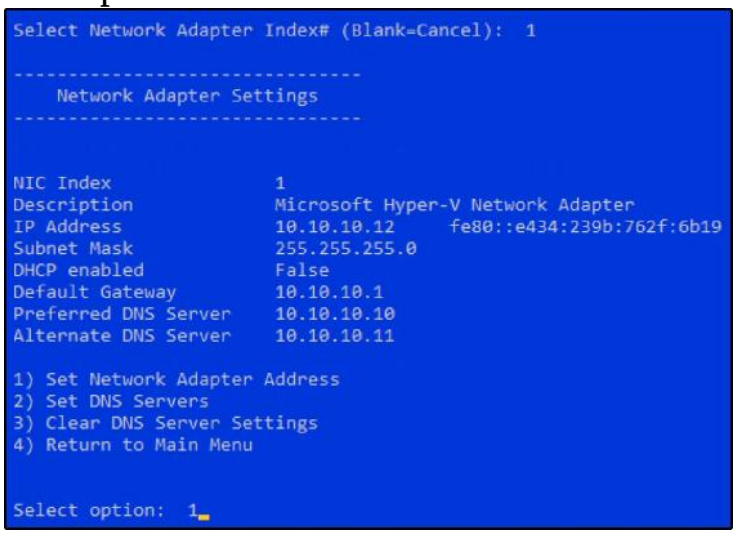

Administrator: C:\Windows\system32\cmd.exe - sconfig
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.
Inspecting system...
Server Configuration
1) Domain/Workgroup: Domain: contoso.local
2) Computer Name: WEB4
3) Add Local Administrator
4) Configure Remote Management Enabled
5) Windows Update Settings: DownloadOnly
6) Download and Install Updates
7) Remote Desktop: Disabled
8) Network Settings
9) Date and Time
10) Telemetry settings Unknown
11) Windows Activation
12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line
Enter number to select an option:

Le opzioni disponibili all'interno di Sconfig sono abbastanza autoesplicative, ma tratteremo le attività comuni eseguite qui. Ancora una volta, queste sono tutte cose che potresti invece realizzare tramite i cmdlet di PowerShell, ma trovo più facile adottare l'approccio Sconfig. Gli usi più comuni di questa interfaccia sono la configurazione delle impostazioni di rete iniziali premendo 8 o la configurazione del nome host del server e dell'appartenenza al dominio utilizzando le opzioni 2 e 1.

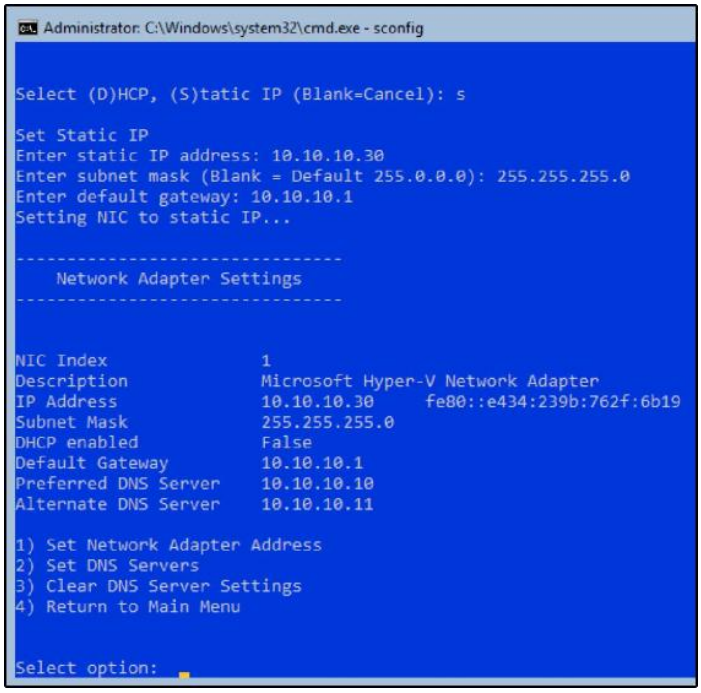
Andrò avanti e premerò 2 sulla tastiera, quindi premerò Invio e mi verrà immediatamente presentato un messaggio che mi chiede di specificare un nuovo nome di computer. Questo è un modo estremamente veloce per configurare il nome host dei nuovi server Server Core. Poiché in realtà non voglio rinominare WEB4, lascerò vuota la selezione e premerò Invio per tornare alla schermata principale.

Ora voglio controllare le impostazioni di rete. Premendo 8 e poi Invio mi porta in Impostazioni di rete, dove posso vedere che il mio indirizzo IP corrente sulla scheda di rete di WEB4 è 10.10.10.12. Questo è corretto, ma cambiamo quell'indirizzo per il gusto di attraversare una vera modifica delle impostazioni di Sconfig.

Per prima cosa ho selezionato l'indice della mia scheda di rete, che era il numero uno. Ora mi vengono mostrate ulteriori informazioni su ciò che è già configurato su questa scheda NIC e ho opzioni per modificare queste informazioni. Selezionando di nuovo l'opzione uno mi consentirà di impostare l'indirizzo della scheda di rete:



Immettere la lettera S, che dice a Sconfig che si desidera immettere un indirizzo IP statico, quindi immettere il nuovo indirizzo IP che si desidera configurare su questa NIC. Cambierò WEB4 in 10.10.10.30, solo per dimostrare che funziona. Dopo aver inserito l'indirizzo IP, devo anche definire una nuova maschera di sottorete e indirizzo gateway:



La scheda di rete di WEB4 è stata immediatamente aggiornata con un nuovo indirizzo IP di 10.10.10.30, come mostrato nell'output risultante. Anche se potrebbe non essere un evento comune visitare lo strumento Sconfig dopo la configurazione iniziale di un'istanza Server Core, questo strumento può far risparmiare tempo quando viene utilizzato per la configurazione iniziale della rete e le impostazioni di denominazione di qualsiasi nuovo Server Core.

Ruoli disponibili in Server Core

Server Core è ovviamente una forma limitata del sistema operativo e alcuni dei ruoli all'interno di Windows Server semplicemente non sono progettati per funzionare correttamente in quel contesto limitato. Fortunatamente per noi, la maggior parte di loro lo è, il che consente agli amministratori di Server 2019 di distribuire la maggior parte della loro infrastruttura critica tramite la piattaforma Server Core più sicura. Di seguito è riportato un elenco dei ruoli attualmente supportati per l'esecuzione in un'istanza di Windows Server 2019 Server Core:

- Servizi certificati Active Directory Servizi di dominio Active Directory Active Directory Federation Services
- Active Directory Lightweight Directory Services Servizi di gestione dei diritti di Active Directory Attestazione dell'integrità del dispositivo
- Server DHCP
- Servizi file server
- DNS
- Servizio di sorveglianza host Hyper-V
- Accesso remoto ai servizi di stampa e documentazione
- Server Web dei servizi di attivazione dei contratti multilicenza (IIS)
- Servizi di aggiornamento di Windows Server

Cosa è successo a Nano Server?

Questa storia sulle piattaforme Windows Server di dimensioni ridotte non terminava con Server Core. Chiunque abbia tenuto sotto controllo le nuove funzionalità in uscita con Server 2016 è consapevole che esisteva un'altra opzione di installazione per il sistema operativo Server 2016 chiamata Nano Server. La premessa di Nano Server era un ancora più piccolo, più sicuro, più efficiente,
sistema operativo minuscolo in grado di eseguire un insieme limitato di ruoli. Sebbene limitato, era ancora in grado di essere installato su una piattaforma server fisica o virtuale, eseguito come un vero sistema operativo per server e poteva ancora ospitare carichi di lavoro tradizionali su di esso.

Sfortunatamente per gli appassionati di Nano Server, e soprattutto per chiunque abbia già fatto il lavoro di installazione e utilizzo, la storia dietro Nano Server è cambiata completamente negli ultimi due anni. Per farla breve: non puoi più usare Nano Server per tutto ciò che può fare un server tradizionale. Non è possibile installarlo su hardware fisico; non puoi nemmeno installare Nano su una VM. Inoltre, le funzionalità di gestione, come PowerShell e WinRM, sono state rimosse da Nano Server e non è possibile installare alcun ruolo infrastrutturale Microsoft su di esso.

Con tutte queste funzionalità che sono state strappate dall'ambito di Nano Server, cosa resta? È morto? Nano Server può fare QUALCOSA?

La risposta sono i contenitori. Se sei interessato a utilizzare i contenitori per creare e ospitare applicazioni scalabili e pronte per il cloud, è qui che ora si concentra Nano. Tratteremo maggiori informazioni sui container e sul fatto che Nano Server è completamente sposato con loro inCapitolo 11, Containers e Nano Server, ma basti dire che il download delle immagini dei container da Microsoft sarà ora l'unico posto in cui troverai Nano Server.

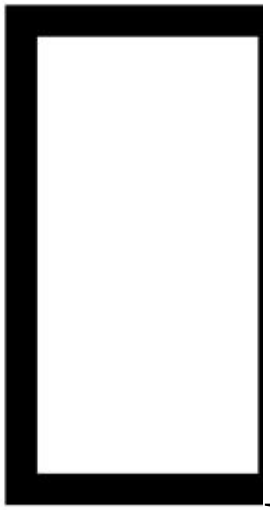
Sommario

Devo essere onesto con te: scrivere questo capitolo è stato esattamente il calcio nelle mutande di cui avevo bisogno per iniziare a pensare di ridurre i miei server. Sono nella stessa barca di molti di voi: so cos'è Server Core e ci ho giocato, ma non ho mai preso le misure per usarlo davvero nell'ambiente di produzione che supporto. Ora che strumenti come Sconfig e il nuovo Windows Admin Center sono disponibili per noi, ho ufficialmente esaurito le scuse sul motivo per cui non dovrei distribuire nuovi ruoli sulle scatole Server Core.
Anche se non fa mai male imparare qualcosa di nuovo, l'utilizzo di Server Core non comporta più il requisito di essere fluenti in PowerShell. I primi giorni di Server Core erano necessari per essere davvero bravi con PowerShell, poiché questo era l'unico modo affidabile per configurare e interfacciarsi con i tuoi minuscoli server, ma questi nuovi strumenti ci consentono di utilizzare la piattaforma più piccola e amministrarla senza memorizzare un mucchio di nuovi cmdlet.

La sicurezza è la ragione principale per cui dovremmo considerare tutti Server Core come il nostro nuovo standard. L'interfaccia grafica di Windows aggiunge molto codice e garantisce molte capacità a coloro che hanno effettuato l'accesso ai server, come la possibilità di navigare in Internet. Questo apre tutti i tipi di porte a vulnerabilità che semplicemente non esistono in Server Core. Il prossimo capitolo tratta delle ridondanze in Windows Server 2019.

Domande

1. Vero o falso: Server Core è l'opzione di installazione predefinita per Windows Server 2019.
2. Vero o falso: è possibile utilizzare PowerShell per modificare un server 2019 dalla modalità Server Core alla modalità Desktop Experience.
3. Quando sei seduto alla console di un'istanza di Windows Server 2019 Server Core appena avviata, quale applicazione vedi sullo schermo?
4. Quale cmdlet può essere utilizzato per visualizzare la configurazione di rete corrente su un Server Core?
5. Quale cmdlet di PowerShell può essere utilizzato per configurare il nome host di un Server Core?
6. Assegna un nome ad alcuni degli strumenti di gestione che possono essere usati per interfacciarsi in remoto con un Server Core.
7. Qual è il nome dell'utilità incorporata in Server Core che può essere avviata per fornire collegamenti rapidi alle attività per la configurazione di indirizzi IP, nome host e appartenenza al dominio?



Ridondanza in Windows Server 2019

Moltiplicalo per due. Questa è una frase che sento spesso quando pianifico le implementazioni per lavoro. Sono sicuro che lo hai anche tu. Ogni volta che stai implementando una nuova tecnologia, devi pianificare tale implementazione con molta attenzione. Scopri di quali server hai bisogno, dove devono essere posizionati e come la rete deve essere configurata per quei ragazzi. Una volta completata la pianificazione, ordina due di tutto, nel caso in cui uno si rompa. Viviamo in un mondo di tecnologia sempre attiva.

I servizi in calo sono inaccettabili, in particolare se ospitiamo servizi cloud o cloud privati. In realtà, qualsiasi applicazione o servizio da cui i nostri utenti dipendono per portare a termine il proprio lavoro è mission-critical e richiede il 100% di uptime, o maledettamente vicino ad esso. Il problema con la ridondanza è che è molto più facile parlare in modo che parlare a piedi. Forse un giorno saremo benedetti con una magia Premi qui per rendere questo pulsante ridondante del server, ma oggi non è quel

giorno. Dobbiamo comprendere le tecnologie a nostra disposizione che ci consentono di fornire ridondanza sui nostri sistemi. Questo capitolo ci introdurrà ad alcune di queste tecnologie. Questo libro è incentrato sul Server 2019 utilizzato in sede, quindi le tecnologie di cui parleremo oggi sono quelle che puoi utilizzare nei tuoi data center locali, sui server reali (fisici o virtuali) che sei responsabile della creazione, configurazione e manutenzione. Sì, il cloud può fornirci alcune magiche opzioni di scalabilità e ridondanza, ma quelle sono facili e spesso non abbiamo nemmeno bisogno di capire come funzionano. Quando utilizziamo i nostri server all'interno delle nostre mura, come possiamo aggiungere una maggiore affidabilità ai nostri sistemi?

Tratteremo i seguenti argomenti trattati in questo capitolo:

- **Bilanciamento del carico di rete** (NLB) Configurazione di un clustering di failover del sito Web con bilanciamento del carico
- Livelli di clustering

- Configurazione di un cluster di failover
- Recenti miglioramenti del clustering in Windows Server
- **Spazi di archiviazione diretta** (S2D)

Bilanciamento carico di rete (NLB)

Spesso, quando sento persone che parlano di ridondanza sui loro server, la conversazione include molte istanze della parola cluster, ad esempio "Se configuriamo un cluster per fornire ridondanza a quei server ..." o "Il nostro sito web principale è in esecuzione su un cluster ... "Sebbene sia fantastico che venga utilizzata una qualche forma di resilienza sui sistemi a cui si riferiscono queste conversazioni, spesso accade che il clustering non sia effettivamente coinvolto da nessuna parte. Quando riassumiamo i dettagli di come sono configurati i loro sistemi, scopriamo che è NLB a fare questo lavoro per loro. Discuteremo il clustering reale più avanti in questo capitolo, ma prima volevo iniziare con l'approccio più comune per rendere ridondanti molti servizi. Bilanciamento carico di rete distribuisce il traffico a livello TCP / IP, il che significa che i sistemi operativi del server stessi non sono completamente consapevoli o non fanno affidamento l'uno sull'altro, con la ridondanza invece fornita a livello di rete. Ciò può essere particolarmente confuso, bilanciamento del carico di rete rispetto al clustering, perché a volte Microsoft si riferisce a qualcosa come un cluster, quando in realtà utilizza Bilanciamento carico di rete per realizzare tali connessioni. Un ottimo esempio è DirectAccess. Quando si hanno due o più server DA insieme in un array, ci sono documenti TechNet e persino posti all'interno della console in cui viene indicato come un cluster. Ma qui non è in corso alcun clustering di failover; la tecnologia sotto il cofano che sta facendo fluire le connessioni a entrambi i nodi è in realtà Windows NLB. Questo può essere particolarmente confuso, bilanciamento del carico di rete e clustering, perché a volte Microsoft si riferisce a qualcosa come un cluster, quando in realtà utilizza Bilanciamento carico di rete per realizzare tali connessioni. Un ottimo esempio è DirectAccess. Quando si hanno due o più server DA insieme in un array, ci sono documenti TechNet e persino posti all'interno della console in cui viene indicato come un cluster. Ma qui non è in corso alcun clustering di failover; la tecnologia sotto il cofano che sta facendo fluire le connessioni a entrambi i nodi è in realtà Windows NLB. Questo può essere particolarmente confuso, bilanciamento del carico di rete e clustering, perché a volte Microsoft si riferisce a qualcosa come un

cluster, quando in realtà utilizza Bilanciamento carico di rete per realizzare tali connessioni. Un ottimo esempio è DirectAccess. Quando si hanno due o più server DA insieme in un array, ci sono documenti TechNet e persino posti all'interno della console in cui viene indicato come un cluster. Ma qui non è in corso alcun clustering di failover; la tecnologia sotto il cofano che sta facendo fluire le connessioni a entrambi i nodi è in realtà Windows NLB. Ma qui non è in corso alcun clustering di failover; la tecnologia sotto il cofano che sta facendo fluire le connessioni a entrambi i nodi è in realtà Windows NLB. Ma qui non è in corso alcun clustering di failover; la tecnologia sotto il cofano che sta facendo fluire le connessioni a entrambi i nodi è in realtà Windows NLB.

Probabilmente hai sentito alcuni dei nomi nel mercato del bilanciamento del carico hardware: F5, Cisco, Kemp, Barracuda. Queste aziende forniscono box hardware dedicati che possono prendere il traffico diretto verso un particolare nome o destinazione e suddividere tale traffico tra due o più server delle applicazioni. Sebbene questo sia generalmente il modo più affidabile per stabilire NLB, è anche il più costoso e rende l'ambiente in generale più complesso. Una caratteristica offerta da questi ragazzi che il bilanciamento del carico di rete di Windows integrato non è in grado di fornire è la terminazione SSL o l'offload SSL, come spesso lo chiamiamo. Questi dispositivi specializzati sono in grado di ricevere il traffico del sito Web dai computer degli utenti, ovvero SSL, e di decrittografare i pacchetti prima di inviarli al server Web appropriato. In questo modo, il server web stesso sta facendo meno lavoro, poiché non Tuttavia, oggi non parleremo affatto di bilanciatori del carico hardware, ma piuttosto delle funzionalità NLB fornite direttamente in Windows Server 2019.

Non è lo stesso del DNS round-robin

Ho scoperto, nel corso degli anni, che l'idea di NLB di alcune persone è in realtà un DNS round-robin. Consentitemi di fare un esempio: supponiamo di avere un sito Web intranet a cui tutti i vostri utenti accedono quotidianamente. È logico che tu voglia fornire un po 'di ridondanza a questo sistema e quindi configurare due server web, nel caso in cui uno si interrompa. Tuttavia, nel caso in cui uno si interrompa, non si desidera richiedere passaggi manuali di cutover per eseguire il failover sul server aggiuntivo, si desidera che avvenga automaticamente. In DNS, è possibile creare due record host A che hanno lo stesso nome, ma puntano a indirizzi IP diversi. Se Server01 è in esecuzione su 10.10.10.5 e Server02 è in esecuzione su 10.10.10.6, è possibile creare due record DNS entrambi denominati INTRANET, indicando un record host a 10.10.10.5 e l'altro record host a 10.10.10.6. Ciò fornirebbe un DNS round-robin, ma non un reale bilanciamento del carico. In sostanza, ciò che accade qui è che quando i computer client raggiungono INTRANET, DNS passerà loro l'uno o l'altro indirizzo IP per connettersi. Al DNS non interessa se quel sito web è effettivamente in esecuzione, risponde semplicemente con un indirizzo IP. Quindi, anche se potresti configurarlo e sembra che funzioni perfettamente perché puoi vedere che i client si connettono sia a Server01 che a Server02, tieni presente. In caso di errore del server, avrai molti client che continuano a funzionare e molti client che ricevono improvvisamente Page non possono essere visualizzati quando DNS decide di inviarli all'indirizzo IP del server che ora è offline. Il DNS passerà loro l'uno o l'altro indirizzo IP per la connessione. Al DNS non interessa se quel sito web è effettivamente in esecuzione, risponde semplicemente con un indirizzo IP. Quindi, anche se potresti configurarlo e sembra che funzioni perfettamente perché puoi vedere che i client si connettono sia a Server01 che a Server02, tieni presente. In caso di errore del server, avrai molti client che continuano a funzionare e molti client che ricevono improvvisamente Page non possono essere visualizzati quando DNS decide di inviarli all'indirizzo IP del server che ora è offline. Il DNS passerà loro l'uno o l'altro indirizzo IP per la connessione. Al DNS non interessa se quel sito web è effettivamente in esecuzione, risponde

semplicemente con un indirizzo IP. Quindi, anche se potresti configurarlo e sembra che funzioni perfettamente perché puoi vedere che i client si connettono sia a Server01 che a Server02, tieni presente. In caso di errore del server, avrai molti client che continuano a funzionare e molti client che stanno ricevendo improvvisamente Page non possono essere visualizzati quando DNS decide di inviarli all'indirizzo IP del server che ora è offline. essere avvisati. In caso di errore del server, avrai molti client che continuano a funzionare e molti client che ricevono improvvisamente Page non possono essere visualizzati quando DNS decide di inviarli all'indirizzo IP del server che ora è offline. essere avvisati. In caso di errore del server, avrai molti client che continuano a funzionare e molti client che ricevono improvvisamente Page non possono essere visualizzati quando DNS decide di inviarli all'indirizzo IP del server che ora è offline.

NLB è molto più intelligente di così. Quando un nodo in un array NLB si interrompe, il traffico che si sposta all'indirizzo IP condiviso verrà indirizzato solo al nodo che è ancora in linea. Lo vedremo di persona a breve, quando configureremo NLB su un nostro sito Web intranet.

Quali ruoli possono utilizzare NLB?

Bilanciamento carico di rete è progettato principalmente per applicazioni senza stato, in altre parole, applicazioni che non richiedono uno stato di memoria a lungo termine o uno stato di connessione. In un'applicazione senza stato, ogni richiesta effettuata dall'applicazione potrebbe essere presa da Server01 per un po ', quindi passare a Server02 senza interrompere l'applicazione. Alcune applicazioni lo gestiscono molto bene (come i siti Web) e altre no.

I servizi Web (IIS) traggono sicuramente i maggiori vantaggi dalla ridondanza fornita da NLB. Bilanciamento carico di rete è abbastanza facile da configurare e fornisce la ridondanza completa per i siti Web in esecuzione sui server Windows, senza incorrere in costi aggiuntivi. Bilanciamento carico di rete può inoltre essere utilizzato per migliorare FTP, firewall e server proxy.

Un altro ruolo che interagisce comunemente con Bilanciamento carico di rete è il ruolo di accesso remoto. In particolare, DirectAccess può utilizzare Bilanciamento carico di rete di Windows integrato per fornire all'ambiente di accesso remoto server con punto di ingresso ridondanti. Quando si configura DirectAccess per utilizzare il bilanciamento del carico, non è immediatamente ovvio che si utilizza la funzionalità Bilanciamento carico di rete incorporata nel sistema operativo perché si configurano le impostazioni di bilanciamento del carico dall'interno della console di gestione dell'accesso remoto, anziché dalla console Bilanciamento carico di rete. Quando si esaminano le procedure guidate di gestione dell'accesso remoto per stabilire il bilanciamento del carico, la console di accesso remoto si sta effettivamente avvicinando al meccanismo di bilanciamento del carico di rete all'interno del sistema operativo e lo sta configurando, in modo che i suoi algoritmi e meccanismi di trasporto siano i pezzi utilizzati da DirectAccess per suddividere il traffico tra più server.

Una delle parti migliori dell'utilizzo di Bilanciamento carico di rete è che puoi apportare modifiche all'ambiente senza influire sui nodi esistenti. Vuoi aggiungere un nuovo server a un array NLB esistente? Nessun problema. Inseriscilo senza tempi di inattività. Devi rimuovere un server per la manutenzione? Nessun problema neanche qui. Bilanciamento carico di rete può essere interrotto su un nodo particolare, consentendo a un altro nodo dell'array di recuperare il margine di flessibilità. In effetti, NLB è in realtà NIC-particolare, quindi puoi eseguire diverse modalità NLB su diverse NIC all'interno dello stesso server. È possibile dire a NLB di fermarsi su una particolare NIC, rimuovendo quel server dall'array per il momento. Ancora meglio, se hai un po 'di tempo prima di dover portare il server offline, puoi emettere un comando drainstop invece di un arresto immediato. Ciò consente alle sessioni di rete esistenti attualmente attive su quel server di terminare in modo pulito. Nessuna nuova sessione fluirà alla NIC che hai interrotto e le vecchie sessioni evaporeranno naturalmente nel tempo. Una volta che tutte le sessioni sono state eliminate da quel server, puoi quindi strapparlo e portarlo giù per la manutenzione.

Indirizzi IP virtuali e dedicati

Il modo in cui NLB utilizza gli indirizzi IP è un concetto importante da comprendere. Prima di tutto, a qualsiasi NIC su un server che farà parte di un array con bilanciamento del carico deve essere assegnato un indirizzo IP statico. Bilanciamento carico di rete non funziona con l'indirizzamento DHCP. Nel mondo NLB, un indirizzo IP statico su una scheda NIC viene indicato come indirizzo IP dedicato (DIP). Questi DIP sono unici per NIC, il che significa ovviamente che ogni server ha il proprio DIP. Ad esempio, nel mio ambiente, WEB1 esegue un indirizzo DIP di 10.10.10.40 e il mio server WEB2 esegue un DIP di 10.10.10.41.

Ogni server ospita lo stesso sito Web sui rispettivi indirizzi DIP. È importante capire che quando si stabilisce l'NLB tra questi due server, è necessario mantenere i singoli DIP sulle scatole, ma creerò anche un nuovo indirizzo IP che verrà condiviso tra i due server. Questo IP condiviso è chiamato indirizzo IP virtuale (VIP). Quando eseguiremo a breve la configurazione del bilanciamento del carico di rete, userò l'indirizzo IP del 10.10.10.42 come mio VIP, che è finora inutilizzato nella mia rete. Ecco un rapido layout degli indirizzi IP che verranno utilizzati durante la configurazione del mio sito Web con bilanciamento del carico di rete:

WEB1 DIP = 10.10.10.40 WEB2 DIP = 10.10.10.41 VIP condiviso = 10.10.10.42

Quando stabilisco il mio record DNS per intranet.contoso.local, che è il nome del mio sito web. Creerò solo un singolo record A dell'host e punterà al mio VIP 10.10.10.42.

Modalità NLB

A breve, ci troveremo nella configurazione effettiva del nostro bilanciamento del carico e dovremo prendere alcune decisioni all'interno di tale interfaccia. Una delle decisioni più importanti è quale modalità NLB vogliamo utilizzare. Unicast è scelto per impostazione predefinita ed è il modo in cui vedo la maggior parte delle aziende impostare il proprio NLB, forse perché è l'opzione predefinita e non hanno mai pensato di cambiarlo. Dedichiamo un minuto per discutere ciascuna delle opzioni disponibili, per assicurarci di poter scegliere quella più appropriata per le tue esigenze di rete.

Unicast

Qui, iniziamo ad entrare nel vivo di come NLB distribuisce i pacchetti tra i diversi host. Dal momento che non abbiamo un bilanciatore del carico fisico che riceve prima il traffico e poi decide dove inviarlo, in che modo i

server con bilanciamento del carico decidono chi può prendere quale flusso di pacchetti?

Per rispondere a questa domanda, dobbiamo fare un po 'di backup e discutere come scorre il traffico all'interno della tua rete. Quando apri un browser web sul tuo computer e visitiHTTP: // WEB1,DNS risolve quell'indirizzo IP a 10.10.10.40, ad esempio. Quando il traffico colpisce i tuoi interruttori e deve essere diretto da qualche parte, gli interruttori devono decidere dove deve andare il traffico 10.10.10.40. Potresti avere familiarità con l'idea degli indirizzi MAC.

Ogni NIC ha un indirizzo MAC e quando si assegna un indirizzo IP a una NIC, registra il proprio indirizzo MAC e IP con l'apparecchiatura di rete. Questi indirizzi MAC sono memorizzati all'interno di una tabella ARP, che è una tabella che risiede nella maggior parte degli switch, router e firewall. Quando al mio server WEB1 è stato assegnato l'indirizzo IP 10.10.10.40, ha registrato il suo indirizzo MAC corrispondente a 10.10.10.40. Quando il traffico deve fluire verso WEB1, gli switch si rendono conto che il traffico destinato a 10.10.10.40 deve andare a quello specifico indirizzo MAC della NIC e lo spara di conseguenza.

Quindi, nel mondo NLB, quando invii traffico a un singolo indirizzo IP suddiviso tra più NIC, come viene elaborato a livello MAC? La risposta con NLB unicast è che l'indirizzo MAC del NIC fisico viene sostituito con un indirizzo MAC virtuale e questo MAC viene assegnato a tutte le NIC all'interno dell'array NLB. Ciò fa sì che i pacchetti che fluiscono a quell'indirizzo MAC vengano consegnati a tutte le NIC, quindi a tutti i server, in quell'array. Se pensi che un sacco di traffico di rete non necessario si stia spostando intorno agli switch, avresti ragione. Bilanciamento carico di rete unicast significa che quando i pacchetti sono destinati all'indirizzo MAC virtuale di un array, il traffico viene sostanzialmente rimbalzato attraverso tutte le porte dello switch prima di trovare e atterrare sulle loro destinazioni.

La parte migliore di unicast è che funziona senza dover effettuare configurazioni speciali sugli switch o sulle apparecchiature di rete nella maggior parte dei casi. Si imposta la configurazione del bilanciamento del carico di rete dall'interno degli strumenti di Windows Server e gestisce il resto. Uno svantaggio dell'unicast è che, poiché lo stesso indirizzo MAC esiste su tutti i nodi, causa alcuni problemi di comunicazione all'interno del nodo. In altre parole, i server abilitati per Bilanciamento carico di rete avranno problemi a comunicare con gli indirizzi IP degli altri. Spesso, questo non ha molta importanza, perché WEB1 raramente avrebbe motivo di comunicare direttamente con WEB2. Ma se hai davvero bisogno che quei server web siano in grado di parlare tra loro in modo coerente e affidabile, la soluzione più semplice è installare una scheda NIC separata

su ciascuno di quei server e utilizzare quella NIC per quelle comunicazioni intra-array,

L'altro aspetto negativo di unicast è che può creare un allagamento degli interruttori. Gli switch non sono in grado di apprendere un percorso permanente per l'indirizzo MAC virtuale, perché abbiamo bisogno che venga consegnato a tutti i nodi del nostro array. Poiché ogni pacchetto che si sposta sul MAC virtuale viene inviato lungo tutte le strade di uno switch in modo che possa raggiungere tutte le NIC in cui deve essere consegnato, ha il potenziale per sopraffare gli switch con questo flusso di pacchetti di rete. Se sei preoccupato per questo o stai ricevendo lamentele dai tuoi addetti alla rete riguardo allo switch flooding, potresti voler controllare una delle modalità multicast per il tuo cluster NLB.

Un metodo alternativo per controllare il flooding degli switch unicast consiste nell'essere creativi con le VLAN sugli switch. Se pianifichi un array di server NLB e desideri assicurarti che il traffico dello switch generato da questo array non influenzi altri sistemi nella tua rete, potresti sicuramente creare una piccola VLAN sugli switch e collegare solo le tue NIC abilitate per NLB a quella VLAN . In questo modo, quando si verifica l'inondazione pianificata, colpisce solo quel piccolo numero di porte all'interno della VLAN, invece di segmentarsi attraverso l'intero switch.

Multicast

La scelta del multicast come modalità NLB comporta alcuni vantaggi e alcuni mal di testa. Il positivo è che aggiunge un indirizzo MAC aggiuntivo a ciascuna scheda NIC. Ogni membro NLB dispone quindi di due indirizzi MAC: l'originale e quello creato dal meccanismo NLB. Ciò offre agli switch e alle apparecchiature di rete un lavoro più semplice per apprendere i percorsi e inviare il traffico alle destinazioni corrette, senza un travolgente flusso di pacchetti. Per fare ciò, è necessario indicare agli switch quali indirizzi MAC devono ricevere questo traffico NLB, altrimenti si provocherà il flooding degli switch, proprio come con unicast. Dire agli switch quali MAC devono essere contattati avviene accedendo agli switch e creando alcune voci ARP statiche per adattarlo. Per qualsiasi azienda con un professionista del networking dedicato, generalmente esperto in apparecchiature Cisco, non sarà un problema. Se non hai familiarità con la modifica delle tabelle ARP e l'aggiunta di route statiche, può essere un po 'fastidioso farlo bene. Alla fine, il multicast è generalmente migliore dell'unicast, ma può essere più un problema amministrativo. La mia preferenza personale tende ancora ad essere unica, soprattutto nelle piccole imprese. L'ho visto utilizzato in molte reti diverse senza problemi, e andare con unicast significa che possiamo lasciare da sola la programmazione dello switch.

IGMP multicast

Meglio ancora, ma non sempre un'opzione, è multicast con Internet Group Management Protocol (IGMP). L'IGMP multicast aiuta davvero a mitigare il flooding degli switch, ma funziona solo se i tuoi switch supportano lo snooping IGMP. Ciò significa che lo switch ha la capacità di guardare all'interno dei pacchetti multicast per determinare esattamente dove dovrebbero andare. Quindi, laddove unicast crea una certa quantità di switch flooding in base alla progettazione, multicast può aiutare a ridurre tale quantità e IGMP può eliminarlo completamente.

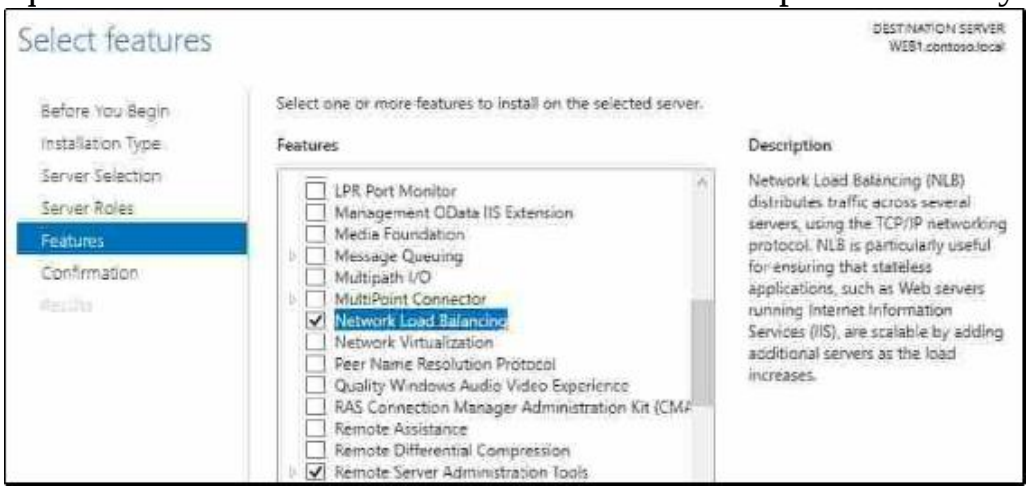
La modalità NLB che scegli dipenderà in gran parte dalle capacità delle tue apparecchiature di rete. Se i tuoi server hanno un solo NIC, prova a usare multicast o avrai problemi all'interno dell'array. D'altra parte, se gli switch e i router non supportano il multicast, non hai scelta: l'unicast sarà l'unica opzione per la configurazione del bilanciamento del carico di rete di Windows.

Configurazione di un sito Web con bilanciamento del carico

Basta parlare; è ora di farlo da soli e di provarlo. Ho due server web in esecuzione sulla rete del mio laboratorio, WEB1 e WEB2. Entrambi utilizzano IIS per ospitare un sito Web intranet. Il mio obiettivo è fornire ai miei utenti un singolo record DNS con cui comunicare, ma fare in modo che tutto il traffico venga suddiviso tra i due server con un vero bilanciamento del carico. Segui i passaggi per renderlo possibile.

Abilitazione di Bilanciamento carico di rete

Per prima cosa, dobbiamo assicurarci che WEB1 e WEB2 siano pronti per eseguire NLB, perché non è installato per impostazione predefinita. Bilanciamento carico di rete è una funzionalità disponibile in Windows Server 2019 e la aggiungi come qualsiasi altro ruolo o funzionalità, eseguendo la procedura guidata Aggiungi ruoli e funzionalità. Aggiungi questa funzionalità su tutti i server che vuoi far parte dell'array NLB:



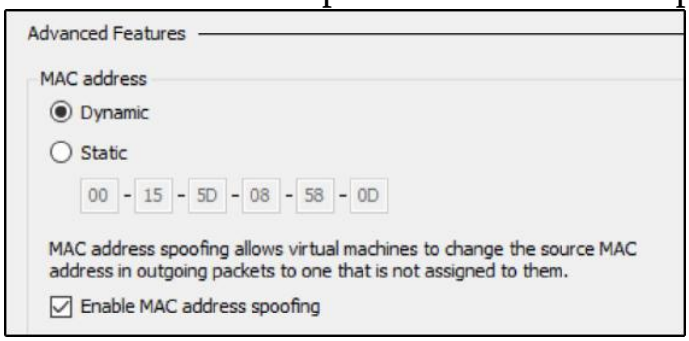
Abilitazione dello spoofing dell'indirizzo MAC sulle VM

Ricordi quando abbiamo parlato di bilanciamento carico di rete unicast e di come l'indirizzo MAC fisico della NIC viene sostituito con un indirizzo MAC virtuale utilizzato per le comunicazioni dell'array NLB? Sì, alle macchine virtuali non piace. Se stai bilanciando il carico di server fisici con NIC fisici, puoi saltare questa sezione. Ma molti di voi eseguiranno server Web che sono VM. Indipendentemente dal fatto che siano ospitati con Hyper-V, VMware o qualche altra tecnologia di virtualizzazione, c'è un'opzione extra nella configurazione della macchina virtuale stessa che dovrai fare, in modo che la tua VM rispetti felicemente questa modifica dell'indirizzamento MAC.

Il nome di questa impostazione sarà qualcosa sulla falsariga di Abilita spoofing dell'indirizzo MAC, sebbene il nome specifico della funzione potrebbe essere diverso a seconda della tecnologia di virtualizzazione utilizzata. L'impostazione dovrebbe essere una semplice casella di controllo che devi abilitare per far funzionare correttamente lo spoofing MAC. Assicurati di farlo per tutti i tuoi NIC virtuali su cui prevedi di utilizzare NLB. Tieni presente che questa è un'impostazione per NIC, non per VM. Se si dispone di più schede di rete su una macchina virtuale, potrebbe essere necessario selezionare la casella per ciascuna scheda di rete, se si prevede di utilizzarle tutte con il bilanciamento del carico.

La VM deve essere arrestata per apportare questa modifica, quindi ho spento i miei server WEB1 e WEB2. Ora trova la casella di controllo e abilitala. Poiché tutto ciò che utilizzo è basato sulla tecnologia Microsoft, sto ovviamente utilizzando Hyper-V come piattaforma per le mie macchine virtuali qui in laboratorio. All'interno di Hyper-V, se faccio clic con il pulsante destro del mouse sul mio server WEB1 e accedo alle impostazioni della VM, posso quindi fare clic sulla scheda di rete per vedere i vari pezzi modificabili sulla NIC virtuale di WEB1. Nelle ultime versioni di Hyper-V, questa impostazione è elencata sotto le proprietà

NIC, all'interno della sezione intitolata Funzionalità avanzate. Ed eccola lì, la mia casella di controllo Abilita spoofing dell'indirizzo MAC. Basta fare clic su di esso per abilitarlo e tutto è pronto:

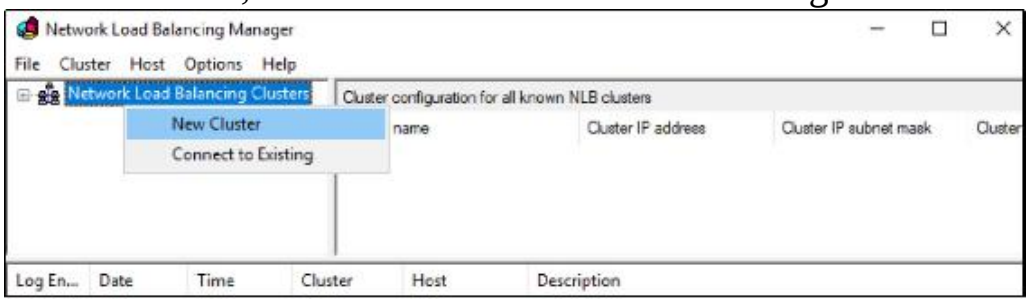


Se Abilita spoofing dell'indirizzo MAC è disattivato, ricorda che la macchina virtuale deve essere completamente spenta prima che venga visualizzata l'opzione. Spegnilo, quindi apri Impostazioni e dai un'altra occhiata. L'opzione dovrebbe ora essere disponibile per la selezione.

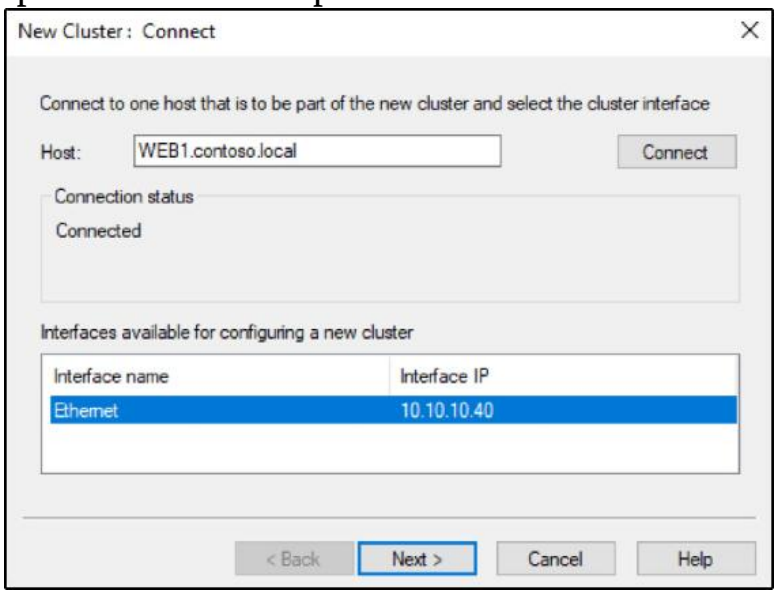
Configurazione di Bilanciamento carico di rete

Riassumiamo dove siamo a questo punto. Ho due server web, WEB1 e WEB2, e ciascuno di essi ha attualmente un unico indirizzo IP. Ogni server ha IIS installato, che ospita un singolo sito web. Ho abilitato lo spoofing dell'indirizzo MAC su ciascuno (perché questi server sono macchine virtuali) e ho appena finito di installare la funzione NLB su ogni server web. Ora abbiamo tutte le parti e le parti in atto per essere in grado di configurare Bilanciamento carico di rete e suddividere il traffico web tra entrambi i server.

Lavorerò da WEB1 per la configurazione iniziale di NLB. Accedi a questo e vedrai che abbiamo un nuovo strumento nell'elenco degli strumenti disponibili all'interno di Server Manager, chiamato Network Load Balancing Manager. Vai avanti e apri quella console. Dopo aver aperto Gestione bilanciamento carico di rete, fai clic con il pulsante destro del mouse su Cluster di bilanciamento del carico di rete e scegli Nuovo cluster, come mostrato nello screenshot seguente:

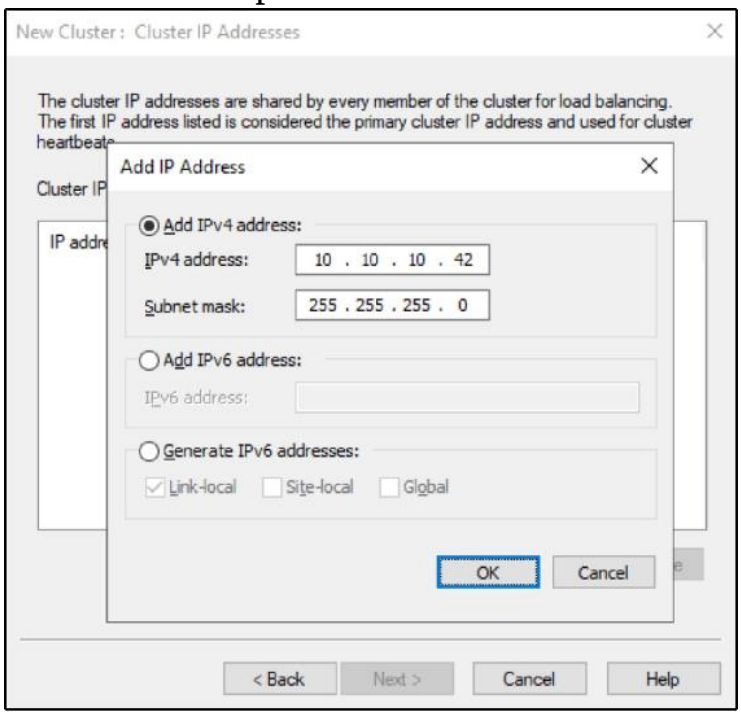


Quando crei un nuovo cluster, è importante notare che attualmente non ci sono macchine in questo cluster. Anche il server su cui stiamo eseguendo questa console non viene aggiunto automaticamente al cluster e dobbiamo ricordarci di inserirlo manualmente in questa schermata. Quindi prima digiterò il nome del mio server WEB1 e farò clic su Connetti. Dopo averlo fatto, il gestore NLB interrogherà WEB1 per NIC e mi fornirà un elenco di NIC disponibili su cui potrei potenzialmente impostare NLB:

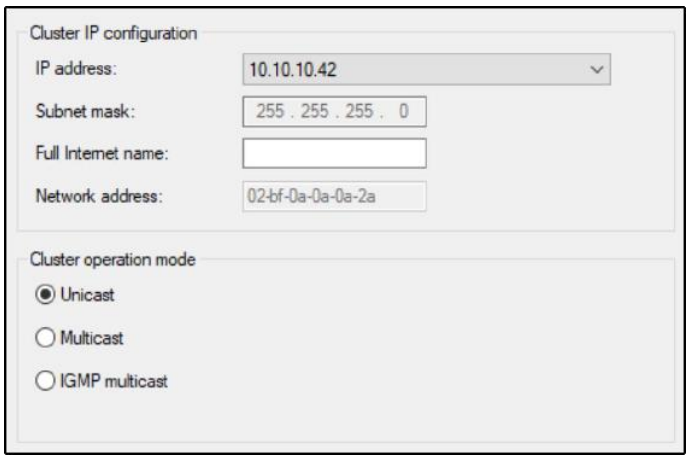


Dato che ho solo una scheda NIC su questo server, la lascio selezionata e faccio clic su Avanti. La seguente schermata ti dà l'opportunità di inserire indirizzi IP aggiuntivi su WEB1, ma poiché stiamo eseguendo solo un indirizzo IP, lascerò questa schermata così com'è e farò di nuovo clic su Avanti.

Ora siamo passati a una finestra che ci chiede di inserire gli indirizzi IP del cluster. Questi sono i VIP che intendiamo utilizzare per comunicare con questo cluster NLB. Come affermato in precedenza, il mio VIP per questo sito Web sarà 10.10.10.42, quindi faccio clic sul pulsante Aggiungi ... e inserisco quell'indirizzo IPv4 insieme alla sua maschera di sottorete corrispondente:

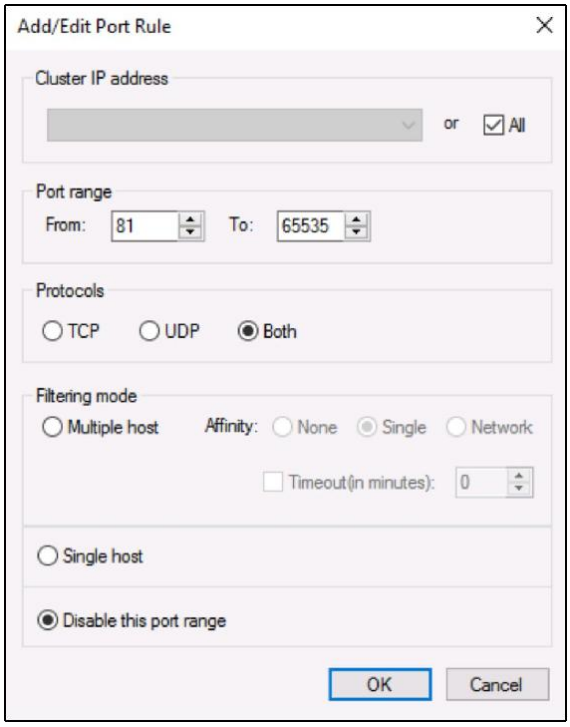


Un altro clic sul pulsante Avanti e ora possiamo vedere la nostra opzione per quale modalità di funzionamento del cluster vogliamo eseguire. A seconda della configurazione di rete, scegli tra Unicast, Multicast e IGMP multicast:

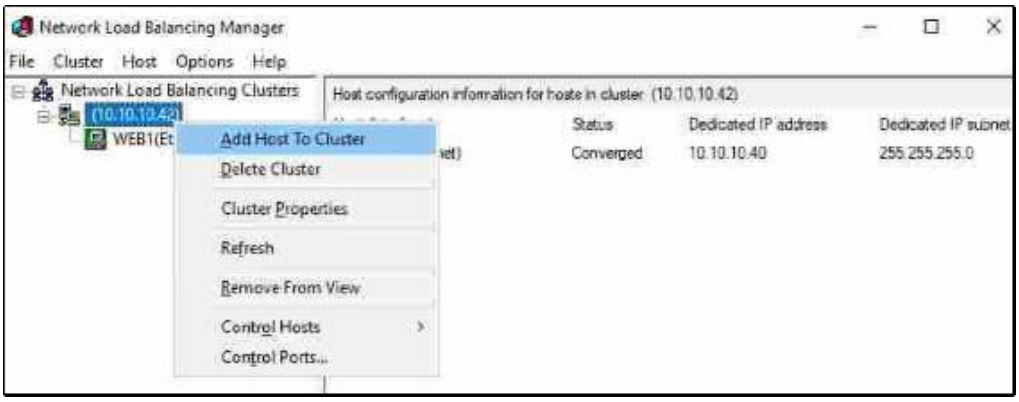


La seguente schermata della nostra procedura guidata NLB consente di configurare le regole delle porte. Per impostazione predefinita, esiste un'unica regola che dice a NLB di bilanciare il carico del traffico in arrivo su qualsiasi porta, ma puoi modificarlo se lo desideri. Non vedo molte persone nel campo che specificano regole qui per distribuire porte specifiche a destinazioni specifiche, ma una caratteristica interessante in questo screenshot è la possibilità di disabilitare determinati intervalli di porte.

Questa funzione potrebbe essere molto utile se desideri bloccare il traffico non necessario a livello di bilanciamento del carico di rete. Ad esempio, lo screenshot seguente mostra una configurazione che impedirebbe il passaggio delle porte 81 e successive attraverso il meccanismo di bilanciamento del carico di rete:

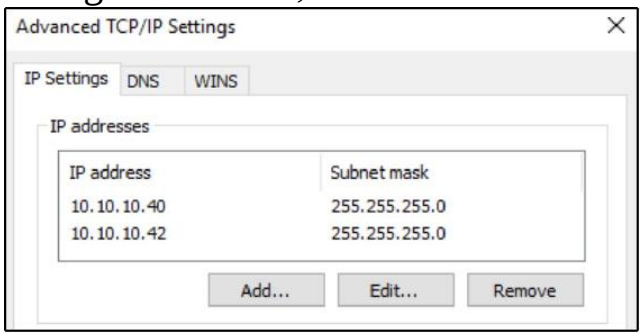


Termina la procedura guidata e ora hai creato un cluster NLB! Tuttavia, a questo punto abbiamo specificato solo le informazioni sul VIP e sul server WEB1. Non abbiamo stabilito nulla su WEB2. Stiamo eseguendo un array NLB, ma attualmente quell'array ha solo un singolo nodo al suo interno, quindi il traffico verso l'array sta atterrando su WEB1. Fare clic con il pulsante destro del mouse sul nuovo cluster e selezionare Aggiungi host al cluster:



Immettere il nome del nostro server WEB2, fare clic su Connetti ed eseguire la procedura guidata per aggiungere il nodo NLB secondario di WEB2 nel cluster. Una volta aggiunti entrambi i nodi al cluster, il nostro array NLB, o cluster, è online e pronto per l'uso. (Vedi, ti ho detto che la parola cluster è usata in molti posti, anche se non si tratta affatto di un cluster di failover!)

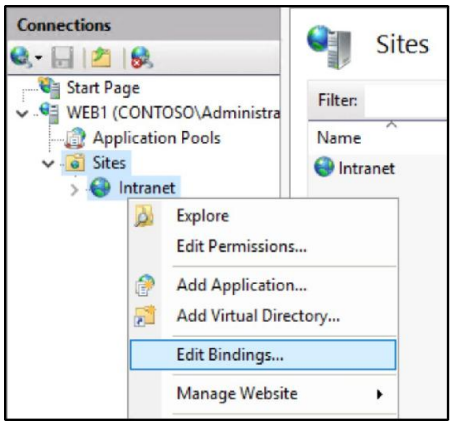
Se dai un'occhiata alle proprietà NIC dei nostri server web e fai clic su Avanzate
pulsante all'interno delle proprietà TCP / IPv4, puoi vedere che il nostro nuovo indirizzo IP del cluster di
È stato aggiunto 10.0.0.42ai NIC. Ogni NIC conterrà ora sia l'indirizzo DIP assegnato ad essa, sia l'indirizzo VIP condiviso nell'array:



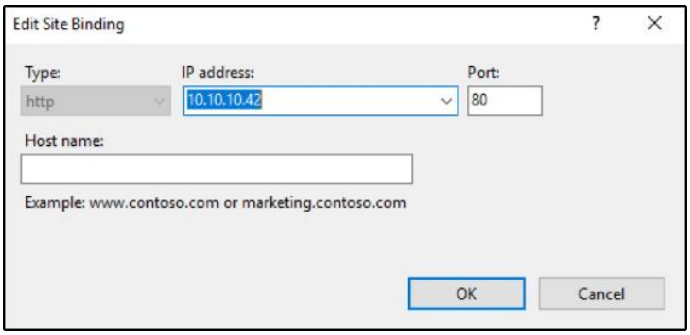
Il traffico che è destinato per il 10.10.10.42 l'indirizzo IP inizia ora a essere suddiviso tra i due nodi, ma in questo momento i siti Web in esecuzione sui server WEB1 e WEB2 sono configurati per essere eseguiti solo sugli indirizzi IP 10.10.10.40 e 10.10.10.41 dedicati , quindi dobbiamo assicurarci di modificarlo in seguito.

Configurazione di IIS e DNS

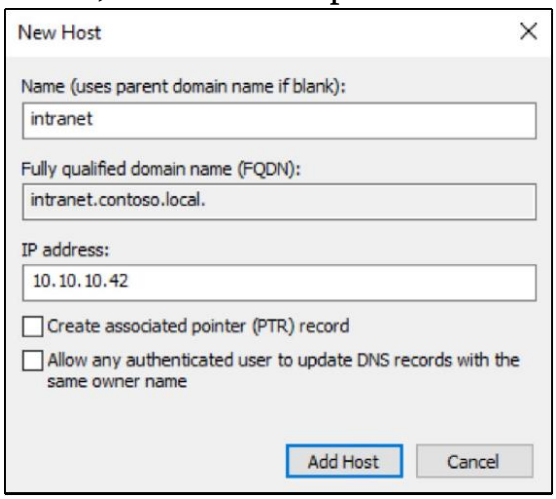
Basta un rapido passaggio all'interno di IIS su ciascuno dei nostri server Web per far sì che il sito Web risponda all'indirizzo IP appropriato. Ora che la configurazione del bilanciamento del carico di rete è stata stabilita e abbiamo confermato che il nuovo indirizzo VIP 10.10.10.42 è stato aggiunto alle schede NIC, possiamo utilizzare quell'indirizzo IP come associazione del sito Web. Apri la console di gestione IIS ed espandi la cartella Siti in modo da poter vedere le proprietà del tuo sito web. Fare clic con il pulsante destro del mouse sul nome del sito e scegliere Modifica associazioni ...:



Una volta all'interno di Site Bindings, scegli il binding che desideri manipolare e fai clic sul pulsante Modifica ... Questo sito Web intranet è solo un semplice sito HTTP, quindi sceglierò il mio binding HTTP per questa modifica. L'associazione è attualmente impostata su 10.10.10.40 su WEB1 e 10.10.10.41 su WEB2. Ciò significa che il sito web risponde solo al traffico che arriva su questi indirizzi IP. Tutto quello che devo fare è cambiare il menu a discesa dell'indirizzo IP nel nuovo VIP, che è 10.10.10.42. Dopo aver apportato questa modifica (su entrambi i server) e aver fatto clic su OK, il sito Web risponde immediatamente al traffico in arrivo tramite l'indirizzo IP 10.10.10.42:



Veniamo ora all'ultimo pezzo del puzzle: DNS. Ricorda, vogliamo che gli utenti abbiano la possibilità di entrare semplicementehttp: // intranet nei loro browser web per navigare questo nuovo sito Web NLB, quindi è necessario configurare di conseguenza un record A dell'host DNS. Questo processo è esattamente lo stesso di qualsiasi altro record host DNS; creane uno e punta intranet.contoso.local a 10.10.10.42:



Testarlo

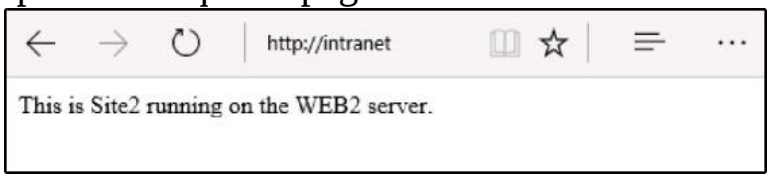
Bilanciamento carico di rete è configurato? Dai un'occhiata.

Le associazioni IIS sono aggiornate? Dai un'occhiata.

È stato creato il record DNS? Dai un'occhiata.

Siamo pronti per testare questa cosa. Se apro un browser Internet su un computer client e accedo a[http: // intranet,](http://intranet) Riesco a vedere il sito web:

Ma come possiamo determinare che il bilanciamento del carico funziona davvero? Se continuo ad aggiornare la pagina o sfoglio da un altro client, continuo ad accedere[http: // intranet ,](http://intranet)e alla fine il meccanismo NLB deciderà che una nuova richiesta deve essere inviata a WEB2, invece che a WEB1. Quando ciò accade, mi viene invece presentata questa pagina:



Come puoi vedere, ho modificato il contenuto tra WEB1 e WEB2 in modo da poter distinguere tra i diversi nodi, proprio ai fini di questo test. Se si trattasse di un vero sito Web intranet di produzione, vorrei assicurarmi che il contenuto di entrambi i siti fosse esattamente lo stesso, in modo che gli utenti fossero completamente all'oscuro del NLB persino in corso. Tutto quello che devono sapere è che il sito web sarà disponibile e funzionante, tutto il tempo.

Svuotamento della cache ARP

In precedenza, abbiamo avuto una piccola discussione su come gli switch mantengono una cache di informazioni ARP, il che riduce il tempo che questi switch devono impiegare per decidere dove devono fluire i pacchetti. Quando si assegna un indirizzo IP a una scheda NIC, l'indirizzo MAC di quella scheda viene associato all'indirizzo IP all'interno della tabella ARP di alcune apparecchiature di rete.
Switch, router, firewall: questi strumenti hanno comunemente ciò a cui ci riferiamo come una tabella ARP,
e quindi hanno un insieme di dati in quella tabella che è noto come cache ARP.

Quando si configura Bilanciamento carico di rete, in particolare unicast, l'indirizzo MAC della scheda di rete viene sostituito con un nuovo indirizzo MAC virtuale. A volte gli switch e le apparecchiature di rete sono molto veloci nel cogliere questo cambiamento e associano il nuovo indirizzo MAC al nuovo indirizzo IP e tutto funziona perfettamente. Tuttavia, trovo che quando si configura Bilanciamento carico di rete, in genere è vero quanto segue: più intelligente e costoso è l'apparecchiatura di rete, più stupido diventa quando si configura Bilanciamento carico di rete. Quello che voglio dire è che la tua apparecchiatura di rete potrebbe continuare a conservare le informazioni del vecchio indirizzo MAC che sono memorizzate nella sua tabella ARP e non vengono aggiornate per riflettere il nuovo indirizzamento MAC.

Che aspetto ha nella vita reale? Il traffico di rete interromperà il flusso da o verso tali NIC. A volte, quando si stabilisce Bilanciamento carico di rete e si accende, tutto il traffico di rete si interrompe improvvisamente verso o da quelle interfacce di rete. Cosa devi fare per risolvere questa situazione?
A volte puoi aspettare e in pochi minuti, ore o anche pochi giorni gli interruttori lasceranno cadere le vecchie informazioni ARP e consentiranno ai nuovi MAC virtuali di registrarsi in quella tabella. Cosa puoi fare per accelerare questo processo? Svuota la cache ARP.

La procedura per eseguire questa operazione sarà diversa a seconda del tipo di apparecchiatura di rete su cui stai lavorando: se si tratta di uno switch o di un router, di che marca è, di quale modello è e così via. Ma ognuno di questi ragazzi dovrebbe avere questa capacità, e dovrebbe essere chiamato qualcosa sulla falsariga di svuotare la cache ARP. Quando si esegue questa funzione sulla propria apparecchiatura, viene eliminata la tabella ARP, eliminando le vecchie informazioni che causano problemi e consentendo ai nuovi indirizzi MAC di registrarsi in modo appropriato nella nuova tabella.

Volevo segnalarlo solo nel caso in cui configurassi Bilanciamento carico di rete, solo per vedere il flusso di traffico cessare sul tuo server. Molto probabilmente, hai a che fare con la cache ARP bloccata su uno o più dispositivi di rete che stanno tentando di trasferire il traffico da e verso il tuo server.

Clustering di failover

Abbiamo stabilito che NLB è un'ottima soluzione per le applicazioni senza stato, con un ottimo esempio sono i siti Web che si desidera rendere altamente disponibili. E gli altri ruoli o funzioni del server che desideri rendere ridondanti? Bene, l'opposto di apolidi è con stato, quindi che ne dici di dare un'elevata disponibilità a parti di tecnologia con stato?

Clustering di failover fornisce questo livello di funzionalità e può essere utilizzato nei casi in cui i nodi all'interno del cluster accedono ai dati condivisi. Questo è un fattore chiave nel modo in cui è progettato il clustering di failover, lo storage utilizzato dai nodi del cluster deve essere condiviso e accessibile da ogni nodo che ne ha bisogno. Esistono molti ruoli e servizi diversi che possono trarre vantaggio dal clustering di failover, ma esistono quattro tecnologie specifiche che sembrano costituire la maggior parte dei cluster attualmente in esecuzione nei data center: Hyper-V, servizi file, Exchange e SQL. Se stai lavorando con una di queste tecnologie, ed è probabile che tu lavori con tutte, devi esaminare le funzionalità di alta disponibilità che possono essere fornite per la tua infrastruttura utilizzando il clustering di failover.

Sebbene il clustering di failover fornito da Windows Server sia creato da Microsoft e abbia la capacità di funzionare molto bene con molti ruoli e servizi Microsoft, è importante notare che è possibile stabilire clustering di failover anche per applicazioni non Microsoft. Anche le applicazioni di terze parti che vengono eseguite sui server Windows nel tuo ambiente, o anche le applicazioni sviluppate internamente, possono trarre vantaggio dal clustering di failover. Finché l'applicazione utilizza l'archiviazione condivisa e puoi specificare le attività che deve essere in grado di eseguire su tali applicazioni per gli strumenti di amministrazione del clustering: come avviare il servizio, come arrestare il servizio, come monitorare l'integrità del servizio,

Clustering di host Hyper-V

Uno degli esempi più potenti di clustering di failover viene visualizzato quando si combina il clustering con Hyper-V. È possibile creare due o più server Hyper-V, raggrupparli insieme e dare loro la capacità di ospitare tutte le macchine virtuali archiviate in quell'ambiente virtuale. Dando a tutti i server host Hyper-V l'accesso allo stesso archivio condiviso in cui sono archiviati i dischi rigidi virtuali e configurando il clustering di failover tra i nodi, puoi creare una soluzione di virtualizzazione incredibilmente potente e ridondante per la tua azienda. Quando un server Hyper-V si arresta, le VM che erano in esecuzione su quell'host Hyper-V eseguiranno il failover su un altro server host Hyper-V e verranno invece avviate da sole.

Dopo un'interruzione minima del servizio durante l'avvio delle VM, tutto torna online automaticamente, senza alcun input amministrativo. Ancora meglio, che ne dici di quando è necessario applicare una patch o altrimenti portare offline un server host Hyper-V per la manutenzione? È possibile forzare facilmente l'esecuzione delle VM su un server membro diverso nel cluster; vengono migrati in tempo reale su quel server, quindi non ci sono tempi di inattività, quindi sei libero di rimuovere il nodo per la manutenzione e terminare di lavorarci prima di reintrodurlo nel cluster. Usiamo macchine virtuali e server per tutti i tipi di carichi di lavoro, quindi non sarebbe fantastico se potessi sbarazzarti di ogni singolo punto di errore all'interno di quell'ambiente di virtualizzazione? Questo è esattamente ciò che può fornire il clustering di failover.

Bilanciamento del carico della macchina virtuale

In effetti, non solo un cluster Hyper-V ha la capacità di ripristinarsi rapidamente in caso di un nodo del server Hyper-V andare offline, ma ora abbiamo una logica di bilanciamento del carico intelligente che funziona insieme a questi servizi in cluster. Se il tuo cluster Hyper-V si sta sovraccaricando di macchine virtuali, è logico che tu aggiunga un altro nodo a quel cluster, dando al cluster più capacità e potenza di calcolo. Ma una volta aggiunto il nodo, quanto lavoro è necessario per far scorrere alcune VM su questo nuovo nodo del cluster?

Nessuna! Finché il bilanciamento del carico delle VM è abilitato, i pesi del cluster verranno valutati automaticamente e i carichi di lavoro delle VM verranno migrati in tempo reale, senza tempi di inattività, al volo, al fine di distribuire meglio il lavoro tra tutti i nodi del cluster, incluso il nuovo server. Il bilanciamento del carico delle VM può essere eseguito e valutato su richiesta, ogni volta che lo si ritiene opportuno, oppure può essere configurato per essere eseguito automaticamente, esaminando l'ambiente ogni 30 minuti, decidendo automaticamente se spostare i carichi di lavoro.

Clustering per servizi di file

Il clustering per i file server è disponibile da parecchio tempo; questa era una delle intenzioni originali dietro il rilascio del clustering. In origine, il clustering di file server era utile solo per l'utilizzo di documenti e file tradizionali, in altre parole, quando i tipi di utenti knowledge-worker hanno bisogno di accedere a file e cartelle su base giornaliera e si desidera che quei file siano altamente disponibili. Fino ad oggi, questo clustering di file server per scopi generici funziona in uno scenario attivo-passivo. Quando più file server sono raggruppati insieme per l'accesso ai file per scopi generici, solo uno di quei nodi file server è attivo e presentato agli utenti alla volta. Solo in caso di tempi di inattività su quel nodo, il ruolo viene spostato su uno degli altri membri del cluster.

File server con scalabilità orizzontale

Sebbene il clustering di file server generale sia ottimo per l'accesso ad hoc di file e cartelle, non era abbastanza completo per gestire i file che erano continuamente aperti o modificati. Un primo esempio di questi file sono i file del disco rigido virtuale utilizzati dalle macchine virtuali Hyper-V.

Ovviamente, era necessario che i file del disco rigido virtuale fossero ridondanti; perdere questi file sarebbe dannoso per le nostre attività. Per fortuna, l'hosting di carichi di lavoro dei dati delle applicazioni come questo è esattamente ciò per cui è stato progettato Scale-Out File Server (SOFS). Se prevedi di ospitare macchine virtuali utilizzando Hyper-V, ti consigliamo di controllare le funzionalità di clustering di failover disponibili per l'uso con i servizi Hyper-V. Inoltre, se intendi utilizzare host Hyper-V in cluster, dovresti controllare SOFS come tecnologia di infrastruttura per supportare quell'ambiente Hyper-V a disponibilità elevata. SOFS aiuta a supportare il clustering di failover fornendo ai file server la capacità di avere più nodi online (attivo-attivo) che rimangono costantemente persistenti tra loro. In questo modo, se un server di archiviazione non funziona, gli altri sono immediatamente disponibili per riprendere il gioco, senza un processo di cutover che comporti tempi di inattività. Questo è importante quando si osserva la differenza tra l'archiviazione di dati statici, come i documenti, e l'archiviazione di file del disco rigido virtuale a cui accedono le VM. Le VM sono in grado di rimanere online durante un'interruzione del file server con SOFS, il che è davvero incredibile!

Livelli di clustering

Un concetto di overhead per il clustering di failover che è importante comprendere sono i diversi livelli in cui il clustering può essere vantaggioso. Esistono due livelli su cui è possibile utilizzare il clustering: è possibile adottare un approccio o / o e utilizzare solo uno di questi livelli di clustering di failover oppure è possibile combinarli entrambi per impressionare davvero i propri amici ad alta disponibilità.

Livello di applicazione raggruppamento

Il clustering a livello di applicazione in genere implica l'installazione del clustering di failover sulle VM. L'utilizzo delle VM non è un requisito fisso, ma è il percorso di installazione più comune. È possibile combinare e abbinare VM con server fisici in un ambiente di cluster, purché ogni server soddisfi i criteri di installazione. Questa modalità di applicazione del clustering è utile quando si dispone di un particolare servizio o ruolo in esecuzione nel sistema operativo che si desidera rendere ridondante. Pensa a questo come più a una capacità di microclustering, in cui stai davvero scavando e rendendo ridondante un componente specifico del sistema operativo con un altro nodo del server che è in grado di recuperare il gioco nel caso in cui il tuo server primario si arresti.

Clustering a livello host

Se il clustering dell'applicazione è micro, il clustering a livello host è più macro. Il miglior esempio che posso fornire di questo è quello che fa iniziare la maggior parte degli amministratori con il clustering di failover in primo luogo: Hyper-V. Supponiamo che tu abbia due server fisici che ospitano entrambi macchine virtuali nel tuo ambiente. Si desidera raggruppare questi server insieme, in modo che tutte le VM ospitate su questi server Hyper-V possano essere ridondanti tra i due server fisici. Se un intero server Hyper-V si arresta, il secondo è in grado di avviare le VM che erano in esecuzione sul nodo primario e, dopo una minima interruzione del servizio, le VM che ospitano i carichi di lavoro effettivi nel tuo ambiente sono tornate installato e funzionante, a disposizione degli utenti e delle loro applicazioni.

Una combinazione di entrambi

Queste due modalità di utilizzo del clustering di failover menzionate in precedenza possono certamente essere combinate insieme per una storia di alta disponibilità ancora migliore e più completa. Lasciamo che questo esempio parli da solo: hai due server Hyper-V, ognuno preparato per eseguire una serie di macchine virtuali. Stai utilizzando il clustering degli host tra questi server, quindi se una scatola fisica si interrompe, l'altra riprende il gioco. Questo di per sé è fantastico, ma usi molto SQL e vuoi assicurarti che anche SQL sia altamente disponibile. È possibile eseguire due macchine virtuali, ciascuna un server SQL, e configurare il clustering di failover a livello di applicazione tra queste due macchine virtuali per i servizi SQL in modo specifico. In questo modo, se succede qualcosa a una singola macchina virtuale, non è necessario eseguire il failover sul server Hyper-V di backup, piuttosto il tuo problema può essere risolto dal secondo nodo SQL che prende il sopravvento. Non c'era bisogno di un'acquisizione di Hyper-V su vasta scala da parte del secondo server fisico, tuttavia hai utilizzato il clustering di failover per assicurarti che SQL fosse sempre online. Questo è un ottimo esempio di clustering oltre al clustering e, pensando in questo senso, puoi iniziare a diventare

piuttosto creativo con tutti i diversi modi in cui puoi utilizzare il clustering nella tua rete.

Come funziona il failover?

Dopo aver configurato il clustering di failover, i più nodi rimangono in comunicazione costante tra loro. In questo modo, quando uno si interrompe, vengono immediatamente consapevoli e possono trasferire i servizi su un altro nodo per riportarli online. Il clustering di failover utilizza il registro per tenere traccia di molte impostazioni per nodo. Questi identificatori vengono mantenuti sincronizzati tra i nodi, quindi quando uno si interrompe, le impostazioni necessarie vengono trasmesse agli altri server e al nodo successivo del cluster viene detto di avviare qualsiasi applicazione, VM o carico di lavoro ospitato sul casella principale che è andata offline. Ci può essere un leggero ritardo nei servizi quando i componenti si avviano sul nuovo nodo, ma questo processo è tutto automatizzato e senza mani, riducendo al minimo i tempi di inattività.

Quando è necessario tagliare i servizi da un nodo a un altro come evento pianificato, ad esempio per l'applicazione di patch o la manutenzione, qui c'è una storia ancora migliore. Attraverso un processo noto come migrazione in tempo reale, puoi trasferire le responsabilità su un nodo secondario senza tempi di inattività. In questo modo, è possibile rimuovere i nodi dal cluster per la manutenzione o l'applicazione di patch di sicurezza o per qualsiasi motivo, senza influire in alcun modo sugli utenti o sul tempo di attività del sistema. La migrazione in tempo reale è particolarmente utile per i cluster Hyper-V, dove spesso avrai la necessità di decidere manualmente su quale nodo sono ospitate le tue VM, al fine di eseguire il lavoro sull'altro nodo o nodi.

In molti cluster esiste un'idea di quorum. Ciò significa che se un cluster viene suddiviso, ad esempio, se un nodo va offline o se ci sono più nodi che sono improvvisamente non disponibili tramite una disconnessione dalla rete di qualche tipo, la logica del quorum prende il sopravvento per determinare quale segmento del cluster è quello che è ancora online. Se hai un cluster di grandi dimensioni che si estende su più sottoreti all'interno di una rete e succede qualcosa a livello di rete che separa i nodi del cluster l'uno dall'altro, tutti i due lati del cluster sanno che non

possono più comunicare con gli altri membri del cluster e quindi entrambi i lati del cluster presumerebbero automaticamente che ora dovrebbero assumersi la responsabilità dei carichi di lavoro del cluster.

Le impostazioni del quorum indicano al cluster quanti guasti ai nodi possono verificarsi prima che sia necessaria un'azione. Poiché l'intero cluster conosce la configurazione del quorum, può aiutare a fornire risposte a quelle domande su quale sezione del cluster deve essere principale nel caso in cui il cluster venga suddiviso. In molti casi, i cluster forniscono il quorum affidandosi a una terza parte, nota come testimone. Come suggerisce il nome, questo testimone controlla lo stato del cluster e aiuta a prendere decisioni su quando e dove il failover diventa necessario. Lo menziono qui come precursore della nostra discussione sulle nuove funzionalità di clustering integrate in Server 2019, una delle quali è un miglioramento nel modo in cui i testimoni lavorano in piccoli ambienti.

Ci sono molte più informazioni da acquisire e comprendere se si intende creare cluster sufficientemente grandi per le impostazioni del quorum e del testimone. Se sei interessato a saperne di più, dai un'occhiata https: //documenti.microsoft.com /en-noi/finestre-server/Conservazione/Conservazione-spazi / capire-quorum.

Configurazione di un cluster di failover

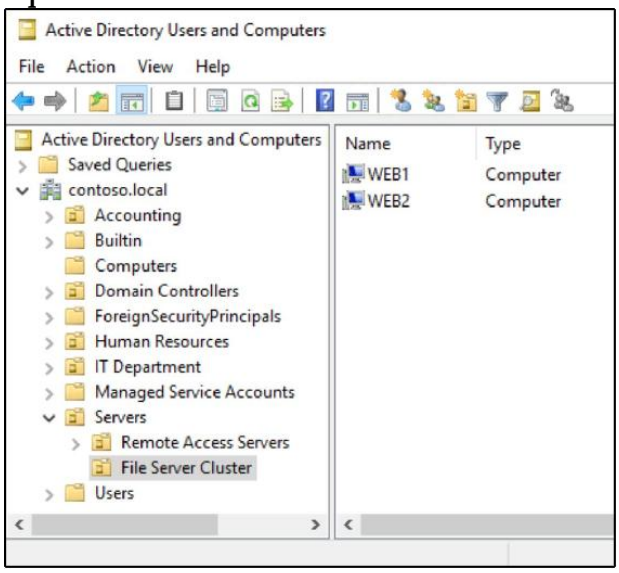
Ci vorranno alcuni minuti per configurare un piccolo cluster di server, in modo che tu possa vedere gli strumenti di gestione e i luoghi che devono essere toccati per farlo. Ora ho eseguito il backup di tutta la configurazione NLB sui miei server WEB1 e WEB2 che abbiamo impostato in precedenza, in modo che al momento siano solo semplici server Web, ancora una volta senza ridondanza tra di loro. Configuriamo il nostro primo cluster di failover e aggiungiamo entrambi questi server a quel cluster.

Costruire i server

Abbiamo due server già in esecuzione con Windows Server 2019 installato. Non è stato configurato nulla di speciale su questi server, ma ho aggiunto il ruolo File server a entrambi, perché alla fine li utilizzerò come cluster di file server. Il punto chiave qui è che dovresti avere i server il più identici possibile, con i ruoli già installati che intendi utilizzare all'interno del cluster.

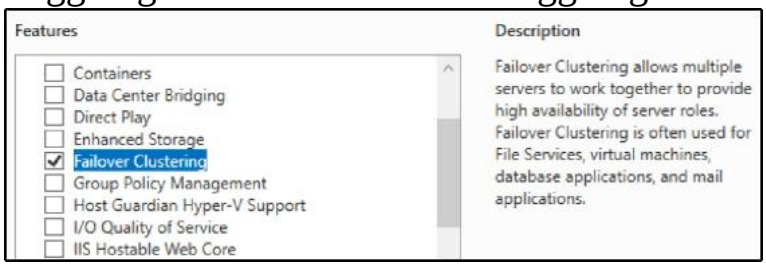
Un'altra nota durante la fase di creazione: se possibile, è consigliabile con il clustering che i server membri appartenenti allo stesso cluster risiedano all'interno della stessa unità organizzativa (OU) in Active Directory (AD). La ragione di ciò è duplice: in primo luogo, garantisce che gli stessi oggetti Criteri di gruppo vengano applicati al set di server, nel tentativo di rendere le loro configurazioni il più identiche possibile.

In secondo luogo, durante la creazione del cluster, alcuni nuovi oggetti verranno generati automaticamente e creati in AD e, quando i server membri risiedono nella stessa unità organizzativa, anche questi nuovi oggetti verranno creati in tale unità organizzativa. È molto comune con un cluster in esecuzione vedere tutti gli oggetti rilevanti in AD essere parte della stessa unità organizzativa e che l'unità organizzativa sia dedicata a questo cluster:



Installazione della funzionalità

Ora che i nostri server sono online e in esecuzione, vogliamo installare le funzionalità di clustering su ciascuno di essi. Il clustering di failover è una funzionalità di Windows Server, quindi apri la procedura guidata Aggiungi ruoli e funzionalità e aggiungila a tutti i nodi del cluster:

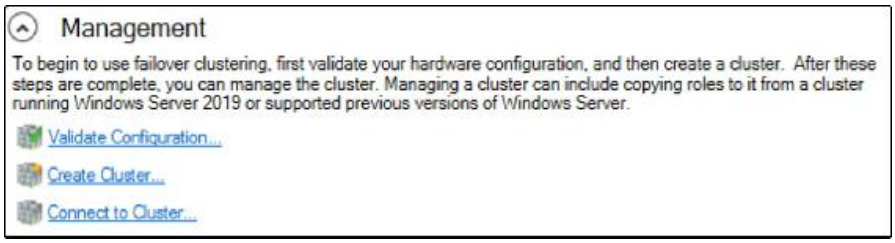


Esecuzione del gestore cluster di failover

Come nel caso della maggior parte dei ruoli o delle funzionalità installabili su Windows Server 2019, una volta implementati, troverai una relativa console di gestione all'interno del menu Strumenti di Server Manager. Se guardo ora all'interno su WEB1, posso vedere che è disponibile un nuovo elenco per Failover Cluster Manager su cui fare clic. Aprirò quello strumento e inizierò a lavorare sulla configurazione del mio primo cluster da questa interfaccia di gestione:

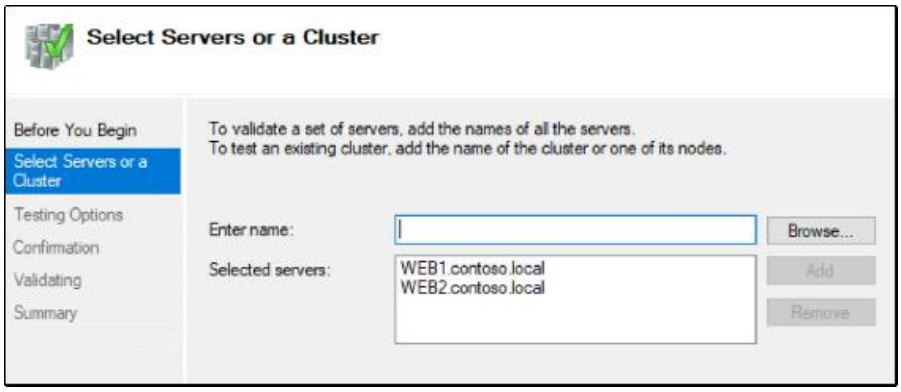
Esecuzione della convalida del cluster

Ora che siamo all'interno di Failover Cluster Manager, noterai un elenco di attività disponibili per l'avvio nella sezione Gestione della console, vicino al centro dello schermo:

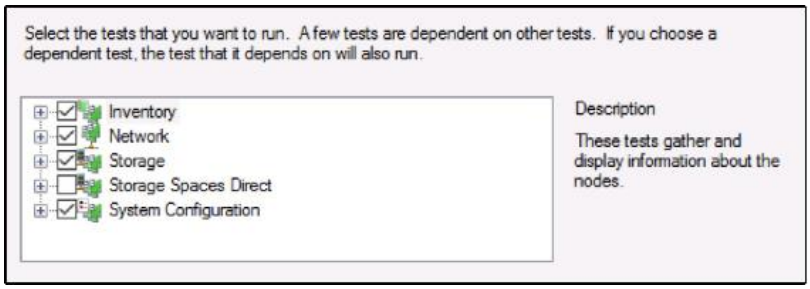


Prima di poter configurare il cluster stesso o aggiungervi qualsiasi nodo del server, dobbiamo prima convalidare la nostra configurazione hardware. Il clustering di failover è un insieme di tecnologie piuttosto complesso e ci sono molti posti in cui configurazioni errate o incongruenze potrebbero mettere di traverso l'intero cluster. Le tue intenzioni dietro la configurazione di un cluster sono ovviamente per una ridondanza affidabile, ma anche un semplice errore nella configurazione dei tuoi server membri potrebbe causare problemi abbastanza grandi che un guasto del nodo non si tradurrebbe in un ripristino automatico, il che vanifica lo scopo del cluster nel primo posto. Per assicurarci che tutte le nostre T siano incrociate e le I siano puntate, ci sono alcuni controlli di convalida completi integrati in Failover Cluster Manager, una sorta di analizzatore di best practice integrato. Questi controlli possono essere eseguiti in qualsiasi momento, prima della creazione del cluster o dopo che è stato eseguito in produzione per anni. Infatti, se mai dovessi aprire un caso di supporto con Microsoft, è probabile che la prima cosa che ti chiederanno di fare sia eseguire gli strumenti di convalida della configurazione e consentire loro di esaminare l'output.

Per avviare il processo di convalida, fare clic sul collegamento Convalida configurazione ... Siamo ora lanciati in una procedura guidata che ci consente di selezionare quali parti della tecnologia del cluster vorremmo convalidare. Ancora una volta, dobbiamo indossare i nostri limiti di pensiero teologico di gestione centralizzata Microsoft e renderci conto che questa procedura guidata non sa o non si preoccupa che sia in esecuzione su uno dei server membri che intendo far parte del cluster. Dobbiamo identificare ciascuno dei nodi del server che vogliamo scansionare per i controlli di convalida, quindi nel mio caso gli dirò che voglio convalidare i server WEB1 e WEB2:


Select Servers or a Cluster
Before You Begin
Select Servers or a Cluster
Testing Options
Confirmation
Validating
Summary
To validate a set of servers, add the names of all the servers.
To test an existing cluster, add the name of the cluster or one of its nodes.
Enter name:
Browse...
Selected servers:
WEB1.contoso.local
WEB2.contoso.local
Add
Remove

La schermata Opzioni di test ti consente di scegliere il pulsante di opzione Esegui solo i test che seleziono e sarai quindi in grado di eseguire solo determinati test di convalida. In genere, quando si configura un nuovo cluster, si desidera eseguire tutti i test in modo da poter garantire che tutto funzioni correttamente. Su un sistema di produzione, tuttavia, è possibile scegliere di limitare il numero di test eseguiti. Ciò è particolarmente vero per quanto riguarda i test sullo storage, poiché questi possono effettivamente portare il cluster temporaneamente offline mentre i test vengono eseguiti e non si vorrebbe interferire con i servizi di produzione online se non si lavora entro una finestra di manutenzione pianificata :

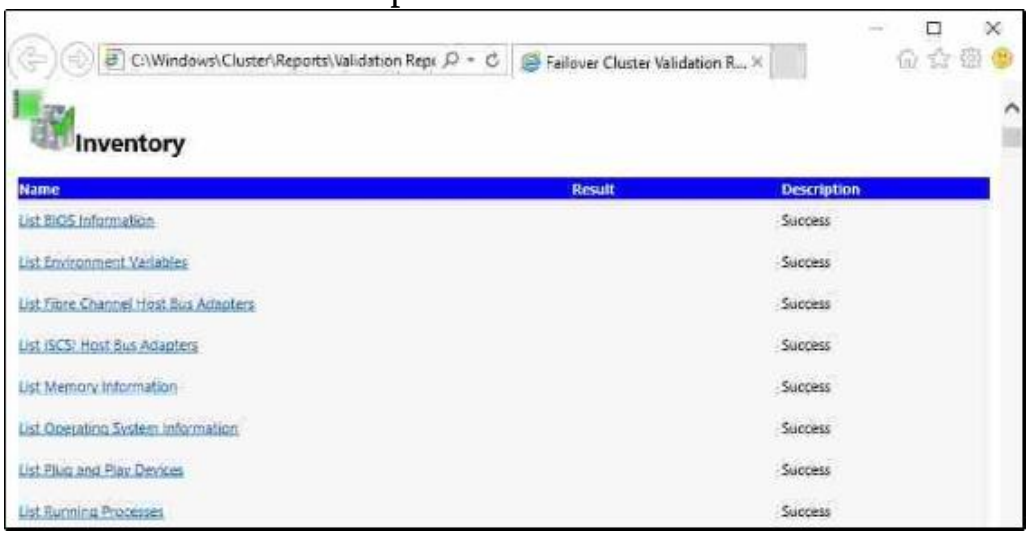


Dato che sto configurando un cluster nuovo di zecca, lascerò eseguire tutti i test. Quindi lascerò l'opzione consigliata selezionata per Esegui tutti i test (consigliato) e continuerò:

Una volta completati i test, vedrai un output di riepilogo dei loro risultati. Puoi fare clic sul pulsante Visualizza rapporto ... per vedere molti dettagli su tutto ciò che è stato eseguito. Tieni presente che ci sono tre livelli di pass / fail. Il verde è buono e il rosso è cattivo, ma il giallo è più come se funzionasse, ma non stai eseguendo le migliori pratiche. Ad esempio, ho solo una scheda NIC in ciascuno dei miei server; la procedura guidata riconosce che, affinché il mio setup sia veramente ridondante sotto tutti gli aspetti, dovrei averne almeno due. Lascerà scorrere e continuerà a

funzionare, ma mi avverte che potrei migliorare ulteriormente questo cluster aggiungendo una seconda NIC a ciascuno dei miei nodi.

Se hai bisogno di riaprire questo rapporto, o prenderne una copia dal server per conservarlo, si trova sul server in cui hai eseguito i test, in C: \ Windows \ Cluster \ Reports:



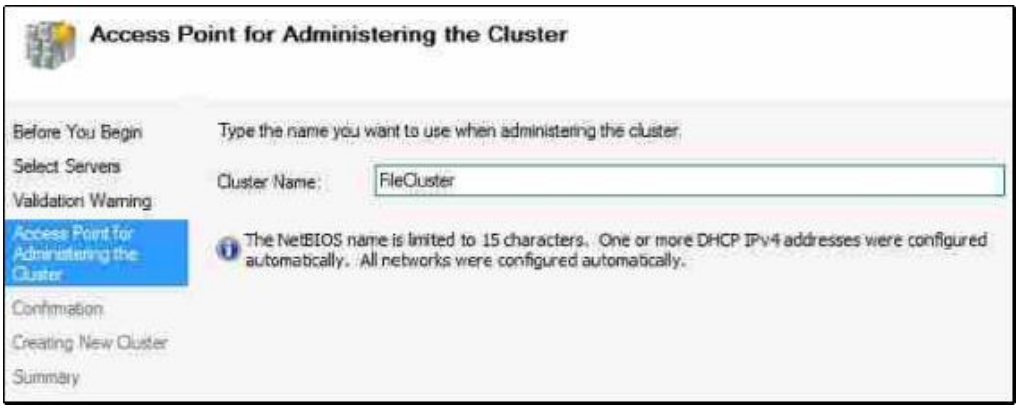
Ricorda, puoi rieseguire i processi di convalida in qualsiasi momento per testare la tua configurazione utilizzando l'attività Convalida configurazione ... all'interno di Failover Cluster Manager.

Esecuzione della procedura guidata Crea cluster

La fase di convalida potrebbe richiedere del tempo se si hanno più risultati che devono essere corretti prima di poter procedere. Ma una volta che il controllo di convalida torna pulito, sei pronto per creare il cluster. Per questo, fare clic sull'azione successiva che abbiamo a disposizione nella nostra console di Gestione cluster di failover: Crea cluster ....

Ancora una volta, dobbiamo prima specificare quali server vogliamo far parte di questo nuovo cluster, quindi inserirò i miei server WEB1 e WEB2. Dopodiché, non abbiamo molte informazioni da inserire sulla configurazione del cluster, ma una parte fondamentale delle informazioni arriva nella schermata del punto di accesso per l'amministrazione del cluster. Qui è dove si identifica il nome univoco che verrà utilizzato dal cluster e condiviso tra i server membri.

Questo è noto come un oggetto CNO (Cluster Name Object) e dopo aver completato la configurazione del cluster, vedrai questo nome apparire come un oggetto all'interno di AD:



Dopo aver terminato la procedura guidata, è possibile visualizzare il nuovo cluster all'interno dell'interfaccia di Failover Cluster Manager e visualizzare in dettaglio le funzioni più particolari all'interno di quel cluster.
Ci sono azioni aggiuntive per cose, come Configura ruolo ..., che sarà importante per impostare la funzione effettiva che questo cluster eseguirà, e Aggiungi
Nodo..., che è il tuo posto per includere ancora più server membri in questo cluster lungo la strada:

Recenti miglioramenti del clustering in Windows Server

La funzionalità di clustering esiste da un po 'di tempo, ma viene continuamente migliorata. Sono stati apportati alcuni grandi cambiamenti e aggiunte al clustering di failover nelle due ultime versioni di LTSC, Server 2016 e Server 2019. Alcune delle modifiche di cui parleremo sono state originariamente introdotte nel 2016, quindi non sono nuove di zecca, ma sono ancora rilevanti per il modo in cui gestiamo i cluster in Server 2019, quindi vale la pena menzionarli qui.

Veri cluster a due nodi con testimoni USB

Durante la configurazione del quorum per un cluster di failover, prima di Server 2019, un cluster a due nodi richiedeva tre server, poiché il server di controllo del quorum doveva risiedere su una condivisione di controllo di qualche tipo, in genere un file server separato.

A partire dal 2019, quel testimone può ora essere una semplice unità USB e non deve nemmeno essere collegato a un server Windows! Esistono molte apparecchiature di rete (switch, router e così via) che possono accettare un supporto di archiviazione file basato su USB e una chiavetta USB collegata a tale dispositivo di rete è ora sufficiente per soddisfare i requisiti per il controllo del cluster. Questa è una vittoria per il clustering avanzato in piccoli ambienti.

Maggiore sicurezza per i cluster

Sono stati apportati numerosi miglioramenti alla sicurezza al clustering di failover in Windows Server 2019. Le versioni precedenti si basavano su New Technology LAN Manager (NTLM) per l'autenticazione del traffico intra-cluster, ma molte aziende stanno adottando misure proattive per disabilitare l'uso di NTLM (all'indirizzo almeno le prime versioni) all'interno delle loro reti. Il clustering di failover ora può eseguire comunicazioni all'interno del cluster utilizzando Kerberos e certificati per la convalida di quel traffico di rete, eliminando il requisito per NTLM.

Un altro controllo di sicurezza / stabilità implementato durante la creazione di un server di controllo della condivisione file del cluster di failover è il blocco dei testimoni archiviati in DFS. La creazione di un testimone all'interno di una condivisione DFS non è mai stata supportata, ma la console in precedenza ti consentiva di farlo, il che significa che alcune aziende hanno fatto esattamente questo e ne hanno pagato il prezzo poiché ciò può causare problemi di stabilità del cluster. Gli strumenti di gestione del cluster sono stati aggiornati per verificare

l'esistenza dello spazio dei nomi DFS durante la creazione di un server di controllo remoto e non consentiranno più che ciò accada.

Clustering multisito

Posso configurare il clustering di failover tra le sottoreti? In altre parole, se ho un data center principale e affitto anche spazio da un CoLo in fondo alla strada, o ho un altro data center in tutto il paese, ci sono opzioni per impostare il clustering tra nodi che sono fisicamente separati? C'è una risposta rapida e semplice qui: sì, al clustering di failover non interessa! Con la stessa facilità con cui i nodi del server si trovassero uno accanto all'altro, il clustering può trarre vantaggio da più siti che ospitano ciascuno i propri nodi cluster e spostare i servizi avanti e indietro tra questi siti.

Clustering tra domini o gruppi di lavoro

Storicamente, siamo stati in grado di stabilire solo il clustering di failover tra i nodi che sono stati aggiunti allo stesso dominio. Windows Server 2016 offre la possibilità di spostarsi al di fuori di questa limitazione e possiamo persino creare un cluster senza che Active Directory sia affatto nel mix. In Server 2016 e 2019 puoi, ovviamente, creare ancora cluster in cui tutti i nodi sono uniti allo stesso dominio e prevediamo che questa sarà la maggior parte delle installazioni disponibili. Tuttavia, se si dispone di server aggiunti a domini diversi, è ora possibile stabilire il clustering tra quei nodi. Inoltre, i server membri in un cluster possono ora essere membri di un gruppo di lavoro e non è necessario che siano aggiunti a un dominio.

Sebbene ciò espanda le capacità disponibili del clustering di failover, presenta anche un paio di limitazioni. Quando si utilizzano cluster multidominio o gruppi di lavoro, sarà limitato solo a PowerShell come interfaccia di gestione del cluster. Se sei abituato a interagire con i tuoi cluster da uno degli strumenti della GUI, dovrai modificare il tuo limite di pensiero su questo. Sarà inoltre necessario creare un account utente locale che possa essere utilizzato dal clustering e fornirlo a ciascuno dei nodi del cluster e questo account utente deve disporre dei diritti amministrativi su tali server.

Migrazione di cluster tra domini

Sebbene la creazione di cluster su più domini sia stata possibile per alcuni anni, la migrazione di cluster da un dominio AD a un altro non era un'opzione. A partire da Server 2019, questo è cambiato. Abbiamo una maggiore flessibilità nel clustering multidominio, inclusa la possibilità di migrare i cluster tra questi domini. Questa funzionalità aiuterà gli amministratori a navigare nelle acquisizioni aziendali e nei progetti di consolidamento dei domini.

Aggiornamenti in sequenza del sistema operativo del cluster

Questa nuova funzionalità che ci è stata data nel 2016 ha un nome strano, ma è una caratteristica davvero interessante. È qualcosa progettato per aiutare coloro che utilizzano il clustering di failover per un po 'di tempo a migliorare il proprio ambiente. Se al momento stai eseguendo un cluster e quel cluster è Windows Server 2012 R2, questo è sicuramente qualcosa da esaminare. L'aggiornamento in sequenza del sistema operativo del cluster consente di aggiornare i sistemi operativi dei nodi del cluster da Server 2012 R2 a Server 2016 e quindi a Server 2019, senza tempi di inattività. Non è necessario interrompere nessuno dei servizi sui carichi di lavoro Hyper-V o SOFS che utilizzano il clustering, è sufficiente utilizzare questo processo di aggiornamento in sequenza e tutti i nodi del cluster eseguiranno la versione più recente di Windows Server. Il cluster è ancora online e attivo e nessuno sa nemmeno che sia successo. Tranne te, ovviamente.

Questo è molto diverso dal processo di aggiornamento precedente, in cui per portare il cluster al Server 2012 R2, era necessario portare il cluster offline, introdurre nuovi nodi del server che eseguono 2012 R2 e quindi ristabilire il cluster. Ci sono stati molti tempi di inattività e un sacco di grattacapi nell'assicurarsi che andasse nel modo più fluido possibile.

Il trucco che rende possibile questo aggiornamento senza interruzioni è che il cluster stesso rimane in esecuzione al livello funzionale 2012 R2, fino a quando non si emette un comando per spostarlo al livello funzionale Server 2016. Fino a quando non si emette tale comando, il clustering viene eseguito al livello funzionale precedente, anche sui nuovi nodi introdotti, che eseguono il sistema operativo Server 2016. Quando aggiorni i tuoi nodi uno alla volta, gli altri nodi che sono ancora attivi nel cluster rimangono online e continuano a servire gli utenti e le applicazioni, quindi tutti i sistemi funzionano normalmente dal punto di vista del carico di lavoro. Quando si introducono nuovi box Server 2016 nel cluster, iniziano a servire carichi di lavoro come i server 2012 R2, ma lo fanno a un livello funzionale 2012 R2. Questo è indicato come modalità mista. Ciò ti consente di rimuovere anche l'ultima scatola 2012 R2, cambiarlo nel 2016 e reintrodurlo, il tutto senza che nessuno lo sappia. Quindi, una volta completati tutti gli aggiornamenti del sistema operativo, eseguire il problema
il comando di PowerShell Update-ClusterFunctionalLevel per capovolgere il funzionale livello e si dispone di un cluster Windows Server 2016 che è stato aggiornato senza problemi con tempi di inattività pari a zero.

Resilienza della macchina virtuale

Come puoi dedurre con successo dal nome, la resilienza della macchina virtuale è un miglioramento nel clustering che avvantaggia specificamente i cluster di server Hyper-V. Ai tempi del clustering di Server 2012 R2, non era raro avere problemi di comunicazione intra-array o intra-cluster. Questo a volte si rappresentava in un guasto temporaneo, il che significa

che il cluster pensava che un nodo stesse andando offline quando in realtà non lo era, e avrebbe avviato un failover che a volte causava più tempi di inattività rispetto a se i modelli di riconoscimento di un errore reale avessero semplicemente stato un po 'meglio in primo luogo. Per la maggior parte, il clustering e il failover dei nodi del cluster hanno funzionato correttamente, ma c'è sempre spazio per miglioramenti. Questo è lo scopo della resilienza delle macchine virtuali. È ora possibile configurare le opzioni per la resilienza, dandoti la possibilità di definire in modo più specifico quale comportamento assumeranno i tuoi nodi durante i guasti dei nodi del cluster. È possibile definire cose come il livello di resilienza, che indica al cluster come gestire gli errori. Puoi anche impostare il tuo periodo di resilienza, ovvero il periodo di tempo in cui le VM possono essere eseguite in uno stato isolato.

Un altro cambiamento è che i nodi non integri del cluster vengono ora messi in quarantena per un periodo di tempo definito dall'amministratore. Non sono autorizzati a ricongiungersi al cluster finché non sono stati identificati come integri e hanno atteso il loro periodo di tempo, prevenendo situazioni come un nodo bloccato in un ciclo di riavvio che si ricongiunge inavvertitamente al cluster e causa problemi continui durante il ciclo su e giù .

Replica archiviazione (SR)

SR è un nuovo modo per sincronizzare i dati tra i server. È una tecnologia di replica dei dati che fornisce la capacità di replica dei dati a livello di blocco tra i server, anche su diversi siti fisici. SR è un tipo di ridondanza che non avevamo visto in una piattaforma Microsoft prima di Windows Server 2016; in passato, dovevamo fare affidamento su strumenti di terze parti per questo tipo di funzionalità. È anche importante discutere di SR sulla scia del clustering di failover, perché SR è la salsa segreta che consente il clustering di failover multisito. Quando si desidera ospitare nodi del cluster in più posizioni fisiche, è necessario un modo per assicurarsi che i dati utilizzati da tali nodi del cluster siano sincronizzati continuamente, in modo che sia effettivamente possibile un failover. Questo flusso di dati è fornito da SR.

Uno dei punti dati chiari su SR è che finalmente consente a una soluzione per un unico fornitore, che ovviamente è Microsoft, di fornire la tecnologia e il software end-to-end per l'archiviazione e il clustering. È anche indipendente dall'hardware, dandoti la possibilità di utilizzare le tue preferenze per il supporto di memorizzazione.

SR è pensato per essere strettamente integrato e una delle tecnologie di supporto di un solido ambiente di clustering di failover. In effetti, l'interfaccia di gestione grafica per SR si trova all'interno del software Failover Cluster Manager, ma è ovviamente configurabile anche tramite PowerShell, quindi assicurati di dare un'occhiata a Clustering di failover e SR come una storia insieme migliore per il tuo ambiente.

Aggiornato con Windows Server 2019 è il fatto che SR è ora disponibile all'interno di Server 2019 Standard Edition! (In precedenza, richiedeva Datacenter, che era proibitivo per alcune implementazioni.)
L'amministrazione di SR è ora disponibile anche nel nuovo Windows Admin Center (WAC).

Spazi di archiviazione diretta (S2D)

S2D è una tecnologia di clustering, ma lo elenco qui separatamente dal clustering di failover generale perché S2D è un componente fondamentale del data center definito dal software (SDDC) e si è concentrato così tanto sui miglioramenti negli ultimi anni che è davvero in una categoria a sé stante.

In poche parole, S2D è un modo per costruire una piattaforma di archiviazione centralizzata basata su rete estremamente efficiente e ridondante, interamente da server Windows. Pur servendo lo stesso scopo generale (archiviazione di file) di un dispositivo NAS o SAN tradizionale, S2D adotta un approccio completamente diverso in quanto non richiede hardware specializzato, né cavi speciali o connettività tra i nodi del cluster S2D.

Per creare S2D, tutto ciò di cui hai bisogno sono i server Windows; più veloce è, meglio è, ma potrebbero essere normali server di tutti i giorni. Questi server devono essere collegati tramite rete, ma non ci sono requisiti speciali qui; semplicemente si connettono tutti a una rete, proprio come qualsiasi altro server nel tuo ambiente. Dopo aver eseguito questi server, è possibile utilizzare le tecnologie di clustering o il nuovo WAC per associare questi server in array S2D.

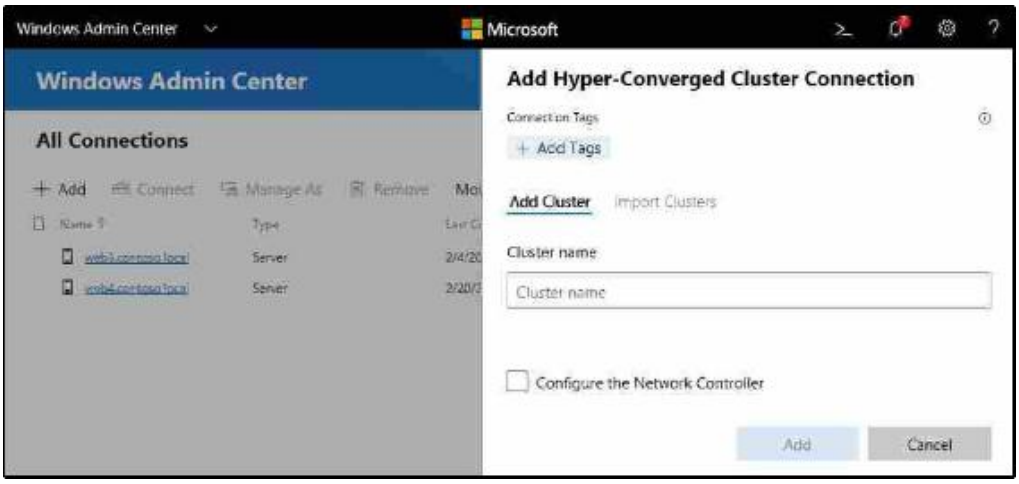
S2D fa parte della storia generale dell'infrastruttura iperconvergente (HCI) ed è un modo meraviglioso per fornire uno storage estremamente veloce e protetto per qualsiasi cosa, ma soprattutto per i carichi di lavoro come i cluster di server Hyper-V. Come già sapete, durante la creazione di un cluster di server Hyper-V, i nodi di quel cluster devono avere accesso all'archiviazione condivisa su cui risiederanno i file del disco rigido della macchina virtuale. S2D è il modo migliore per fornire tale archiviazione centralizzata.

S2D prenderà i dischi rigidi all'interno dei server dei nodi del cluster S2D e combinerà tutto il loro spazio insieme in pool di archiviazione definiti dal software. Questi pool di archiviazione sono configurati con funzionalità di memorizzazione nella cache e persino tolleranza agli errori

incorporata. Ovviamente non vorresti che un singolo nodo S2D, o anche un singolo disco rigido offline, causasse un intoppo alla tua soluzione S2D, e ovviamente Microsoft non vuole che ciò accada. Pertanto, quando si raggruppano i server e tutti i loro dischi rigidi in questi grandi pool di archiviazione S2D, vengono automaticamente configurati con parità tra quelle unità in modo che i componenti particolari che vanno offline non causino la perdita di dati o addirittura rallentino il sistema.

S2D è la migliore piattaforma di archiviazione per cluster SOFS e Hyper-V.

Mentre S2D basato su Server 2016 è stato configurato principalmente tramite PowerShell (il che purtroppo significa che molti amministratori non l'hanno ancora provato), Windows Server 2019 ci offre il nuovo set di strumenti WAC e ora WAC include opzioni integrate per la configurazione di un S2D ambiente:



S2D è una di quelle tecnologie che garantisce il proprio libro, ma chiunque desideri provare o iniziare con questa straordinaria tecnologia di archiviazione dovrebbe iniziare da https: //documenti. microsoft.com /en-noi/finestre-server/Conservazione/Conservazione-spazi /Conservazione-spazi-diretto-panoramica.

Novità in Server 2019

Per quelli di voi che hanno già familiarità con il concetto di S2D e vogliono sapere cosa c'è di nuovo o di diverso nel gusto Server 2019, ecco alcuni dei miglioramenti che sono arrivati con questa ultima versione del sistema operativo:

- **Uso migliorato dei volumi Resilient File System (ReFS)**: Ora abbiamo funzioni di deduplicazione e compressione sui volumi ReFS ospitati da S2D. Testimone USB: ne abbiamo già discusso brevemente, quando si utilizza un testimone per supervisionare un cluster S2D costituito da solo due nodi, ora è possibile utilizzare una chiave USB collegato a un'apparecchiatura di rete, piuttosto che eseguire un terzo server per questo scopo di testimonianza.
- **WAC**: WAC ora include strumenti e funzionalità per la definizione e la gestione dei cluster S2D. Ciò renderà l'adozione molto più semplice per le persone che non hanno molta familiarità con PowerShell.

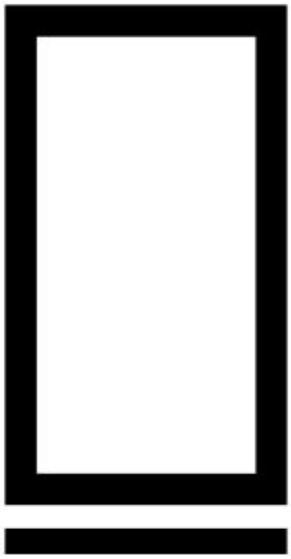
- **Capacità migliorata**: Ora possiamo ospitare quattro petabyte per cluster.
- **Velocità migliorata**: Sebbene S2D sia stato veloce sin dalla prima versione, abbiamo alcuni miglioramenti in termini di efficienza in Server 2019. Alla conferenza Ignite dello scorso anno, Microsoft ha presentato un cluster S2D a 8 nodi in grado di raggiungere 13.000.000 di IOP. Santo cielo!

Sommario

La ridondanza è una componente fondamentale nel modo in cui pianifichiamo l'infrastruttura e creiamo server nel mondo di oggi. Windows Server 2019 ha alcune potenti funzionalità integrate che puoi utilizzare nei tuoi ambienti, a partire da oggi! Spero che raccogliendo un po 'più di informazioni su NLB e clustering di failover, sarai in grado di espandere le capacità della tua organizzazione impiegando queste tecniche e estendendo i limiti del tempo di attività del servizio. A mio parere, se c'è una strada da seguire in questo capitolo, è iniziare a costruire il proprio HCI utilizzando S2D e il clustering di failover per creare resilienza nella propria infrastruttura Hyper-V. HCI cambierà letteralmente il tuo modo di lavorare e ti darà una tranquillità che non pensavi fosse possibile in un mondo che mira al 99. Tempo di attività del 999%. Nel prossimo capitolo esamineremo PowerShell.

Domande

1. Quale tecnologia è più appropriata per rendere ridondante il traffico del server web: bilanciamento del carico di rete o clustering di failover?
2. In Bilanciamento carico di rete, cosa significano gli acronimi DIP e VIP?
3. Quali sono le tre modalità NLB?
4. In Windows Server 2019, "Bilanciamento carico di rete" è un ruolo o una funzionalità?
5. Quali ruoli vengono utilizzati più spesso con il clustering di failover?
6. Che tipo di dispositivo di piccole dimensioni può ora essere utilizzato come testimone del quorum del cluster (questo è nuovo di zecca a partire da Server 2019)?
7. Vero o falso: Spazi di archiviazione diretta richiede l'utilizzo di dischi rigidi SSD.



PowerShell

Siamo onesti, molti di noi usano ancora il prompt dei comandi su base giornaliera. Se hai tagliato e stai utilizzando il nuovo prompt di PowerShell in sostituzione totale del prompt dei comandi, ti applaudo! Tuttavia, tendo ancora ad aprire cmd.exe per abitudine, anche se con le versioni più recenti di Windows 10 e Windows Server 2019, sto decisamente facendo uno sforzo più consapevole per utilizzare il più recente, più blu, più carino e un'interfaccia più potente che è PowerShell. In questo capitolo, esploreremo alcuni dei motivi per cui dovresti farlo anche tu. Oltre al fatto che Microsoft sembra aver ridotto la dimensione del testo predefinita nel prompt dei comandi per dissuaderci dall'usarlo, cosa che trovo piuttosto divertente,

n questo capitolo tratteremo i seguenti argomenti: Perché passare a PowerShell?

- Lavorare in PowerShell
- Ambiente di scripting integrato

PowerShell Gestione remota di un server

- Configurazione dello stato desiderato

Perché passare a PowerShell?

Non credo che ci siano dubbi nella mente delle persone sul fatto che PowerShell sia davvero l'evoluzione del prompt dei comandi, ma il motivo per cui molti di noi utilizzano ancora la vecchia interfaccia è che ha ancora tutte le capacità per realizzare ciò di cui abbiamo bisogno fare sui nostri server. Ciò che contiene davvero il prompt dei comandi è la capacità di fare le stesse cose che abbiamo sempre fatto dal prompt dei comandi e nient'altro. Senza rendersene conto, ci sono molte funzioni che usi la GUI per realizzare che non possono essere eseguite bene dall'interno di una finestra del prompt dei comandi.

Le limitazioni all'interno del prompt dei comandi che ti costringono a utilizzare il mouse per l'interfaccia con la GUI non esistono con PowerShell. È completamente completo e in grado di modificare quasi tutti gli aspetti del sistema operativo Windows. In che modo PowerShell è diventato molto più potente del prompt dei comandi? Si differenzia da qualsiasi shell I / O classica in quanto è costruita su .NET e funziona molto più come un linguaggio di programmazione che come semplici comandi di input e output.

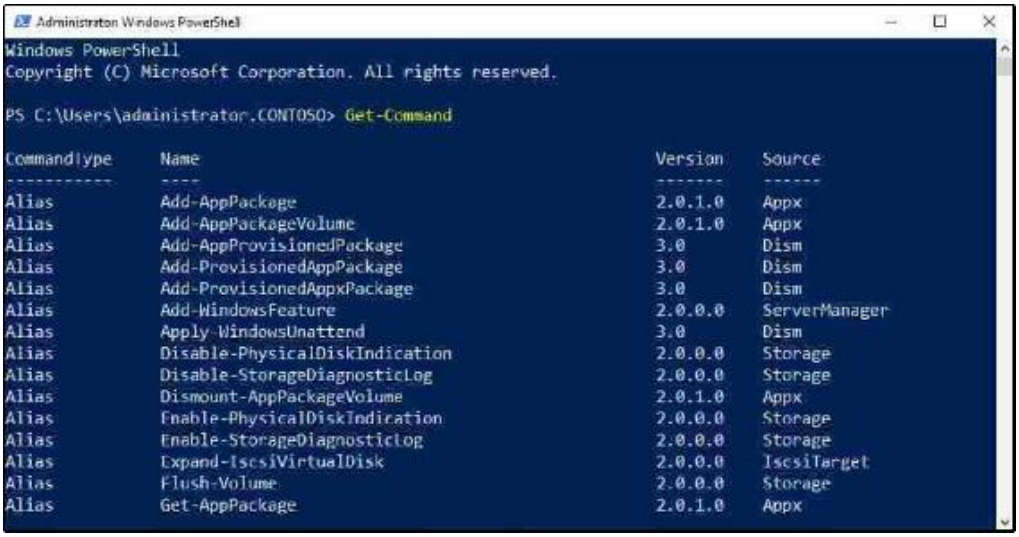
Cmdlet

La maggior parte delle funzionalità che un amministratore di server tradizionale utilizzerà si presenta sotto forma di cmdlet (pronunciato command-let). Questi sono comandi che esegui dal prompt di PowerShell, ma puoi pensarli come strumenti piuttosto che come semplici comandi. I cmdlet possono essere utilizzati sia per ottenere informazioni da un server sia per impostare informazioni e parametri su un server. Molti cmdlet hanno nomi intuitivi che iniziano con get o set e, in modo simile al modo in cui funzionano la maggior parte delle interfacce della riga di comando, ogni cmdlet ha varie opzioni o variabili che possono essere configurate e contrassegnate alla fine del cmdlet, in modo da renderlo fare cose speciali. È utile comprendere che i cmdlet sono sempre costruiti in una sintassi verbo-nome. Si specifica l'azione che si desidera eseguire, ad esempio ottenere o impostare, e poi il tuo nome è il pezzo all'interno di Windows che stai cercando di manipolare. Di seguito sono riportati alcuni semplici esempi di cmdlet in PowerShell per darti un'idea di come appaiono e di come vengono denominati in modo abbastanza semplice:

- Get-NetIPAddress : Con questo cmdlet, possiamo vedere gli indirizzi IP sul nostro sistema.
- Set-NetIPAddress : Possiamo usare questo ragazzo per modificare un indirizzo IP esistente. New-NetIPAddress : Questo cmdlet ci consente di creare un nuovo indirizzo IP sul computer.

- Rinomina computer : Come abbiamo visto in precedenza nel libro, Rinomina computer è un veloce e un modo semplice per impostare il nome host del computer di un sistema.

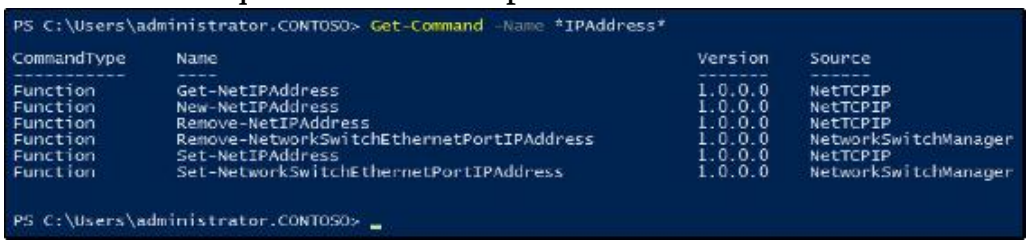
Se hai difficoltà a trovare il nome o la sintassi di un particolare comando, il sito Web di Documenti in linea di Microsoft (in precedenza e talvolta ancora chiamato TechNet) ha una pagina completa di informazioni dedicate a ciascun cmdlet all'interno di PowerShell. Questo può essere incredibilmente utile, ma a volte non vuoi prenderti il tempo di fare un salto su Internet solo per trovare il nome di un comando che semplicemente non riesci a ricordare al momento. Uno dei cmdlet più utili in PowerShell mostra un elenco di tutti i cmdlet disponibili. Assicurati di controllare Get-Command:



Whoa, ci sono pagine e pagine e pagine di cmdlet! Piuttosto che scorrere l'intero elenco per trovare quello che stai cercando, è facile filtrare questo elenco in base ai criteri che desideri. Se fossimo interessati a vedere solo i comandi che si occupano di indirizzamento IP, potremmo provare:

Get-Command -Name * IPAddress *

Il cmdlet Get-Command combinato con il parametro -Name consente di eseguire selettivamente cercare elementi utili in PowerShell che si riferiscono a qualsiasi nome o parte di un nome:



PowerShell è la spina dorsale

Come scoprirai in questo capitolo, l'interfacciamento con PowerShell mette tutti i tipi di potenza a portata di mano. Quello che a volte troviamo, tuttavia, è che gli amministratori non si fidano completamente di PowerShell, perché sono abituati a eseguire queste azioni e ad apportare queste modifiche da un'interfaccia grafica. Dopo aver eseguito un singolo cmdlet di PowerShell per impostare una configurazione che avrebbe richiesto una dozzina di clic del mouse diversi per ottenere la stessa operazione, è facile pensare che in realtà non deve aver fatto nulla. Era troppo facile e ha elaborato il mio comando troppo rapidamente, giusto? Farei comunque meglio ad accedere a quell'interfaccia grafica, solo per ricontrollare che PowerShell abbia effettivamente svolto il lavoro.

Quando ho iniziato a utilizzare PowerShell, ero tentato di fare esattamente questo, sempre. Ma più l'ho usato e più ho iniziato a scavare in quelle stesse interfacce grafiche, più mi sono reso conto che non sono l'unico a usare PowerShell. Molte delle GUI dello strumento di amministrazione utilizzano anche PowerShell! Senza nemmeno rendertene conto, usi PowerShell per alcune attività all'interno del sistema operativo Windows Server. Quando apri quella console di gestione per qualunque cosa tu stia cambiando sul server, effettui le tue configurazioni e poi fai clic sul pulsante Vai o Fine, come fa quella console grafica a mettere in atto la tua configurazione? PowerShell. Dietro le quinte, in background, la console prende le informazioni che inserisci, inserendo tali informazioni nei cmdlet di PowerShell, ed eseguirli per eseguire l'effettivo lavoro di configurazione. Molti degli strumenti di amministrazione che eseguiamo dall'interno di Server Manager adottano questo approccio, accettando modifiche e configurazioni da te e quindi formulando tali impostazioni in comandi di PowerShell che vengono eseguiti in background per rendere effettive le modifiche.

Quindi, se esiti a iniziare a utilizzare PowerShell perché sembra diverso o non ti fidi che il processo sia uniforme rispetto al modo in cui avrebbe funzionato nella GUI, dimentica tutto questo. Perché spesso quando si

utilizzano i clic del mouse per modificare le impostazioni sul server, si richiamano effettivamente i cmdlet di PowerShell.

Scripting

Più usi PowerShell, più potente diventa. Oltre a eseguire singoli comandi e cmdlet ad hoc, è possibile creare script estesi in grado di eseguire tutti i tipi di operazioni diverse. Ho detto che PowerShell ha somiglianze con un normale linguaggio di programmazione e lo script è il punto in cui iniziamo a navigare in quel territorio. PowerShell offre la possibilità di creare file di script, cosa che faremo da soli a breve, salvando gli script per una facile esecuzione di quegli stessi script più e più volte. Le variabili possono anche essere utilizzate, come in altre forme di codifica, in modo da poter fornire input variabili e oggetti che possono essere utilizzati dagli script, al fine di renderli più flessibili e spremere ancora più funzionalità da essi.

Server Core

Se ci fosse un'area in cui penso che noi amministratori di server potremmo fare un lavoro migliore nell'utilizzo della tecnologia a nostra disposizione, sta usando PowerShell per soddisfare il modello Microsoft di gestione centralizzata. Quando abbiamo un'attività che deve essere eseguita su un server, è nostra tendenza predefinita accedere a quel server (di solito tramite RDP), quindi utilizzare il mouse per iniziare a fare clic e fare il lavoro. L'accesso al server sta diventando sempre più inutile e potremmo risparmiare molto tempo utilizzando gli strumenti di gestione centrale a nostra disposizione. PowerShell è uno di questi strumenti. Invece di eseguire RDP in quel server, usa semplicemente il prompt di PowerShell sul tuo computer locale per raggiungere e modificare tale impostazione sul server remoto.

Questo tipo di gestione remota diventa non solo efficiente ma necessaria, poiché iniziamo a occuparci maggiormente di server headless. Spero di vedere un maggiore utilizzo di Server Core nelle nostre organizzazioni nei prossimi anni e l'interazione con questi server richiederà un cambiamento nella tua mentalità amministrativa. Acquisendo familiarità con l'esecuzione delle attività quotidiane dall'interno di PowerShell ora, ti attrezzerai meglio per l'amministrazione futura di queste macchine headless, che richiederanno di interfacciarle in modo diverso da come ti senti a tuo agio oggi.

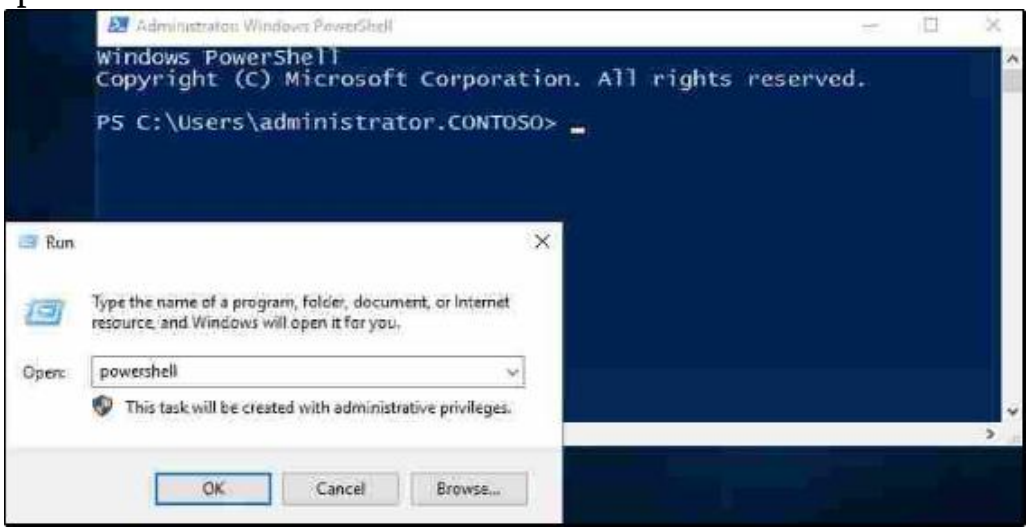
Lavorare in PowerShell

Il primo passo per eseguire un lavoro reale con PowerShell è acquisire familiarità con l'interfacciamento con la piattaforma e acquisire familiarità con le routine quotidiane di lavoro da questa riga di comando, piuttosto che fare affidamento sul puntatore del mouse. Qui, esploreremo alcuni dei modi più comuni in cui ho visto gli amministratori di server utilizzare PowerShell per migliorare il loro carico di lavoro quotidiano.

Avvio di PowerShell

Abbastanza semplice: la prima cosa che dobbiamo fare è aprire PowerShell per iniziare a usarlo. La console di PowerShell è installata per impostazione predefinita in tutte le versioni recenti di Windows, quindi puoi eseguirla dal menu Start, aggiungerla al desktop o accedervi in qualsiasi modo in cui normalmente apri qualsiasi applicazione.

Poiché tendo a preferire usare la mia tastiera per tutto, il modo in cui normalmente apro PowerShell è tenere premuto il tasto WinKey e premere R per aprire un prompt Esegui, digitare la parola powershell e premere Invio:



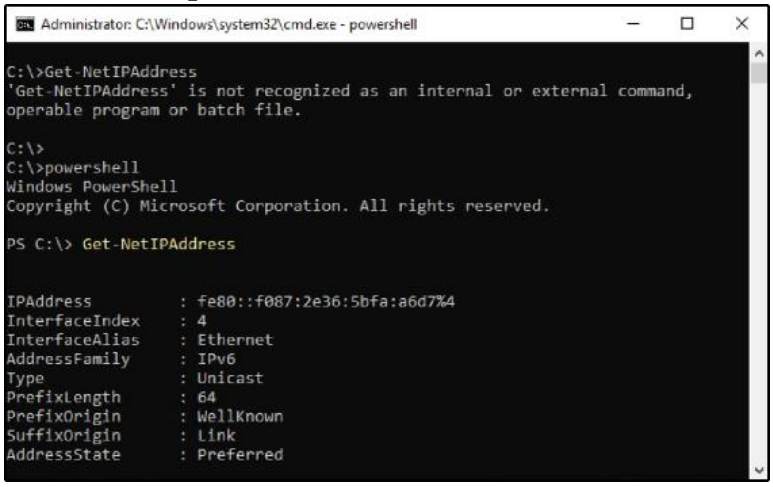
Come puoi vedere, poiché ho effettuato l'accesso a un account amministrativo sul mio server, il mio prompt di PowerShell è stato aperto con autorizzazioni elevate. Ciò è visibile nel fatto che la parola Amministratore è elencata nella barra degli strumenti superiore della finestra di PowerShell. È importante notare che, proprio come il prompt dei comandi, è possibile aprire un prompt di PowerShell con autorizzazioni utente normali o privilegi di amministratore elevati. In genere è più sicuro lavorare all'interno di una normale sessione di PowerShell che non dispone di diritti elevati, a meno che l'attività che si sta tentando di eseguire non richieda tali autorizzazioni aggiuntive.

Un altro modo semplice e veloce per aprire PowerShell su qualsiasi piattaforma Windows più recente è fare clic con il pulsante destro del mouse sul pulsante Start e selezionarlo direttamente dall'elenco delle attività rapide che viene presentato. Come puoi vedere nello screenshot seguente, ho fatto clic con il pulsante destro del mouse sul pulsante Start di una delle mie nuove caselle Server 2019 e posso scegliere da qui di aprire PowerShell o anche un prompt di PowerShell elevato (amministrativo):

Se fai clic con il pulsante destro del mouse sul pulsante Start e non trovi le opzioni per PowerShell, ma piuttosto per aprire il prompt dei comandi, non essere sgomento. Questa è un'opzione configurabile; puoi mostrare le opzioni Prompt dei comandi o PowerShell nel menu delle attività di amministrazione rapide. Se fai clic con il pulsante destro del mouse sulla barra delle applicazioni e selezioni le impostazioni della barra delle applicazioni, troverai un'opzione chiamata Sostituisci prompt dei comandi con Windows PowerShell nel menu quando faccio clic con il pulsante destro del mouse sul pulsante di avvio o premo il tasto Windows + X. La commutazione di questa opzione farà oscillare il menu di amministrazione rapido avanti e indietro tra le due interfacce della riga di comando.

Hai anche la possibilità di accedere a un prompt di PowerShell dall'interno di una finestra del prompt dei comandi esistente. Normalmente, quando si lavora dal prompt dei comandi, non è possibile utilizzare alcun cmdlet di PowerShell. Andiamo avanti e proviamo. Aprire una finestra del prompt dei comandi di amministrazione e provare a digitare il nome di uno dei cmdlet menzionati in precedenza. Forse digita Get-NetIPAddress per mostrarci quali indirizzi IP risiedono su questo sistema. Spiacenti, non è riuscito perché il prompt dei comandi non riconosce il cmdlet Get-NetIPAddress.

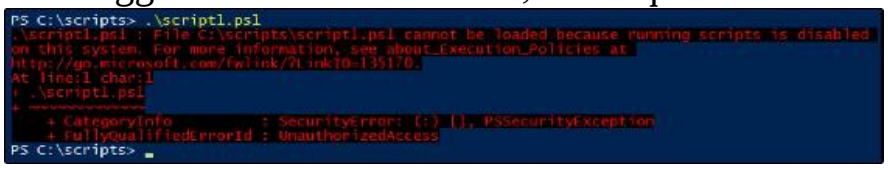
Ora digitapowershell e premere Invio. Invece di aprire una finestra di PowerShell separata, il prompt cambia ma la finestra dell'applicazione stessa rimane la stessa. Ora sei entrato nella shell di PowerShell dall'interno della finestra nera del prompt dei comandi e puoi iniziare a utilizzare i cmdlet come desideri. L'esecuzione di Get-NetIPAddress di nuovo ora produce alcune informazioni:



È possibile tornare dalla modalità PowerShell alla modalità normale del prompt dei comandi digitando exit.

Criterio di esecuzione predefinito

Quando lavori direttamente con l'interfaccia della riga di comando di PowerShell, puoi semplicemente aprire PowerShell, iniziare a digitare i cmdlet e iniziare a lavorare. Tuttavia, uno dei grandi vantaggi dell'utilizzo di PowerShell arriva quando inizi a giocare con la creazione, il salvataggio e l'esecuzione di script. Se apri PowerShell, crei uno script e poi provi a eseguirlo, a volte scoprirai che non riesce con un grande messaggio di errore disordinato, come questo:



Ciò non dovrebbe accadere su una nuova istanza di Windows Server 2019, ma potrebbe accadere se sono presenti oggetti Criteri di gruppo applicati al nuovo server o se si utilizza un sistema operativo diverso e si sta tentando di eseguire alcuni script di PowerShell; potresti trovarti bloccato in uno di questi messaggi di errore appena fuori dal cancello. Mentre la natura di alcune versioni di Windows per bloccare l'esecuzione di script per impostazione predefinita è un miglioramento della sicurezza, può essere un fastidio aggirare quando si cerca di fare qualcosa. Per fortuna, se riscontri questo problema, la risoluzione è semplice: devi semplicemente regolare il Default Execution Policy (DEP) all'interno di PowerShell, in modo che consenta l'esecuzione degli script correttamente.

Questo non è un semplice interruttore ON / OFF. Esistono cinque diversi livelli all'interno del DEP ed è importante comprenderli ciascuno in modo da poter impostare il DEP di conseguenza, in base alla sicurezza che si desidera applicare sui server. Ecco le descrizioni di ogni livello, in ordine dal più sicuro al meno sicuro.

Limitato

Il criterio Restricted consente l'esecuzione di comandi e cmdlet, ma interrompe del tutto l'esecuzione degli script.

AllSigned

Ciò richiede che qualsiasi script in esecuzione debba essere firmato da un editore attendibile. Quando è impostato su AllSigned, anche gli script che scrivi tu stesso dovranno essere sottoposti a quel processo di convalida e firmati prima che possano essere eseguiti.

RemoteSigned

RemoteSigned è il criterio predefinito in Windows Server 2019. Per gli script che sono stati scaricati da Internet, è necessario che questi script siano firmati con una firma digitale da un editore di cui ti fidi.

Tuttavia, se scegli di creare i tuoi script, consentirà l'esecuzione di questi script locali senza richiedere la firma digitale.

Senza restrizioni

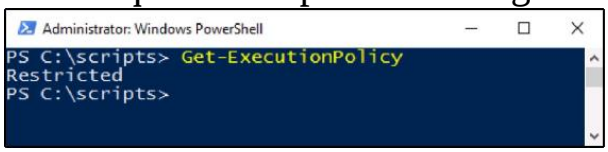
Gli script possono essere eseguiti, firmati o non firmati. Viene comunque visualizzato un messaggio di avviso durante l'esecuzione di script scaricati da Internet.

La modalità Bypass

In modalità Bypass, nulla viene bloccato e non vengono forniti avvisi quando si eseguono script. In altre parole, sei da solo.

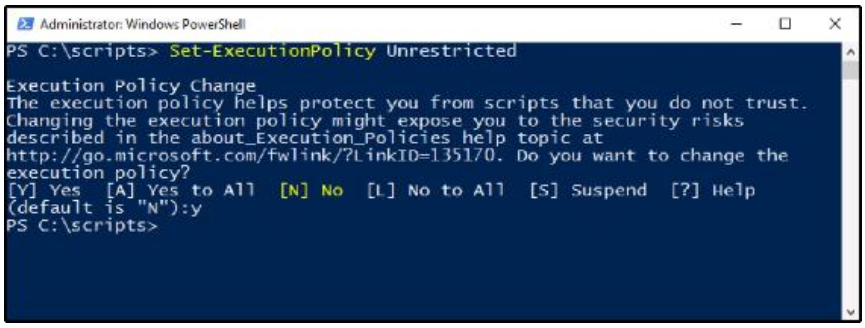
A volte un singolo criterio di esecuzione non soddisfa tutte le tue esigenze, a seconda di come utilizzi gli script di PowerShell. I DEP possono essere ulteriormente migliorati impostando un ambito dei criteri di esecuzione che consente di impostare diversi criteri di esecuzione per diversi aspetti del sistema. Ad esempio, i tre ambiti che è possibile manipolare sono Process, CurrentUser e LocalMachine. Per impostazione predefinita, il DEP influisce su LocalMachine in modo che tutti gli script in esecuzione aderiscano al DEP. Ma se è necessario modificare questo comportamento in modo che diversi DEP siano impostati per CurrentUser o anche per un singolo processo, si ha la possibilità di farlo.

Se non si è sicuri dello stato corrente del DEP o si sospetta che qualcuno possa averlo modificato, è possibile visualizzare facilmente il criterio di esecuzione attualmente assegnato con un semplice cmdlet chiamato Get-ExecutionPolicy. Come puoi vedere nell'immagine seguente, il mio è impostato su Restricted, il che spiega il mio precedente messaggio di errore quando ho provato a eseguire uno script:



Dopo aver deciso il livello di DEP che si desidera sul server o sulla workstation, è possibile impostarlo di conseguenza con un rapido cmdlet. Ad esempio, poiché questo è un laboratorio di prova e desidero che gli script possano essere eseguiti e non sono molto preoccupato per la sicurezza poiché sono isolato, cambierò il mio in Unrestricted. Ecco il mio comando per fare proprio questo:

Set-ExecutionPolicy Unrestricted


Administrator: Windows PowerShell
PS C:\scripts> Set-ExecutionPolicy Unrestricted
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust.
Changing the execution policy might expose you to the security risks
described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the
execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "N"):y
PS C:\scripts>

Ricorda, in questo momento stiamo eseguendo PowerShell su questo sistema locale (mi è capitato di essere connesso al mio server WEB3), quindi l'unico criterio di esecuzione che sto impostando è quello locale per il mio sistema WEB3. Se volessi modificare questa impostazione a livello globale o per un gruppo di macchine contemporaneamente, potrei utilizzare Criteri di gruppo per tale modifica. La posizione all'interno di Criteri di gruppo per la configurazione dei criteri di esecuzione degli script di PowerShell è Configurazione computer | Politiche | Modelli amministrativi | Componenti di Windows | Windows PowerShell | Attiva l'esecuzione dello script.

Utilizzando il tasto Tab

Prima di iniziare a navigare all'interno di PowerShell, c'è una cosa importante che voglio sottolineare: abituati a premere il tasto Tab quando sei all'interno del prompt di PowerShell! Se si digitano le prime lettere di qualsiasi comando o cmdlet e quindi si preme Tab, il resto del nome del cmdlet verrà automaticamente popolato sullo schermo.

Se digitiamo get-co e quindi premiamo Tab, il prompt popola automaticamente il cmdlet Get-Command completo. Poiché sono presenti più cmdlet che iniziano con get-co, se premi Tab più volte puoi vedere che scorre tutti i cmdlet disponibili che iniziano con quelle lettere.

Tab funziona anche con i nomi di file e cartelle. Ad esempio, ho scaricato un hotfix che deve essere installato su un server. Voglio avviare questo hotfix utilizzando il prompt di PowerShell che ho già aperto, ma non voglio spendere un intero minuto o più cercando di digitare l'enorme nome del file di questo hotfix. Sono già passato alla cartella in cui risiede il mio hotfix e ora se digito semplicemente le prime lettere del nome del file e premo il tasto Tab, PowerShell popolerà il resto del nome del file. Da lì, tutto ciò che dobbiamo fare è premere Invio per avviare il programma di installazione:

Cmdlet utili per le attività quotidiane

Quando ho iniziato a incorporare PowerShell nel mio flusso di lavoro quotidiano, ho trovato utile tenere a portata di mano un elenco di comandi e cmdlet di uso comune. Fino a quando non si arriva al punto in cui vengono memorizzati e una seconda natura, se non si dispone di un modo semplice e veloce per richiamare quei comandi, è probabile che non li utilizzerai e tornerai al vecchio metodo di configurazione del tuo server. Di seguito è riportato un elenco di alcuni degli elementi che utilizzo regolarmente durante la creazione di server. Alcuni sono comandi tradizionali che funzionerebbero anche da un prompt dei comandi e alcuni sono cmdlet, ma sono tutti utili quando si lavora all'interno di una finestra di PowerShell:

- Get-Command: è utile per trovare comandi o cmdlet aggiuntivi che potresti voler eseguire o cercare.
- Get-Command -Name * esempio * : Migliora l'utilità di Get-Command di aggiungendo il -Nome passare alla fine di esso, in modo da poter filtrare i risultati in base a qualsiasi tipo di cmdlet che si sta cercando.
- GC: Questo è semplicemente un breve alias per Get-Command. Volevo solo sottolineare questo perch é alcuni dei cmdlet di PowerShell hanno alias, come gcm, che consentono di avviare questi cmdlet di uso comune con meno sequenze di tasti.
- Get-Alias: poich é abbiamo appena menzionato l'alias GCM per Get-Command, potresti chiederti quali altri alias sono disponibili all'interno di PowerShell. Per visualizzare un elenco completo, è sufficiente collegare il cmdlet Get-Alias.
- Rinomina computer : Consente di impostare un nuovo nome host per il server.
- Aggiungi computer : Usa il Aggiungi computer cmdlet per unire server o computer a un file dominio.
- Nome host: mostra il nome del sistema su cui stai attualmente lavorando. Uso sempre il nome host per assicurarmi di lavorare davvero sul server che penso di essere. Hai mai riavviato il server

sbagliato? Io ho. Eseguendo un rapido comando hostname, puoi stare tranquillo che la funzione che stai per eseguire sta realmente accadendo sul sistema corretto.

- $ env: nomecomputer: questo ti presenta il nome host del sistema su cui stai lavorando, ma lo chiamo per mostrare che PowerShell pu ò facilmente attingere alle variabili d'ambiente per estrarre le informazioni. Il

il comando hostname più semplice è utile quando si è connessi a un sistema locale e stanno semplicemente cercando di verificarne il nome, ma la capacità di estrarre informazioni da una variabile, come $ env: nomecomputer, sarà molto più utile quando si creano script o si tenta di eseguire una funzione su un sistema remoto.

- Logoff: il nome è autoesplicativo, Logoff ti disconnette dal sistema. Anziché cercare di trovare la funzione di disconnessione facendo clic all'interno del menu Start del server, è possibile lanciare un rapido comando di disconnessione in un prompt dei comandi o in una finestra di PowerShell e ti disconnetterà immediatamente da quella sessione. Lo uso sempre quando chiudo le connessioni RDP.

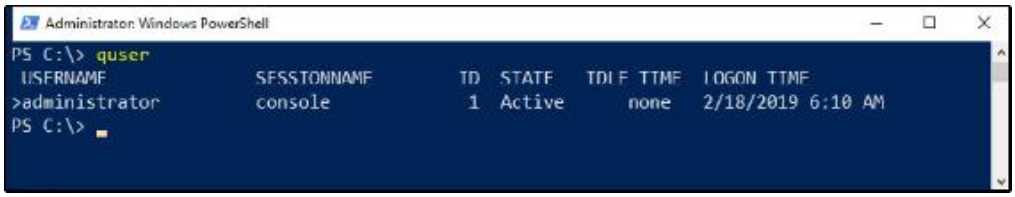
Sia l'arresto che il riavvio del computer sono utili per arrestare o riavviare un server. Sul mio computer, questi comandi sono più comunemente preceduti dal comando hostname. Quando si riavvia un server, è necessario prestare particolare attenzione a riavviare la macchina corretta, quindi trovo che sia meglio aprire un prompt di PowerShell, eseguire un rapido controllo del nome host e quindi eseguire un comando di riavvio dallo stesso prompt. Ciò garantisce il riavvio del server restituito nell'output del nome host.

spegnimento / r / t 0

Se esegui un semplice comando di spegnimento, il sistema si spegnerà in un minuto. non sonocerto perché questa è l'impostazione predefinita, poiché non ho mai trovato alcun amministratore IT che volesse effettivamente aspettare quel minuto in più prima di spegnere il proprio sistema. È invece più efficiente impostare un limite di tempo prima che inizi lo spegnimento. Nel comando precedente, ho detto al comando shutdown che voglio riavviare invece di spegnermi, questo è ciò che fa / r; Gli ho anche detto di aspettare zero secondi prima di eseguire questo riavvio. In questo modo, avviene immediatamente; Non devo aspettare i 60 secondi predefiniti.

Interroga utente o quser

Spesso più utile in Negli ambienti RDS, il comando quser mostrerà tutti gli utenti che sono attualmente connessi a un server, comprese le statistiche sul fatto che siano collegati localmente o in remoto e per quanto tempo la loro sessione è stata attiva:



qutente / computer: WEB1

L'utilizzo di quser in combinazione con l'opzione / computer consente di vedere il utenti registrati su un sistema remoto. In questo modo, puoi rimanere connesso a un singolo server nella tua farm RDS, ma controllare le sessioni utente per tutti i tuoi sistemi senza dovervi accedere. È anche possibile scrivere uno script che esegua questo comando su ciascuno dei server host della sessione e restituisca i dati a un file. Questo output potrebbe quindi essere eseguito in base a una pianificazione e utilizzato come meccanismo di report per tenere traccia di quali utenti sono stati collegati a quali server host della sessione RDS in un dato momento.

Install-WindowsFeature

Usa PowerShell per semplificare l'installazione di ruoli e funzionalità sui tuoi server.

New-NetIPAddress -InterfaceIndex 12 -IPAddress 10.10.10.40 -PrefixLength 24 -DefaultGateway 10.10.10.1

Usa New-NetIPAddress per assegnare indirizzi IP ai tuoi NIC. Tieni presente che il filele informazioni nel cmdlet precedente sono chiaramente dati di esempio e devono essere sostituite con le tue informazioni.

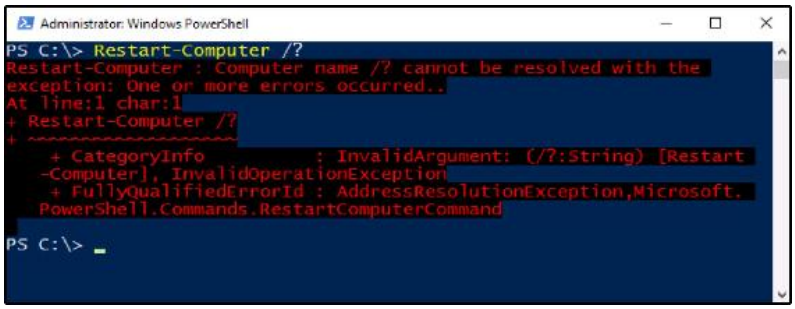
Set-DnsClientServerAddress -InterfaceIndex 12 -ServerAddresses 10.10.10.2,10.10.10.3

Utilizzato spesso in combinazione con New-NetIPAddress, utilizzalo per impostare gli indirizzi del server DNS nelle proprietà NIC.

Utilizzo di Get-Help

Quante centinaia di volte hai usato il /? passare nel prompt dei comandi per ottenere alcune informazioni aggiuntive su un comando che si desidera eseguire? Le informazioni aggiuntive fornite da questa funzione di aiuto a volte possono fare la differenza tra un comando che è utile o completamente inutile. I cmdlet di PowerShell hanno una funzione simile, ma non puoi semplicemente /? alla fine di un cmdlet di PowerShell perché uno spazio dopo un cmdlet in PowerShell indica che si sta per specificare un parametro da utilizzare con quel cmdlet. Ad

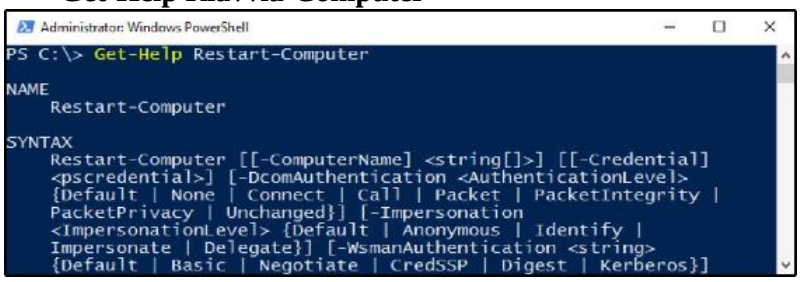
esempio, se proviamo a usare /? con il cmdlet Restart-Computer per trovare ulteriori informazioni su come utilizzare Restart-Computer, non riuscirà a riconoscere il punto interrogativo come parametro valido e il nostro output è il seguente:



Invece, c'è una funzione di aiuto ancora più potente all'interno di PowerShell. Get-Help è un cmdlet stesso e, come ogni cmdlet, dobbiamo utilizzare le informazioni che seguono il cmdlet per specificare e estrarre le informazioni che stiamo cercando. Quindi, invece di usare Get-Help alla fine di un comando, come facevamo con il punto interrogativo, lo usiamo come un'entità a sé stante.

L'esecuzione di Get-Help da sola dà solo noi Di più informazione di il Ottenere aiuto comando, che può essere utile da esaminare, ma in questo momento siamo più interessati a scoprire come utilizzare Get-Help per fornirci ulteriori informazioni per un cmdlet che vogliamo eseguire, come la funzione Restart-Computer. Quello che dobbiamo fare è utilizzare Get-Help come cmdlet, quindi specificare l'altro cmdlet come parametro da passare a Get-Help, inserendo uno spazio tra di loro:

Get-Help Riavvia-Computer



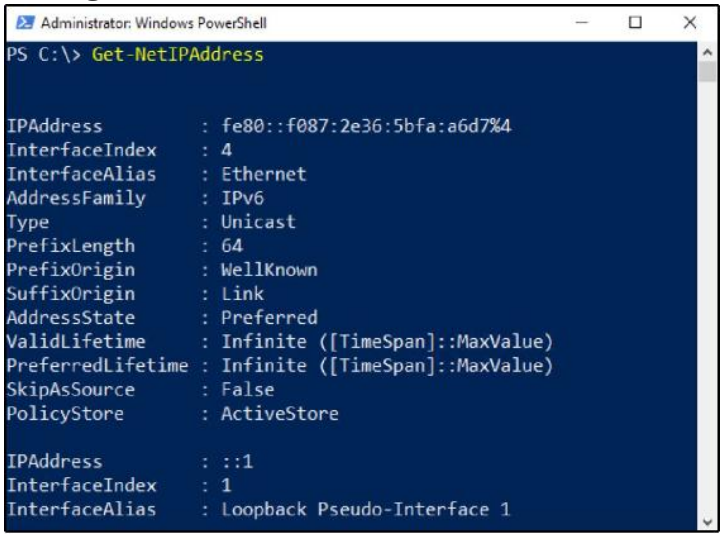
Le informazioni fornite da Get-Help sono molto complete; in alcuni casi, ha tuttole stesse informazioni che puoi trovare su TechNet. Assicurati di iniziare a utilizzare Get-Help per approfondire la tua conoscenza di qualsiasi cmdlet in PowerShell!

Formattazione dell'output

Durante la ricerca di informazioni in PowerShell, mi capita spesso di incontrare il caso in cui mi vengono fornite così tante informazioni che è difficile ordinarle. Stai cercando di trovare cmdlet utili da Get-Command o forse rintracciare un particolare alias con Get-Alias? L'output di questi cmdlet può essere incredibilmente lungo. Sebbene abbiamo discusso alcuni parametri che è possibile utilizzare per ridurre questo output, come la specifica di parametri - Name particolari, ci sono un paio di parametri di formattazione che possono anche essere aggiunti ai cmdlet, al fine di modificare l'output dei dati.

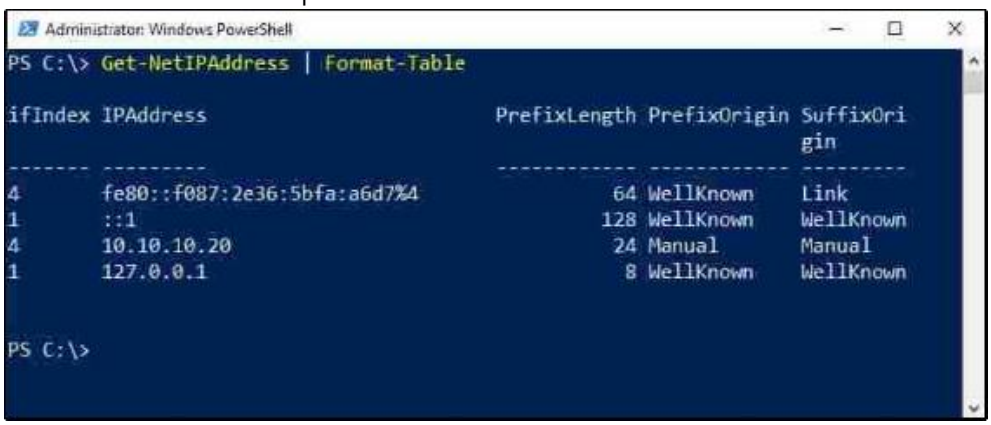
Formato-tabella

Lo scopo di Format-Table è piuttosto semplice: prende l'output dei dati da un comando e lo inserisce in un formato tabella. Questo generalmente rende le informazioni molto più facili da leggere e lavorare. Diamo un'occhiata a un esempio. Abbiamo usato Get-NetIPAddress un paio di volte, ma, siamo onesti, il suo output è un po 'disordinato. L'esecuzione del cmdlet da solo sul mio server virtuale, a cui è assegnata una sola NIC, si traduce in quattro pagine di dati all'interno della mia finestra di PowerShell, con tutti i tipi di campi informativi che sono vuoti o non importanti per trovare gli indirizzi IP assegnati al mio server:



Se aggiungiamo semplicemente Format-Table alla fine del mio cmdlet Get-NetIPAddress, il file i dati generati sono molto più facili per gli occhi, pur continuando a darmi le informazioni importanti che sto davvero cercando: gli indirizzi IP utilizzati nel sistema:

Get-NetIPAddress | Formato-tabella



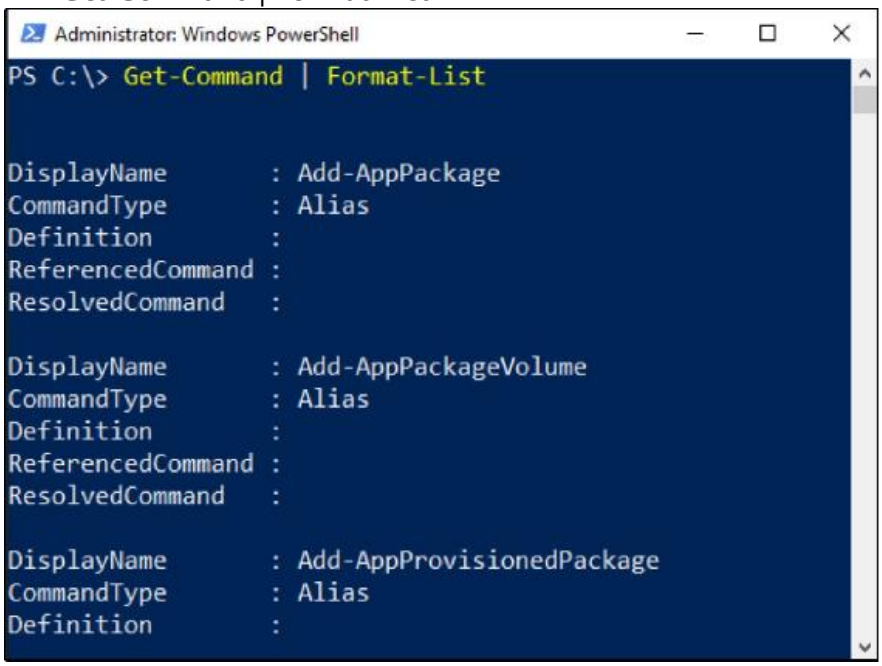
Alcuni di voi potrebbero avere familiarità con un cmdlet chiamato Select-Object, che può eseguire le stesse funzioni di Format-Table. Mentre Select-Object sembra essere il cmdlet più conosciuto, nella mia esperienza, in realtà è meno potente di Format-Table, quindi ti suggerisco di dedicare un po 'di tempo a giocare con quello di cui abbiamo discusso qui.

Format-List

Simile al modo in cui funziona Format-Table, puoi utilizzare Format-List per visualizzare output del comando come elenco di proprietà. Facciamo un rapido tentativo. Sappiamo già che Get-Command ci fornisce i cmdlet disponibili all'interno di PowerShell e, per impostazione predefinita, ce li fornisce in un formato tabella.

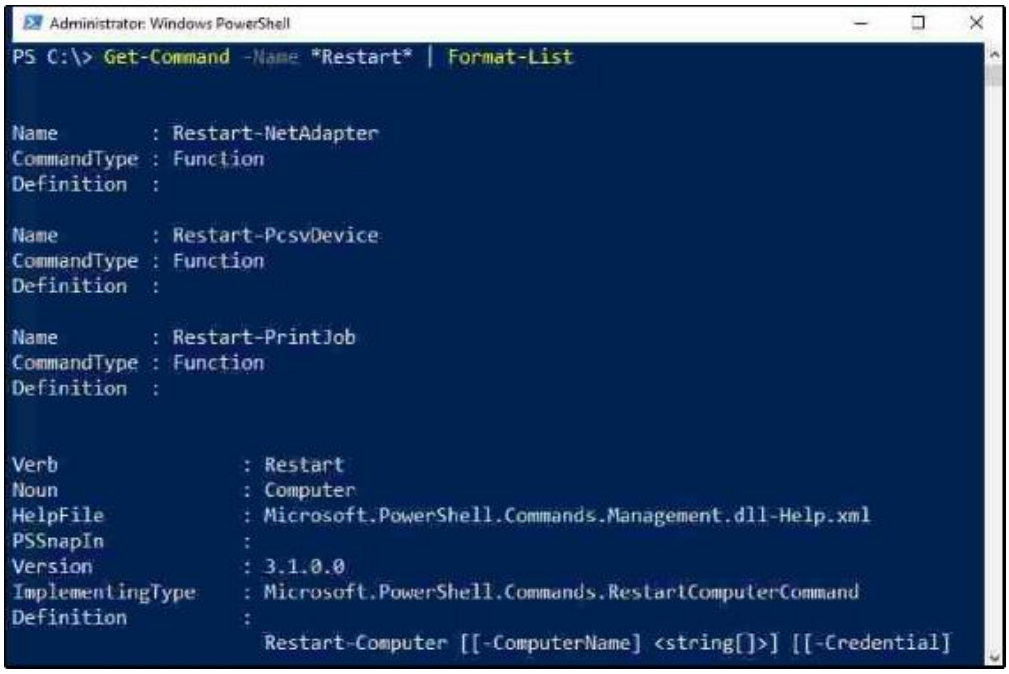
Se invece volessimo visualizzare quell'output in un elenco, con più informazioni fornite su ogni cmdlet, potremmo dire a Get-Command di produrre i suoi dati in formato elenco, con il seguente comando:

Get-Command | Format-List



Ciò si traduce in un output di informazioni tremendamente lungo, così lungo in effetti che la mia finestra di PowerShell ha avuto problemi a visualizzarlo tutto. Forse abbiamo bisogno di ridurre un po 'queste informazioni restringendo la nostra attenzione. Cerchiamo tutti i cmdlet che includono la parola Riavvia durante la visualizzazione in formato elenco:

Get-Command -Name * Riavvia * | Format-List


Administrator: Windows PowerShell
PS C:\> Get-Command -Name *Restart* | Format-List
Name : Restart-NetAdapter
CommandType : Function
Definition :
Name : Restart-PcsvDevice
CommandType : Function
Definition :
Name : Restart-PrintJob
CommandType : Function
Definition :
Verb : Restart
Noun : Computer
HelpFile : Microsoft.PowerShell.Commands.Management.dll-Help.xml
PSSnapIn :
Version : 3.1.0.0
ImplementingType : Microsoft.PowerShell.Commands.RestartComputerCommand
Definition :
Restart-Computer [[-ComputerName] <string[]>] [[-Credential]

Ambiente di scripting integrato di PowerShell

La maggior parte degli amministratori di server ha familiarità con il concetto di creazione di file batch da utilizzare nel mondo del prompt dei comandi. Hai una serie di comandi che vuoi eseguire in sequenza? Hai bisogno di eseguire questa sequenza di comandi più volte su server diversi o più e più volte in futuro? Lanciare più comandi all'interno di un documento di testo e quindi salvarlo con l'estensione del file .BAT si tradurrà in un file batch che può essere eseguito su qualsiasi computer Windows, emettendo quei comandi in sequenza, il che ti farà risparmiare il tempo e lo sforzo di dover eseguire il plunk questi comandi più e più volte all'interno dell'interfaccia della riga di comando.

Lo scripting in PowerShell è la stessa idea, ma è molto più potente. I comandi nel prompt dei comandi sono utili, ma limitati, mentre i cmdlet di PowerShell hanno la capacità di manipolare qualsiasi cosa all'interno del sistema operativo. Con PowerShell, abbiamo anche la possibilità di fare riferimento a elementi dall'interno delle variabili di ambiente o dal registro; possiamo facilmente impartire comandi a sistemi remoti e possiamo persino utilizzare variabili all'interno di uno script PowerShell, proprio come faresti con qualsiasi linguaggio di programmazione completo.

Esploriamo un paio di modi diversi che possono essere utilizzati per iniziare a creare i primi script di PowerShell.

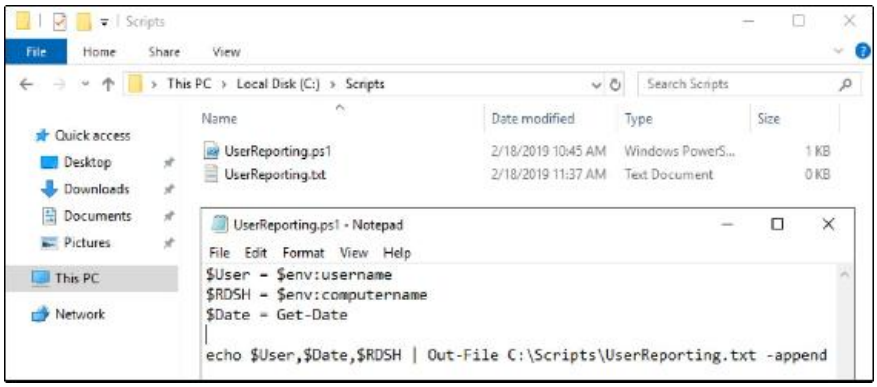
File PS1

La creazione di un semplice file .PS1 (un file di script di PowerShell) è quasi esattamente la stessa idea come creando un file .BAT. Tuttinon devi far altro che aprire un documento di testo utilizzando il tuo editor preferito, inserire una serie di comandi o cmdlet e quindi salvare il file come FILENAME.PS1. Finché il tuo ambiente PowerShell consente l'esecuzione di script - vedi in precedenza nel capitolo sul DEP - ora hai la possibilità di fare doppio clic su quel file .PS1, o avviarlo da qualsiasi prompt di PowerShell, per eseguire la serie di cmdlet dentro quel copione. Facciamo un tentativo e dimostriamo che possiamo ottenere uno script semplice e operativo.

Dal momento che creerai solo script che servono a uno scopo, pensiamo a un esempio del mondo reale. Lavoro un po 'con i server terminal - scusatemi, server RDS - e una richiesta comune da parte dei clienti è un registro di ciò che gli utenti hanno effettuato l'accesso a quali server. Un modo semplice per raccogliere queste informazioni consiste nel creare uno script di accesso che registri le informazioni sulla sessione dell'utente in un file durante l'accesso. Per fare ciò, è necessario creare uno script che posso configurare per l'esecuzione durante il processo di accesso. Per rendere lo script un po 'più interessante e flessibile in futuro, utilizzerò alcune variabili per il mio nome utente, la data e l'ora correnti e registrerò

il nome del server RDS a cui si è effettuato l'accesso. In questo modo, posso esaminare l'insieme collettivo di registri lungo la strada e determinare facilmente quali utenti erano su quali server. Userò il Blocco note per creare questo script. Ho aperto una nuova istanza di Blocco note, inserito i seguenti comandi e ora lo sto salvando come C: \ Scripts \ UserReporting.ps1:

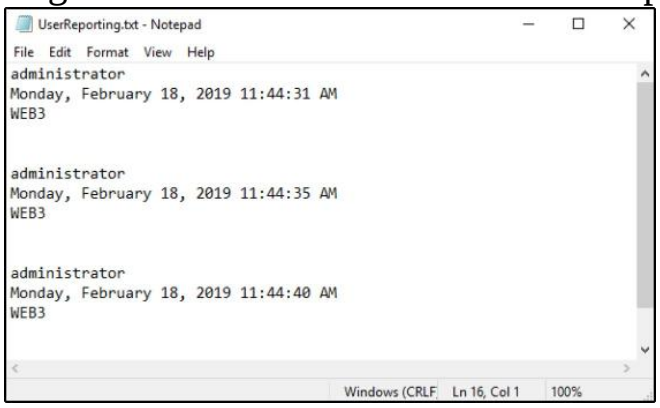
$ User = $ env: nomeutente $ RDSH = $ env: nomecomputer $ Date = echo Get-Date
$ Utente, $ Date, $ RDSH | File in uscita C: \ Scripts \ UserReporting.txt -append



Probabilmente puoi già dire cosa sta facendo questo script, ma esaminiamolo comunque. Innanzitutto, stiamo definendo tre variabili. Sto dicendo allo script che $ User deve essere uguale, indipendentemente dalla variabile di ambiente del nome utente del sistema visualizzata. $ RDSH sarà il nome del server in cui l'utente accede, estratto anche accedendo alle variabili di ambiente del server. La terza variabile definita è $ Date, che estrae semplicemente la data di sistema corrente chiamando un cmdlet di PowerShell denominato Get-Date.

Dopo aver inserito tutte le informazioni nelle variabili di PowerShell, sto quindi trasmettendo questi tre elementi in un file di testo che si trova sul disco rigido del mio server.

Se eseguo questo script alcune volte, posso aprire il mio file UserReporting.txt e vederlo ogni volta che lo script viene eseguito, registra correttamente le mie variabili specificate in questo file di report:



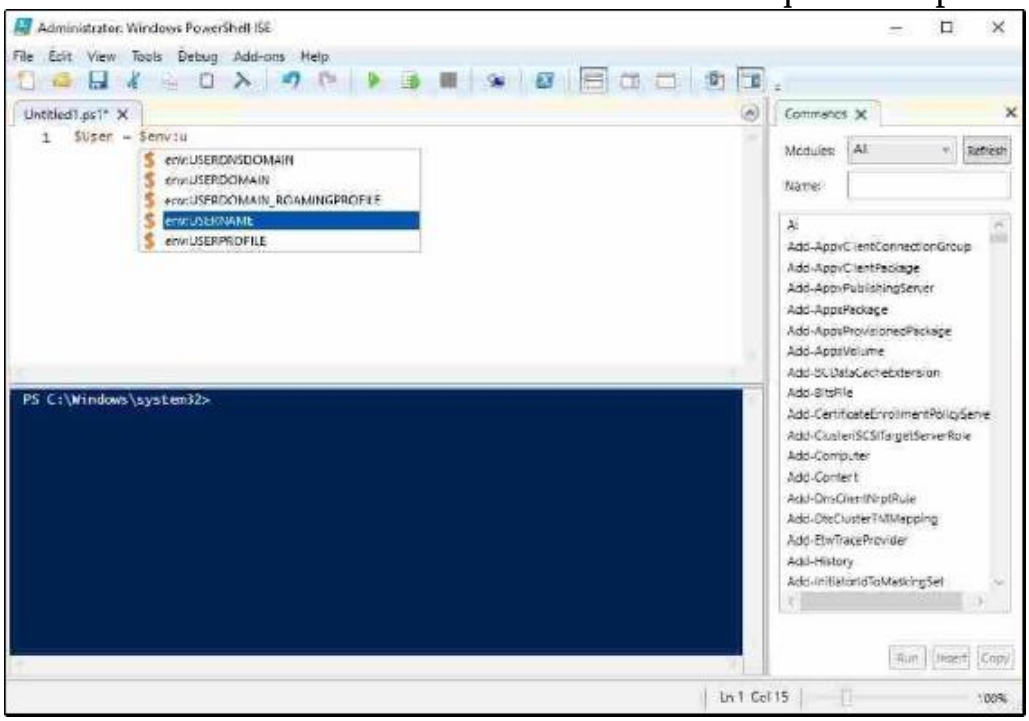
Ambiente di scripting integrato di PowerShell

Se devo essere onesto, mettere insieme quel semplice script che abbiamo appena eseguito ha richiesto alcuni tentativi ed errori. Non avevo una copia prontamente disponibile per lavorare e dovevo testare un paio di linee individualmente in PowerShell prima di essere sicuro che avrebbero funzionato nel mio script. Ho anche provato per la prima volta a estrarre il nome utente senza utilizzare la variabile di ambiente e non ha funzionato. Perché ho avuto così tanti problemi a mettere insieme solo poche semplici righe di codice? Perché mentre digito quelle righe in Blocco note, non ho assolutamente idea se funzioneranno quando salvo e cerco di eseguire quello script. Tutto il testo è solo nero con uno sfondo bianco, e mi fido completamente delle mie conoscenze e capacità di scripting per mettere insieme qualcosa che funzioni davvero.

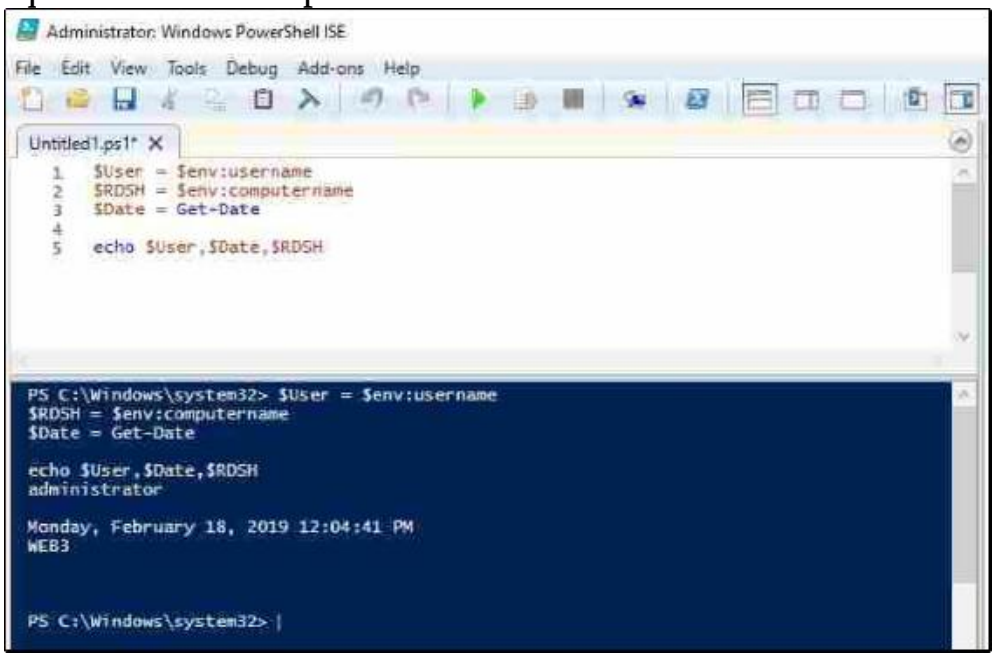
Per fortuna, abbiamo accesso a PowerShell Integrated Scripting Environment (ISE). Questo è un programma che viene installato per impostazione predefinita in Windows Server 2019; è una shell di scripting che consente di scrivere script di PowerShell e fornisce assistenza lungo il percorso. Andiamo avanti e apriamolo. Se disponi di file di script PowerShell per PS1, puoi semplicemente fare clic con il pulsante destro del mouse su uno di essi e scegliere Modifica. Altrimenti, facendo clic con il pulsante destro del mouse sull'icona dell'applicazione PowerShell (dalla barra delle applicazioni, ad esempio), troverai un'opzione per avviare Windows PowerShell ISE direttamente da quel menu:


Tasks
Run as Administrator
Run ISE as Administrator
Windows PowerShell ISE
Windows PowerShell
Pin to taskbar
Close window

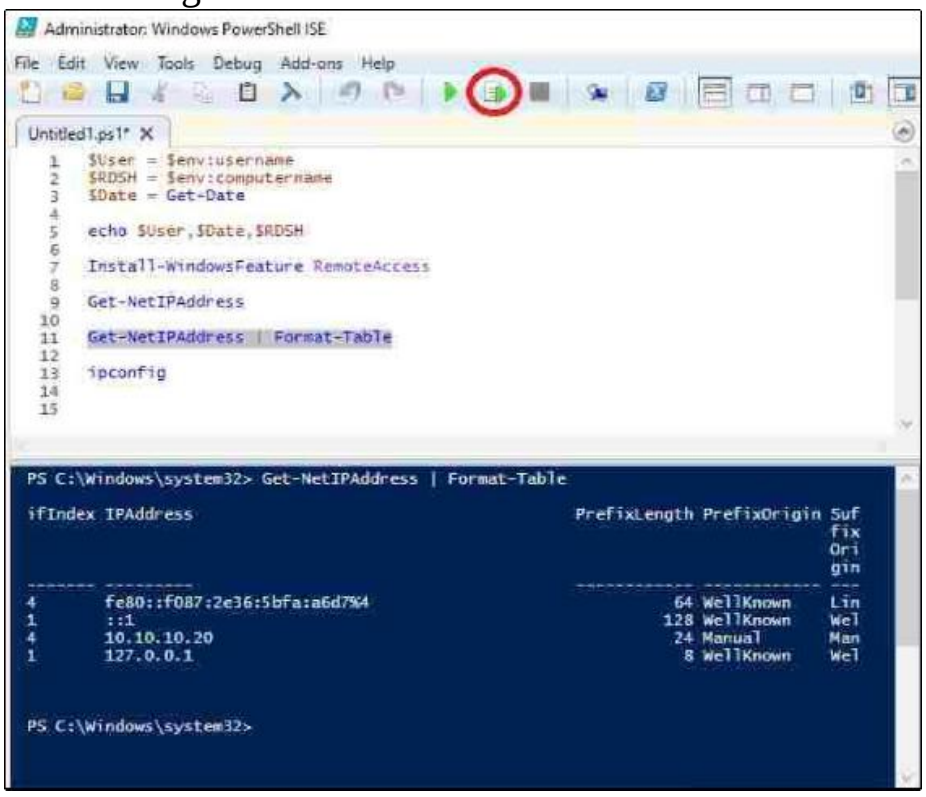
Ora, se iniziamo a digitare le stesse informazioni di script che ho usato in Blocco note pochi minuti fa, puoi vedere che anche mentre digitiamo, riceviamo popup e prompt che ci aiutano a decidere quali cmdlet o variabili vogliamo utilizzare. Simile al modo in cui funzionano le nostre tastiere a completamento automatico sui nostri smartphone, ISE fornirà suggerimenti su ciò che stai iniziando a digitare, in modo che tu non debba necessariamente ricordare come vengono chiamati i cmdlet oi parametri; puoi fare un'ipotesi plausibile su quale lettera inizia e quindi sceglierne una dall'elenco che viene presentato. C'è anche un elenco a destra di tutti i comandi disponibili ed è ricercabile! Questa è un'ottima funzionalità che aiuta davvero a far funzionare questi script:



Utile anche il mini schermo blu di PowerShell che occupa la metà inferiore della finestra di sviluppo all'interno di ISE. Fondamentalmente, quando si digitano alcuni comandi, ISE aiuta ad assicurarsi che funzionino tutti codificando a colori i cmdlet e i parametri per una facile identificazione, quindi è possibile fare clic sul pulsante freccia verde nella barra delle applicazioni etichettato Esegui script (F5). Anche se non hai ancora salvato lo script da nessuna parte, ISE si avvia tramite i tuoi comandi e presenta l'output nella seguente finestra del prompt di PowerShell. Ciò ti consente di testare il tuo script o di testare le modifiche che stai apportando a uno script esistente, senza dover salvare il file e quindi avviarlo separatamente da una finestra di PowerShell tradizionale:



Ancora meglio è che puoi evidenziare sezioni particolari del tuo script e scegliere di eseguire solo parti isolate del codice. Ciò ti consente di testare alcune sezioni di uno script o di fare qualcosa di creativo, come mantenerne uno grande. Il file di script PS1 è pieno di comandi PowerShell comuni che potresti utilizzare quotidianamente e quando hai la necessità di eseguirne solo uno, puoi semplicemente evidenziare il testo che desideri eseguire e fare clic su Esegui selezione Pulsante (F8). Evidenziando il testo prima di eseguire lo script da ISE, verranno attivati solo i cmdlet selezionati. Nello screenshot seguente, puoi vedere che ho numerosi cmdlet elencati nel mio file di script, ma solo quello evidenziato è stato eseguito:



Gestione remota di un server

Ora che abbiamo lavorato un po 'sull'istanza locale di PowerShell e abbiamo esplorato un paio di metodi che possono essere utilizzati per iniziare a creare script, è il momento di dare un'occhiata più da vicino a come PowerShell si adatta alle tue esigenze di amministrazione centralizzata. Se inizi a utilizzare PowerShell per l'amministrazione del server, ma stai ancora eseguendo RDP nei server e quindi apri PowerShell da lì, stai sbagliando. Sappiamo già che puoi toccare server remoti in Server Manager in modo che possano essere gestiti centralmente, e sappiamo anche che gli strumenti all'interno di Server Manager sono, per la maggior parte, solo l'emissione di una serie di cmdlet di PowerShell quando fai clic sui pulsanti . Combina queste due informazioni e puoi supporre che i comandi e i cmdlet di PowerShell possano essere facilmente eseguiti su sistemi remoti,

Prendendo questa idea e procedendo con essa, esamineremo i criteri necessari affinché ciò avvenga nel nostro ambiente. Ci assicureremo che uno dei nostri server sia pronto per accettare connessioni PowerShell remote, quindi utilizzeremo un prompt di PowerShell su una macchina diversa per estrarre informazioni e apportare modifiche a quel server remoto.

Preparazione del server remoto

Ci sono solo un paio di elementi che devono essere in esecuzione e abilitati sui server remoti per poter inserire PowerShell in essi da una macchina diversa. Se tutti i tuoi server sono Windows Server 2019 (in effetti, se sono tutti Windows Server 2012 o versioni successive), la comunicazione remota di PowerShell è abilitata per impostazione predefinita e potresti essere in grado di saltare le prossime due sezioni. Tuttavia, se provi a utilizzare il comando remoto di PowerShell e non funziona per te, è importante capire come funziona sotto il cofano. In questo modo, è possibile risolverlo e stabilire manualmente funzionalità

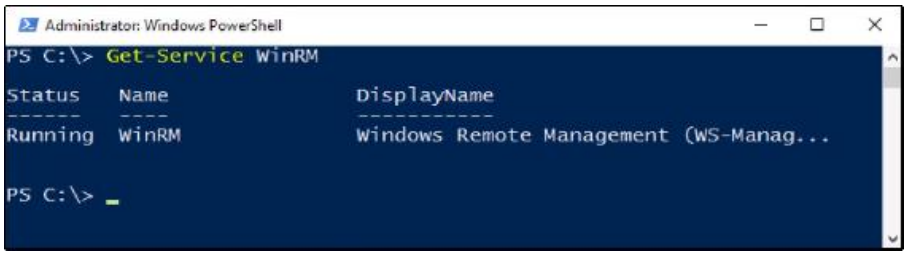
remote nel caso in cui si riscontrino problemi o si eseguano alcuni sistemi operativi meno recenti in cui potrebbero essere necessari questi passaggi.

Il servizio WinRM

Un pezzo del puzzle della gestione remota è il servizio WinRM. Assicurati semplicemente che questo servizio sia in esecuzione. Se lo hai interrotto come una sorta di protezione avanzata o vantaggio di sicurezza, dovrai annullare tale modifica e ripristinare il servizio e farlo funzionare per poter utilizzare il comando remoto di PowerShell.

Puoi controllare lo stato del servizio WinRM da services.msc, ovviamente, o poiché stiamo usando PowerShell in questo capitolo, puoi controllarlo con il seguente comando:

Get-Service WinRM



Abilita-PSRemoting

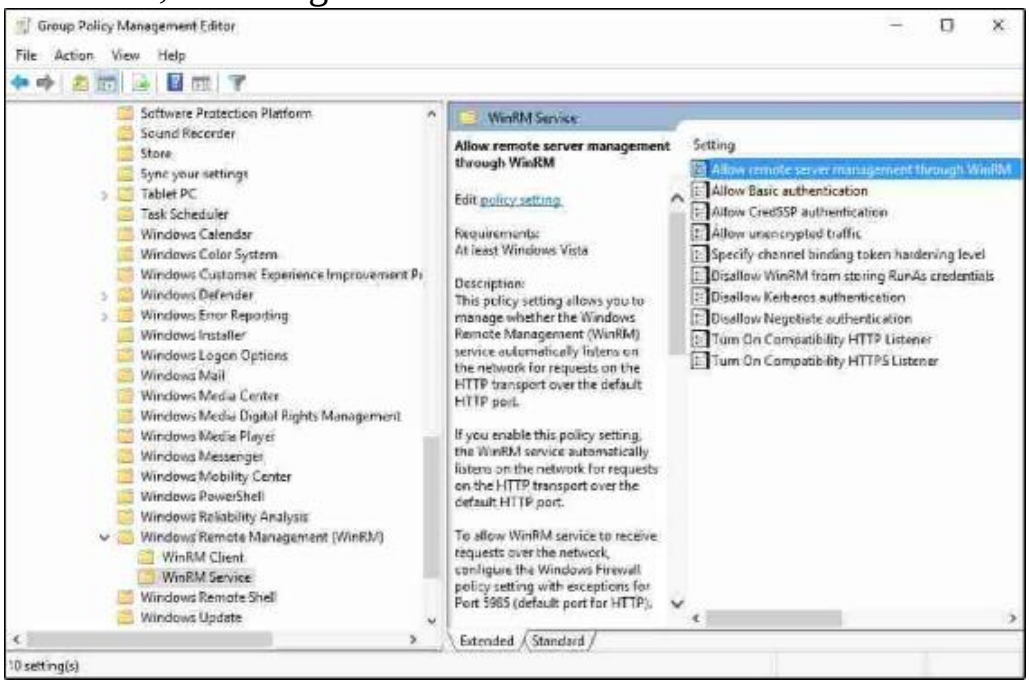
In genere, l'unica altra cosa che deve essere eseguita sul server remoto è eseguire un singolo, semplice cmdlet. Bene, deve avere accesso alla rete, ovviamente, o non sarai affatto in grado di vederlo sulla rete. Ma oltre ad assicurarti che la connettività e il flusso di rete funzionino direttamente dalla console del tuo nuovo server, sei quindi pronto per emettere il comando PowerShell che consente a questo server di essere in grado di accettare connessioni PowerShell remote in entrata:

Abilita-PSRemoting -Force

Utilizzando -Force alla fine di il Comando Enable-PSRemoting cause il comando per roll senza chiederti conferme. Ci sono alcune cose diverse che Enable-PSRemoting sta facendo in background qui. Innanzitutto, sta tentando di avviare il servizio WinRM. Perché ho già specificato che dovresti controllarlo manualmente? Perché se lo hai disabilitato come parte di una strategia di blocco, interferirai con questo processo. Il controllo di WinRM prima di utilizzare Enable-PSRemoting aumenta le possibilità di successo durante l'esecuzione del cmdlet Enable-PSRemoting. Ci sono altre due cose che questo comando sta facendo: avviare il listener per le connessioni remote e creare una regola del firewall sul sistema per consentire a questo traffico di passare correttamente.

Se si intende utilizzare il servizio remoto di PowerShell su larga scala, è scoraggiante pensare di accedere a ogni singolo server ed eseguire questo comando. Per fortuna, non devi! Come con la maggior parte delle funzioni nel mondo Windows, possiamo utilizzare Criteri di gruppo per apportare questa modifica automaticamente. Creare un nuovo oggetto Criteri di gruppo, collegarlo e filtrarlo in modo appropriato in modo che si applichi solo ai server che si desidera gestire centralmente, quindi configurare questa impostazione: Configurazione computer | Politiche | Modelli amministrativi | Componenti di Windows | Gestione remota di Windows (WinRM) | Servizio WinRM.

Impostare Consenti la gestione del server remoto tramite WinRM su Abilitato, come segue:



Consentire macchine da altri domini o gruppi di lavoro

Se si lavora con server che fanno tutti parte dello stesso dominio aziendale, che sarà il più delle volte, l'autenticazione tra macchine è facile da realizzare. Si fidano automaticamente l'uno dell'altro a questo livello. Tuttavia, sul server che stai preparando ad accettare connessioni remote, se ti aspetti che quei computer saranno membri di un dominio diverso che non è attendibile - o anche membri di un gruppo di lavoro - allora dovrai emettere un comando per fidarti manualmente dell'individuo computer che si connetteranno. Ad esempio, se intendo gestire tutti i miei server da un computer client chiamato Win10Client che non è considerato attendibile dai server, dovrei eseguire il seguente comando su questi server:

Set-Item wsman: \ localhost \ client \ trustedhosts Win10Client

Se si desidera consentire a qualsiasi macchina di connettersi in remoto, è possibile sostituire il nome del singolo computer con un *, ma in generale non sarebbe una buona pratica, poiché si potrebbero creare problemi consentendo a qualsiasi macchina di connettersi al server in questo modo.

Connessione al server remoto

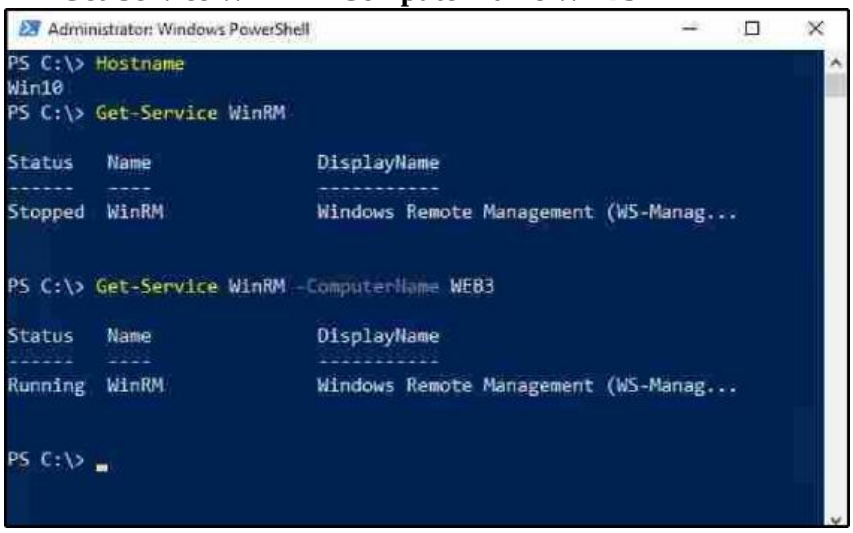
In genere vedo che gli amministratori utilizzano PowerShelling remoto in due modi diversi. È possibile eseguire alcuni comandi su sistemi remoti su base ad hoc mentre il prompt di PowerShell è ancora locale oppure è possibile avviare una sessione remota di PowerShell in piena regola per fare in modo che il prompt di PowerShell si comporti come se fosse in esecuzione direttamente su quel sistema remoto .
Diamo un'occhiata a entrambe le opzioni.

Utilizzando -ComputerName

Molti dei cmdlet disponibili in PowerShell, in particolare quelli che iniziano con Get-, possono essere usati con il parametro -ComputerName. Ciò specifica che il comando che stai per eseguire deve essere eseguito sul sistema remoto specificato nella sezione - ComputerName. Per i nostri esempi di PowerShell remoto, userò un prompt di PowerShell sul mio computer client Windows 10 per accedere alle informazioni su alcuni dei miei server nella rete. Voglio interrogare il servizio WinRM, per assicurarmi che sia attivo e funzionante. Per dimostrarti che sto comunicando da remoto con WEB3, vedrai nell'output che ho prima interrogato il mio servizio WinRM locale, che mi è capitato di disabilitare sulla mia workstation Win10.

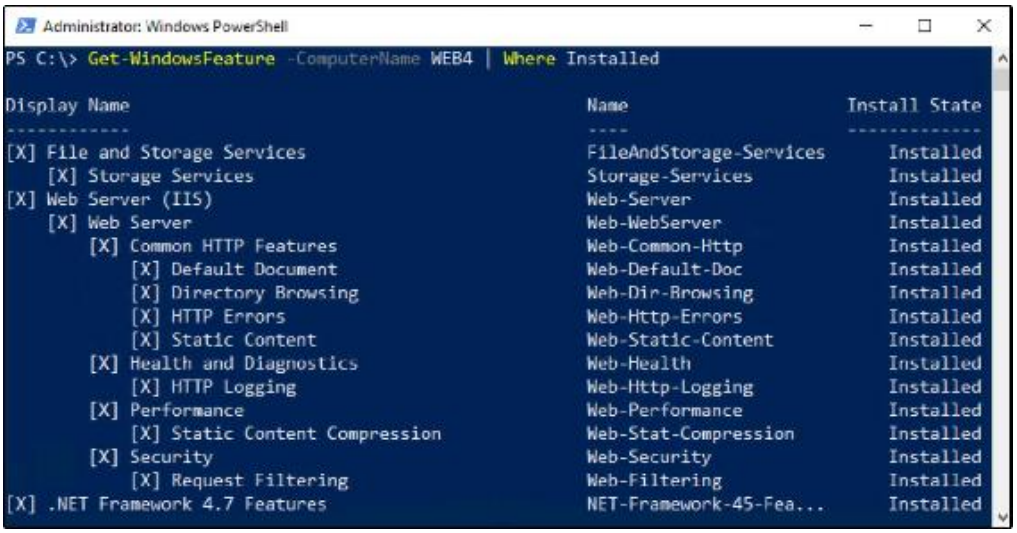
Vedi che il mio servizio WinRM locale viene visualizzato come Arrestato, ma quando emetto lo stesso comando specificando di interrogare ComputerName di WEB3, mi raggiunge e mi informa che il servizio WinRM è effettivamente in esecuzione con successo sul server WEB3:

Nome host
Get-Service WinRM
Get-Service WinRM -ComputerName WEB3



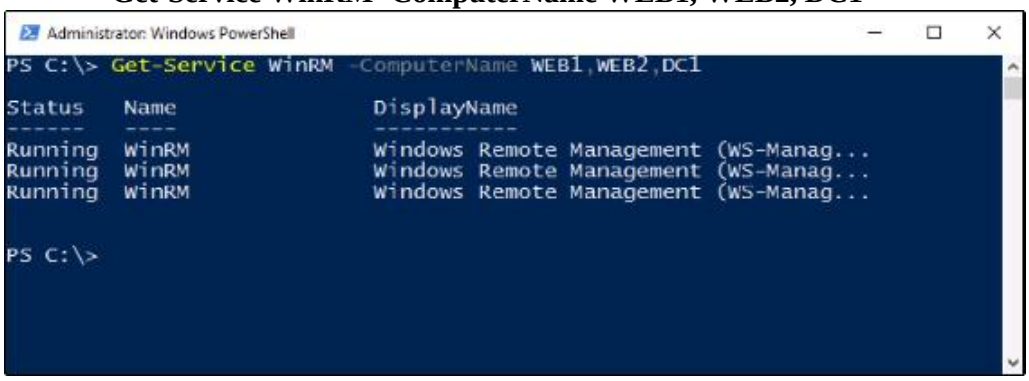
In alternativa, forse voglio interrogare la nuova istanza Server Core che abbiamo impostato poco fa e controllare quali ruoli sono attualmente installati su WEB4:

Get-WindowsFeature -ComputerName WEB4 | Dove installato



Il parametro -ComputerName può anche accettare più nomi di server contemporaneamente. SeVolevo controllare lo stato del servizio WinRM su alcuni dei miei server, utilizzando un unico comando, potevo fare qualcosa del genere:

Get-Service WinRM -ComputerName WEB1, WEB2, DC1



Utilizzando Enter-PSSession

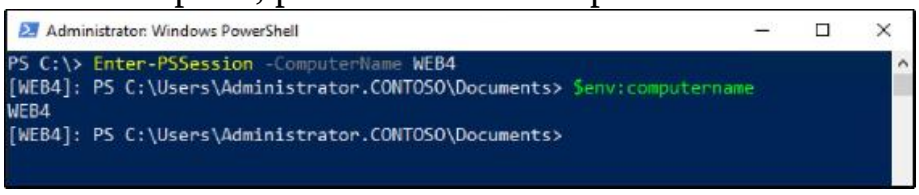
D'altra parte, a volte sono presenti molti cmdlet diversi che si desidera eseguire su un determinato server. In questo caso, ha più senso richiamare l'istanza di PowerShell completamente capace e completamente remota su quel server remoto. Se apri PowerShell sul tuo sistema locale e utilizzi il cmdlet Enter-PSSession, il prompt di PowerShell sarà una rappresentazione remota completa di PowerShell su quel server remoto. Sarai quindi in grado di emettere comandi in quel prompt e verranno eseguiti come se fossi seduto a un prompt di PowerShell dalla console di quel server. Ancora una volta, ho effettuato l'accesso al mio computer client Windows 10 e ho aperto PowerShell. Quindi utilizzo il seguente comando per connettermi in remoto al mio server WEB4:

Immettere-PSSession -ComputerName WEB4

Vedrai il prompt cambiare, indicando che ora sto lavorando nel contesto di WEB4 server.

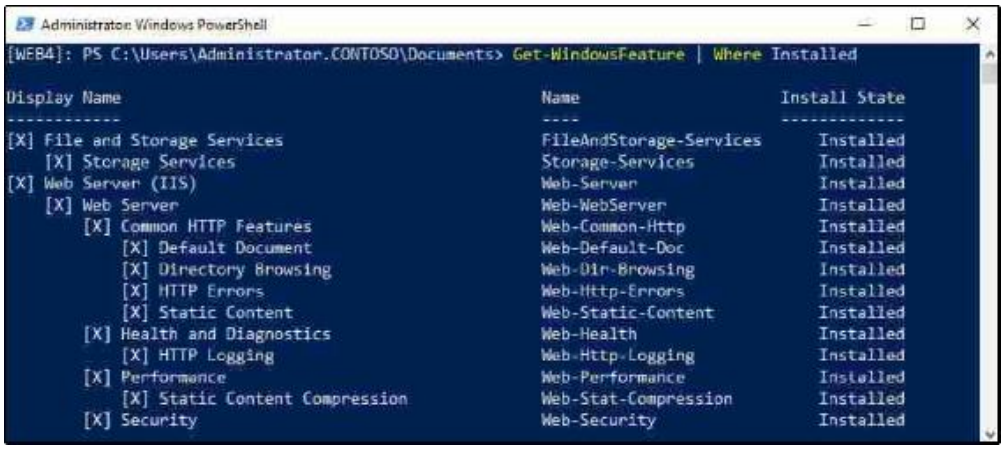
Se il tuo account utente non ha accesso al server, puoi specificare credenziali alternative da utilizzare durante la creazione di questa connessione remota. Aggiungi semplicemente il tuo fileEnter-PSSession cmdlet con -NOME UTENTE credenziale per specificare un account utente diverso

I comandi che emetto da questo punto in avanti verranno eseguiti su WEB4. Verifichiamo questo. Se controllo un semplice $ env: nomecomputer, puoi vedere che mi presenta il nome host WEB4:



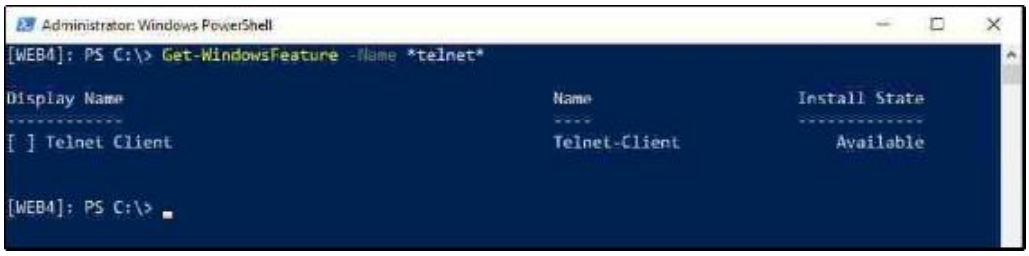
E per verificare ulteriormente ciò, se controllo i ruoli e le funzionalità di Windows installati, puoi vedere che ho il ruolo di server Web installato, come abbiamo ottenuto quando abbiamo inizialmente configurato questo Server Core come server Web. Chiaramente, non ho il ruolo di Web Server installato sulla mia workstation Windows 10; PowerShell sta estraendo questi dati dal server WEB4.

Get-WindowsFeature | Dove installato



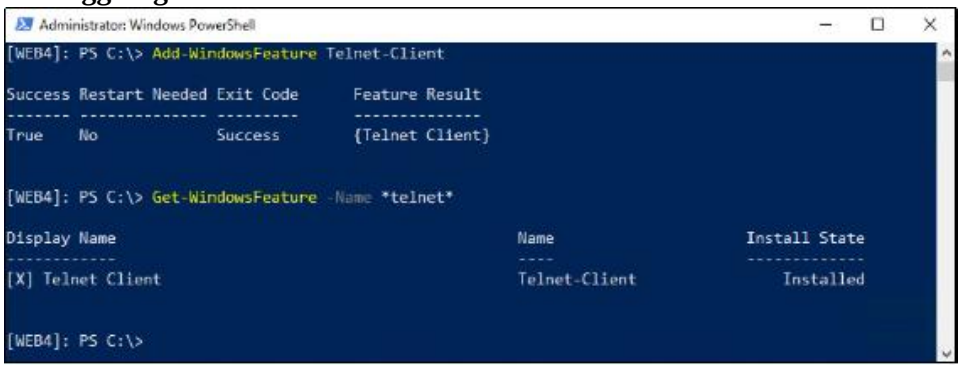
Questa è roba piuttosto potente. Siamo seduti sul nostro computer desktop locale, abbiamo una sessione remota di PowerShell in esecuzione sul server WEB4 e ora siamo in grado di estrarre tutti i tipi di informazioni da WEB4 perché è come se stessimo lavorando da PowerShell proprio su quel server. Facciamo un ulteriore passo avanti e proviamo ad apportare una modifica alla configurazione su WEB4, solo per verificare che possiamo. Forse possiamo installare una nuova funzionalità su questo server. Uso abbastanza spesso Telnet Client per testare la connettività di rete, ma posso vedere che attualmente non è installato su WEB4.

Get-WindowsFeature -Nome * telnet *



Utilizzando il cmdlet Add-WindowsFeature, dovrei essere in grado di lavorare rapidamente installazione di quella funzionalità:

Aggiungi-WindowsFeature Telnet-Client



Questa funzionalità di PowerShell remota è potente, non solo per i tuoi server che eseguono l'interfaccia grafica completa di Desktop Experience, ma anche per interagire con le distribuzioni di Server Core incentrate sulla sicurezza. Acquisire familiarità con il lavoro in sessioni remote di PowerShell sarà essenziale per una corretta distribuzione di Server Core nella tua infrastruttura.

Configurazione dello stato desiderato

Ci sono alcune nuove e potenti funzionalità nelle versioni più recenti di PowerShell, fornite da qualcosa chiamato DSC (Desired State Configuration). DSC è una piattaforma di gestione collegata a PowerShell, che fornisce alcune nuove funzioni e cmdlet che puoi sfruttare negli script per abilitare alcune funzionalità davvero interessanti. Come suggerisce il nome, consente di creare configurazioni all'interno di PowerShell che forniranno uno stato desiderato. Cosa intendo dire? Bene, in un senso di base, DSC si assicura che gli script di PowerShell che crei funzioneranno sempre allo stesso modo, su tutti i server in cui li applichi. È abbastanza facile creare uno script in modo che funzioni correttamente sul server da cui stai lavorando, ma se provi a distribuire lo stesso script su un server diverso che potrebbe risiedere in un'unità organizzativa (OU) diversa o avere elementi diversi installati su di esso per cominciare, lo script potrebbe produrre risultati diversi da quelli originariamente previsti fare. DSC è stato creato per contrastare queste differenze.

Durante la creazione della configurazione DSC, si identificano ruoli, impostazioni, funzioni, account, variabili e così via particolari che si desidera mantenere nello stato specifico desiderato. Una volta identificate e configurate queste variabili, DSC lavorerà per garantire che rimangano dove sono state impostate e che rimangano uniformi in base alla politica di configurazione DSC, il che significa che sono uniformi rispetto agli altri server su cui è stato eseguito questo script.

DSC aiuta anche a prevenire modifiche indesiderate sui server. Se il tuo script abilitato per DSC ha identificato che un particolare servizio dovrebbe essere sempre in esecuzione sui tuoi server e quel servizio si interrompe per qualche motivo, DSC può essere lì per aiutarti a riavviarlo in modo che non si verifichi un'interruzione. In alternativa, forse hai uno script che configura un server in base a un particolare insieme di standard e un'altra persona nell'IT arriva e regola quella configurazione sul server stesso, forse accede e interrompe un servizio intenzionalmente per qualche motivo. Normalmente, ciò potrebbe causare un'interruzione per quel server, ma DSC ripristinerà il servizio in modo da mantenere lo stato desiderato configurato in origine per questo server. DSC è la tua tata di scripting, per così dire. Aiuta a creare configurazioni che rimarranno uniformi su più piattaforme e funzioneranno per garantire che queste configurazioni siano sempre vere. Puoi quindi essere certo che i tuoi server siano sempre in esecuzione nel contesto dello stato desiderato specificato.

Dopo aver creato una configurazione che identifica gli elementi che si desidera installare o monitorare, qualcosa chiamato Local Configuration Manager (LCM) funziona per garantire che le risorse rimangano entro le specifiche di configurazione. LCM esegue regolarmente il polling del sistema, osservando irregolarità e modifiche e, se necessario, intraprende azioni per riportare i server nel DSC.

L'obiettivo finale di DSC è mantenere tutto costante e coerente tra i tuoi server e servizi. Le capacità di DSC e l'accesso per raggiungere sempre più posti nel sistema operativo crescono costantemente, poiché i ruoli vengono riscritti per accettare i parametri e il monitoraggio DSC. Alla

fine, credo che l'obiettivo di Microsoft sarà che ogni server esegua uno script di configurazione DSC, assicurandosi che funzioni costantemente secondo i tuoi standard e contribuendo a mantenere il tuo stato di uptime del 99,999%.

C'è molto da imparare su DSC e ti incoraggio a esplorare ulteriormente questo argomento una volta acquisita familiarità con la creazione e l'utilizzo degli script di PowerShell. Ecco alcuni ottimi punti di partenza per saperne di più su DSC:

- https://msdn.microsoft.com/en-us/powershell/dsc/overview
- https://mva.microsoft.com/en-US/training-courses/getting-started-with- PowerShell-desiderato-stato-configurazione-dsc - 8672? l = ZwHuclG1_2504984382

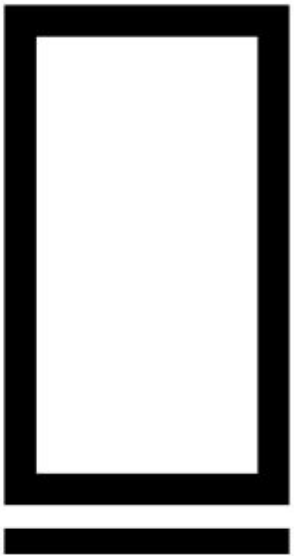
Sommario

In Windows Server 2019, vediamo in più punti che l'amministrazione tramite PowerShell è il percorso consigliato per interagire con i nostri server. Poiché le GUI di gestione ora sono solo shell che eseguono script PowerShell e l'opzione di installazione predefinita per Windows Server è Server Core, possiamo presumere che i server headless e orientati alla riga di comando saranno i nostri server del futuro. Anche se PowerShell è stato al centro delle funzionalità del nostro sistema operativo dal Server 2012, fino a questo punto credo che PowerShell sia stato visto dalla maggior parte degli amministratori semplicemente come un modo alternativo di gestire i server. Sì, so che esiste e che dovrei iniziare a usarlo, e lo scripting sembra piuttosto interessante, ma posso ancora fare tutto ciò che voglio con il vecchio prompt dei comandi o il pulsante del mouse. Quella vecchia mentalità sta cambiando rapidamente.

Ora che stiamo sperimentando l'inizio di nuove tecnologie, come DSC, possiamo vedere che PowerShell sta iniziando a sviluppare funzionalità che semplicemente non esistono da nessun'altra parte nel sistema operativo. Questo, combinato con l'accessibilità alla gestione remota fornita dalla piattaforma PowerShell standardizzata che può essere utilizzata su tutti i tuoi attuali dispositivi Windows (anche contro i server che si trovano all'interno di Azure!), Significa che vedremo sicuramente sempre più PowerShell nelle successive operazioni Microsoft sistemi e servizi. Il capitolo successivo si occupa di container e nano server.

Domande

1. Qual è il modo più veloce per passare da un prompt dei comandi a PowerShell?
2. Qual è il cmdlet che visualizzerà tutti i cmdlet di PowerShell disponibili?
3. Quale cmdlet di PowerShell può essere utilizzato per connettere il prompt di PowerShell a un computer remoto?
4. Quale estensione di file ha un file di scripting di PowerShell?
5. A quale impostazione è configurato il criterio di esecuzione predefinito su una nuova istanza di Windows Server 2019?
6. Quale tasto sulla tastiera può essere utilizzato per popolare automaticamente il resto di un cmdlet o di un nome file quando si lavora in un prompt di PowerShell?
7. Quale servizio deve essere in esecuzione su un sistema prima che possa essere connesso a una connessione PowerShell remota?



Contenitori e Nano Server

Molte delle nuove tecnologie incluse in Windows Server 2019 sono progettate per riflettere le funzionalità fornite dal cloud computing, dando vita ai tuoi cloud privati e garantendoti la possibilità di produrre le stesse soluzioni fornite dai provider di cloud pubblico all'interno della tua infrastruttura fisica. Anche le ultime iterazioni del sistema operativo Server hanno ruotato attorno alla virtualizzazione e l'idea di contenitori di applicazioni è qualcosa che attinge a entrambe queste mentalità. I contenitori di applicazioni renderanno la distribuzione delle applicazioni più snella, più sicura e più efficiente.
I contenitori sono un'idea relativamente nuova nel mondo Microsoft e non ho ancora sentito molti amministratori IT parlarne, ma presto cambierà. Questo è qualcosa che sta migliorando il computing Linux da un po 'di tempo e questo nuovo sistema operativo Windows Server lo porta un po' più vicino a casa per noi negozi incentrati su Microsoft.

Gli sviluppatori di applicazioni saranno molto interessati ai contenitori di applicazioni forniti da Windows Server 2019 e, in verità, probabilmente comprendono i concetti alla base dei contenitori molto meglio di un amministratore di server tradizionale. Sebbene la premessa di questo libro non si concentri sulle opportunità di sviluppo e chiaramente non si concentri su Linux, discuteremo dei contenitori perché i vantaggi forniti non sono solo per gli sviluppatori. Anche noi, come operazioni di sistema, trarremo vantaggio dall'utilizzo dei container e, se non altro, sarà importante per noi sapere e capire come concettualizzare e come avviare i container in modo da poter fornire l'infrastruttura che i nostri sviluppatori sono richiederà.

In questo capitolo tratteremo alcuni argomenti relativi ai contenitori delle applicazioni; in particolare, le nuove funzionalità disponibili in Windows Server 2019 per portare questa tecnologia nei nostri data center:

- Comprensione dei contenitori di applicazioni Contenitori e Nano Server
- Confronto tra contenitori di Windows Server e contenitori Hyper-V Docker e Kubernetes
- Lavorare con i contenitori

Comprensione dei contenitori delle applicazioni

Cosa significa contenere un'applicazione? Al giorno d'oggi abbiamo un'idea abbastanza buona di contenere i server, per mezzo della virtualizzazione. Prendere l'hardware fisico, trasformarlo in un host di virtualizzazione come Hyper-V e quindi eseguire molte macchine virtuali su di esso è una forma di contenimento per quelle VM. In sostanza, li stiamo inducendo a credere di essere la loro stessa entità, completamente ignari del fatto che condividono risorse e hardware con altre VM in esecuzione su quell'host. Allo stesso tempo che condividiamo le risorse hardware, siamo in grado di fornire forti livelli di isolamento tra le VM, perché dobbiamo assicurarci che l'accesso e le autorizzazioni non possano diffondersi tra le VM, in particolare in uno scenario di provider cloud, poiché ciò significherebbe un disastro .

I contenitori delle applicazioni sono la stessa idea, a un livello diverso. Laddove le VM si concentrano sulla virtualizzazione dell'hardware, i container sono più simili alla virtualizzazione del sistema operativo. Piuttosto che creare VM per ospitare le nostre applicazioni, possiamo creare container, che sono molto più piccoli. Quindi eseguiamo le applicazioni all'interno di questi contenitori e le applicazioni vengono indotte con l'inganno a pensare di essere in esecuzione su un'istanza dedicata del sistema operativo.

Un enorme vantaggio nell'utilizzo dei container è l'unità che portano tra i team di sviluppo e quelli operativi. In questi giorni sentiamo sempre il termine DevOps, che è una combinazione di processi di sviluppo e operativi per rendere più efficiente l'intero processo di implementazione dell'applicazione. L'utilizzo dei container avrà un enorme impatto sulla mentalità DevOps, dal momento che gli sviluppatori possono ora fare il loro lavoro (sviluppare applicazioni) senza bisogno di adattarsi alle operazioni e al lato infrastrutturale delle cose. Quando l'applicazione viene creata, le operazioni possono prendere il container in cui risiede l'applicazione e semplicemente avviarlo all'interno della loro infrastruttura

container, senza preoccuparsi che l'applicazione possa rompere i server o avere problemi di compatibilità.

Prevedo sicuramente che i container prendano il posto di molte macchine virtuali, ma questo accadrà solo se gli amministratori si avvicinano e lo provano da soli. Parliamo di alcuni vantaggi particolari che i contenitori portano in tavola.

Condivisione di risorse

Proprio come quando parliamo di hardware suddiviso tra le VM, i contenitori di applicazioni significano che stiamo prendendo blocchi fisici di hardware e li dividiamo tra i contenitori. Questo ci consente di eseguire molti container dallo stesso server, sia esso un server fisico o virtuale.

Tuttavia, solo in questo, non vi è alcun vantaggio rispetto alle VM, perché condividono semplicemente anche l'hardware. Il punto in cui iniziamo davvero a vedere i vantaggi nell'utilizzo di contenitori piuttosto che VM separate per tutte le nostre applicazioni è che tutti i nostri contenitori possono condividere lo stesso sistema operativo di base. Non solo provengono dallo stesso set di base, il che rende estremamente veloce portare nuovi contenitori online, ma significa anche che condividono le stesse risorse del kernel. Ogni istanza di un sistema operativo ha il proprio set di processi utente e spesso è difficile eseguire più applicazioni insieme sui server perché tali applicazioni hanno tradizionalmente accesso allo stesso set di processi e possono essere influenzate negativamente da tali processi. processi. In altre parole, è il motivo per cui tendiamo a far girare così tanti server in questi giorni, mantenendo ogni applicazione sul proprio server, in modo che non possano avere un impatto negativo a vicenda. A volte le app semplicemente non amano mischiare. Il kernel in Windows Server 2019 è stato migliorato in modo da poter gestire più copie dei processi in modalità utente. Ciò significa che non solo hai la possibilità di eseguire istanze della stessa applicazione su molti server diversi, ma significa anche che puoi eseguire molte applicazioni diverse, anche se in genere non amano coesistere, sullo stesso server.

Solitudine

Uno degli enormi vantaggi dei contenitori di applicazioni è che gli sviluppatori possono creare le loro applicazioni all'interno di un contenitore in esecuzione sulla propria workstation! Una macchina host per l'hosting di contenitori può essere un Windows Server o una workstation Windows 10. Quando viene creata all'interno di questa sandbox del contenitore, gli sviluppatori sapranno che la loro applicazione contiene tutte le parti, i pezzi e le dipendenze di cui ha bisogno per funzionare correttamente e che funziona in un modo che non richiede componenti aggiuntivi dal funzionamento sottostante sistema. Ciò significa che lo sviluppatore può creare l'applicazione, assicurarsi che

funzioni nel proprio ambiente locale e quindi far scorrere facilmente il contenitore dell'applicazione sui server di hosting dove verrà avviato e pronto per l'uso in produzione. Quel server di produzione potrebbe anche essere una risorsa fornita dal cloud, ma all'applicazione non interessa. L'isolamento del contenitore dal sistema operativo aiuta a mantenere l'applicazione standardizzata in modo che sia facilmente mobile e spostabile, e fa risparmiare tempo e grattacapi allo sviluppatore poiché non devono adattarsi alle differenze nei sistemi operativi sottostanti durante il processo di sviluppo .

L'altro aspetto dell'isolamento è l'aspetto della sicurezza. Questa è la stessa storia di più macchine virtuali in esecuzione sullo stesso host, in particolare in un ambiente cloud. Vuoi che esistano limiti di sicurezza tra queste macchine, infatti la maggior parte delle volte non vuoi che siano consapevoli l'una dell'altra in alcun modo. Vuoi persino l'isolamento e la segregazione tra le macchine virtuali e il sistema operativo host, perché sicuramente non vuoi che il tuo provider di servizi di cloud pubblico si curi all'interno delle tue VM. La stessa idea si applica ai contenitori delle applicazioni.

I processi in esecuzione all'interno di un contenitore non sono visibili al sistema operativo ospitante, anche se stai consumando risorse da quel sistema operativo. I contenitori mantengono due diverse forme di isolamento. Esiste l'isolamento dello spazio dei nomi, il che significa che i contenitori sono limitati al proprio file system e registro. Poi c'è anche l'isolamento delle risorse, il che significa che possiamo definire quali risorse hardware specifiche sono disponibili per i diversi contenitori e non sono in grado di sottrarsi a vicenda. A breve, discuteremo di due diverse categorie di contenitori, contenitori di Windows Server e contenitori Hyper-V.
Questi due tipi di contenitori gestiscono l'isolamento in modi diversi, quindi resta sintonizzato per ulteriori informazioni su questo argomento.

Sappiamo che i contenitori condividono le risorse e vengono creati dalla stessa immagine di base, pur mantenendo i loro processi separati in modo che il sistema operativo sottostante non possa influire negativamente sull'applicazione e anche in modo che l'applicazione non possa tankare il sistema operativo host. Ma come viene gestito l'isolamento da un aspetto di rete? Ebbene, i contenitori delle applicazioni utilizzano la tecnologia dello switch virtuale Hyper-V per mantenere tutto direttamente sul lato della rete. Infatti, quando inizi a utilizzare i contenitori, vedrai rapidamente che a ogni contenitore è assegnato un indirizzo IP univoco per mantenere l'isolamento a questo livello.

Scalabilità

La combinazione della rotazione dalla stessa immagine di base e l'isolamento del contenitore crea una scalabilità e una storia di crescita molto avvincenti. Pensa a un'applicazione web che ospiti il cui utilizzo potrebbe variare notevolmente da un giorno all'altro. Fornire risorse sufficienti per sostenere questa applicazione durante i periodi di punta ha tradizionalmente significato che paghiamo più del dovuto per le risorse di elaborazione quando l'applicazione non viene utilizzata in modo massiccio. Le tecnologie cloud forniscono scalabilità dinamica per questi

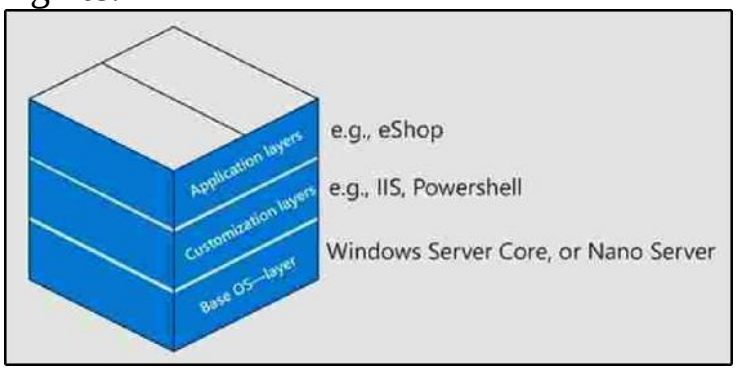
tipi moderni di applicazioni, ma lo fanno spesso attivando o disattivando intere macchine virtuali. Ci sono tre problemi comuni con applicazioni scalabili dinamicamente come questa. Il primo è il tempo necessario per produrre macchine virtuali aggiuntive; anche se tale processo è automatizzato, la tua domanda potrebbe essere sopraffatta per un periodo di tempo mentre le risorse aggiuntive vengono portate online. La nostra seconda sfida è la lotta che lo sviluppatore deve affrontare per rendere l'applicazione così agnostica da non preoccuparsi se ci sono incongruenze tra le diverse macchine su cui potrebbe essere in esecuzione la loro applicazione. Il terzo è il costo. Non solo il costo dell'hardware, poiché le nuove VM in linea consumeranno ciascuna un intero set di risorse del kernel, ma anche i costi monetari. Far girare macchine virtuali su e giù nel tuo ambiente cloud può diventare rapidamente costoso. Questi sono tutti ostacoli che non esistono quando si utilizzano i contenitori come metodo per la distribuzione delle applicazioni. La nostra seconda sfida è la lotta che lo sviluppatore deve affrontare per rendere l'applicazione così agnostica da non preoccuparsi se ci sono incongruenze tra le diverse macchine su cui potrebbe essere in esecuzione la loro applicazione. Il terzo è il costo. Non solo il costo dell'hardware, poiché le nuove VM in linea consumeranno ciascuna un intero set di risorse del kernel, ma anche i costi monetari. Far girare macchine virtuali su e giù nel tuo ambiente cloud può diventare rapidamente costoso. Questi sono tutti ostacoli che non esistono quando si utilizzano i contenitori come metodo per la distribuzione delle applicazioni. La nostra seconda sfida è la lotta che lo sviluppatore deve affrontare per rendere l'applicazione così agnostica da non preoccuparsi se ci sono incongruenze tra le diverse macchine su cui potrebbe essere in esecuzione la loro applicazione. Il terzo è il costo. Non solo il costo dell'hardware, poiché le nuove VM in linea consumeranno ciascuna un intero set di risorse del kernel, ma anche i costi monetari. Far girare macchine virtuali su e giù nel tuo ambiente cloud può diventare rapidamente costoso. Questi sono tutti ostacoli che non esistono quando si utilizzano i contenitori come metodo per la distribuzione delle applicazioni. man mano che le nuove VM in linea consumeranno ciascuna un intero set di risorse del kernel, ma anche costi monetari. Far girare macchine virtuali su e giù nel tuo ambiente cloud può diventare rapidamente costoso. Questi sono tutti ostacoli che non esistono quando si

utilizzano i contenitori come metodo per la distribuzione delle applicazioni. man mano che le nuove VM disponibili online consumeranno ciascuna un intero set di risorse del kernel, ma anche costi monetari. Far girare macchine virtuali su e giù nel tuo ambiente cloud può diventare rapidamente costoso. Questi sono tutti ostacoli che non esistono quando si utilizzano i contenitori come metodo per la distribuzione delle applicazioni.

Poiché i contenitori delle applicazioni utilizzano lo stesso kernel sottostante e la stessa immagine di base, il loro tempo di vita è estremamente veloce. I nuovi contenitori possono essere attivati o disattivati molto rapidamente e in batch, senza dover attendere l'avvio dei processi di avvio e in modalità kernel. Inoltre, poiché abbiamo fornito allo sviluppatore questa struttura di contenitore isolata all'interno della quale creare l'applicazione, sappiamo che la nostra applicazione sarà in grado di funzionare con successo ovunque avviamo uno di questi contenitori. Non dovrai più preoccuparti se la nuova VM che sarà online sarà standardizzata correttamente o meno, perché i contenitori per una particolare applicazione sono sempre gli stessi e contengono tutte le dipendenze importanti di cui l'applicazione ha bisogno, proprio all'interno di quel contenitore.

Contenitori e Nano Server

Questo argomento ci riporta alla nostra discussione su Nano Server e sul motivo per cui è parzialmente scomparso come opzione di installazione di Windows Server. Prima di discutere lo scopo che ora serve Nano Server, diamo una rapida occhiata alla struttura di un contenitore basato su Windows. Ecco un grafico preso in prestito da una presentazione di diapositive pubblica che faceva parte di una presentazione di Microsoft Ignite:



Il livello più basso di un contenitore è il sistema operativo di base. Quando si avvia un contenitore, è necessario un set di base di codice e kernel da cui partire. Questo sistema operativo di base può essere Server Core o Nano Server.

Il livello successivo di un contenitore è il livello di personalizzazione. È qui che risiedono le tecnologie che verranno utilizzate alla fine dalla tua applicazione. Ad esempio, i nostri contenitori possono includere IIS per l'hosting di un sito Web, PowerShell o anche qualcosa come .NET. Ognuno di questi set di strumenti risiede in questo livello.

Infine, la fetta superiore della torta contenitore è lo strato di applicazione. Questa, ovviamente, è l'app specifica che prevedi di ospitare all'interno di questo contenitore, a cui accedono i tuoi utenti.

Sebbene Server Core sia un ottimo sistema operativo per la creazione di server piccoli ed efficienti, è ancora un peso massimo rispetto a Nano Server. Nano è così incredibilmente diverso e così incredibilmente piccolo che non è davvero un confronto. Probabilmente ti ricordi prima dove abbiamo installato Server Core e ne è uscito un disco rigido di circa 6 GB. Sebbene sia molto più piccolo di una versione Desktop Experience di Windows Server, pensa a questo. Un'immagine di base di Nano Server può essere inferiore a 500 MB!

È sorprendentemente piccolo. Inoltre, gli aggiornamenti a Nano Server dovrebbero essere pochi e rari. Ciò significa che non dovrai occuparti di patch e aggiornamenti mensili sui contenitori delle applicazioni. Infatti, poiché i contenitori includono tutto ciò di cui hanno bisogno per eseguire le applicazioni ospitate su di essi, è generalmente previsto che quando devi aggiornare qualcosa su un contenitore, dovrai semplicemente andare avanti e costruire una nuova immagine del contenitore, piuttosto piuttosto che aggiornare quelli esistenti. Se Nano Server riceve un aggiornamento, è sufficiente creare un nuovo contenitore, installare e testare l'applicazione su di esso e distribuirlo. Hai bisogno di apportare alcune modifiche all'applicazione stessa? Piuttosto che capire come aggiornare l'immagine del container esistente, è facile e veloce crearne una nuova, testarla al di fuori del proprio ambiente di produzione e, una volta pronta,

Nano Server è ora utilizzato solo come sistema operativo di base per i contenitori. Si tratta di un cambiamento importante rispetto al rilascio di Server 2016, quando l'ambito che Nano avrebbe dovuto fornire era molto più ampio. Se utilizzi Nano Server per carichi di lavoro al di fuori delle immagini del contenitore, devi iniziare a lavorare sullo spostamento di tali carichi di lavoro in server più tradizionali, come Server Core.

Forse ti starai chiedendo: "Perché qualcuno dovrebbe usare Server Core come base per un'immagine container, se Nano Server è disponibile?" La risposta più semplice a questa domanda è la compatibilità delle

applicazioni. Nano Server è incredibilmente piccolo e come tale è ovviamente privo di gran parte del codice che esiste all'interno di Server Core. Quando inizi a cercare di utilizzare i contenitori per ospitare le tue applicazioni, è una buona idea utilizzare il Nano Server più piccolo come base, se possibile, ma spesso le tue applicazioni semplicemente non saranno in grado di funzionare su quella piattaforma e in questi casi, lo farai utilizzare Server Core come sistema operativo di base.

Contenitori di Windows Server e contenitori Hyper-V

Quando si avviano i contenitori, è importante sapere che esistono due categorie di contenitori che è possibile eseguire in Windows Server 2019. Tutti gli aspetti dei contenitori di applicazioni di cui abbiamo parlato finora si applicano ai contenitori di Windows Server o a Hyper-Contenitori V. Come i contenitori di Windows Server, i contenitori Hyper-V possono eseguire lo stesso codice o le stesse immagini al loro interno, pur mantenendo le loro garanzie di forte isolamento per assicurarsi che le cose importanti rimangano separate. La decisione tra l'utilizzo di contenitori di Windows Server o contenitori Hyper-V si ridurrà probabilmente al livello di sicurezza necessario per mantenere i contenitori. Discutiamo le differenze tra i due in modo che tu possa capire meglio la scelta che stai affrontando.

Contenitori di Windows Server

Allo stesso modo in cui i contenitori Linux condividono i file del kernel del sistema operativo host, i contenitori Windows Server utilizzano questa condivisione per rendere efficienti i contenitori. Ciò significa, tuttavia, che mentre lo spazio dei nomi, il filesystem e l'isolamento di rete sono in atto per mantenere i contenitori separati l'uno dall'altro, esiste un potenziale di vulnerabilità tra i diversi contenitori di Windows Server in esecuzione su un server host. Ad esempio, se dovessi accedere al sistema operativo host sul server del contenitore, sarai in grado di vedere i processi in esecuzione di ciascun contenitore. Il contenitore non è in grado di vedere l'host o altri contenitori ed è ancora isolato dall'host in vari modi, ma sapere che l'host è in grado di visualizzare i processi all'interno del contenitore ci mostra che esiste una certa interazione con questo livello di condivisione . I contenitori di Windows Server saranno più utili nelle circostanze in cui il server host del contenitore e i contenitori stessi si trovano all'interno dello stesso limite di attendibilità. Nella maggior parte dei casi, ciò significa che i contenitori di Windows

Server saranno più utili per i server di proprietà dell'azienda e eseguiranno solo contenitori di proprietà dell'azienda e considerati affidabili. Se ti fidi sia del tuo server host che dei tuoi contenitori e sei d'accordo con queste entità che si fidano l'una dell'altra, la distribuzione dei normali contenitori di Windows Server è l'uso più efficiente delle tue risorse hardware. e gestisci solo container di proprietà dell'azienda e di cui si fida. Se ti fidi sia del tuo server host che dei tuoi contenitori e sei d'accordo con queste entità che si fidano l'una dell'altra, la distribuzione dei normali contenitori di Windows Server è l'uso più efficiente delle tue risorse hardware. e gestisci solo container di proprietà dell'azienda e di cui si fida. Se ti fidi sia del tuo server host che dei tuoi contenitori e sei d'accordo con queste entità che si fidano l'una dell'altra, la distribuzione dei normali contenitori di Windows Server è l'uso più efficiente delle tue risorse hardware.

Contenitori Hyper-V

Se stai cercando una maggiore quantità di isolamento e confini più forti, è qui che ti imbatterai nei contenitori Hyper-V. I contenitori Hyper-V sono più simili a una versione super ottimizzata di una macchina virtuale. Sebbene le risorse del kernel siano ancora condivise dai contenitori Hyper-V, quindi sono ancora molto più performanti delle macchine virtuali complete, ogni contenitore Hyper-V ottiene la propria shell Windows dedicata all'interno della quale può essere eseguito un singolo contenitore. Ciò significa che hai un isolamento tra i contenitori Hyper-V che è più alla pari con l'isolamento tra le VM, e tuttavia sei ancora in grado di avviare nuovi contenitori a piacimento e molto rapidamente perché l'infrastruttura del contenitore è ancora al suo posto. I contenitori Hyper-V saranno più utili nelle infrastrutture multi-tenant, dove vuoi assicurarti che nessun codice o attività possa essere trapelato tra il contenitore e l'host o tra due contenitori diversi che potrebbero essere di proprietà di entità diverse. In precedenza, abbiamo discusso in che modo il sistema operativo host può vedere nei processi in esecuzione all'interno di un contenitore di Windows Server, ma questo non è il caso dei contenitori Hyper-V. Il sistema operativo host è completamente inconsapevole e non è in grado di attingere a quei servizi in esecuzione all'interno dei contenitori Hyper-V stessi. Questi processi sono ora invisibili. e incapace di attingere a quei servizi in esecuzione all'interno dei contenitori Hyper-V stessi. Questi processi sono ora invisibili. e incapace di attingere a quei servizi in esecuzione all'interno dei contenitori Hyper-V stessi. Questi processi sono ora invisibili.

La disponibilità dei contenitori Hyper-V significa che anche se si dispone di un'applicazione che deve essere fortemente isolata, non è più necessario dedicare una macchina virtuale Hyper-V completa a questa applicazione. È ora possibile avviare un contenitore Hyper-V, eseguire l'applicazione in quel contenitore e avere un isolamento completo per l'applicazione, continuando a condividere le risorse e fornire un'esperienza migliore e più scalabile per tale applicazione.

Docker e Kubernetes

Docker è un progetto open source - un set di strumenti, in realtà - che è stato originariamente progettato per assistere con l'esecuzione di container su sistemi operativi Linux. Aspetta un attimo, cosa? Le parole Linux e open source scritte ancora una volta all'interno di un libro Microsoft! A cosa sta arrivando questo mondo? Vedete, i container stanno rapidamente diventando un grosso problema, e giustamente. In Server 2016, Microsoft ha intrapreso alcuni passaggi per iniziare a reinventare la ruota dei contenitori, con l'inclusione di cmdlet di PowerShell che potrebbero essere utilizzati per avviare e controllare i contenitori in esecuzione su Windows Server, ma la piattaforma Docker è cresciuta a un ritmo così rapido che Microsoft ora si aspetta davvero che chiunque desideri eseguire contenitori sui propri computer Windows lo farà tramite il set di strumenti Docker. Se desideri utilizzare o persino testare i contenitori nel tuo ambiente, "

Docker è una piattaforma container. Ciò significa che fornisce i comandi e gli strumenti necessari per scaricare, creare, impacchettare, distribuire ed eseguire i contenitori. Docker per Windows è completamente supportato per essere eseguito sia su Windows 10 che su Windows Server 2019. Installando Docker per Windows, acquisisci tutti gli strumenti necessari per iniziare a utilizzare i contenitori per migliorare l'isolamento e la scalabilità dell'applicazione.

Gli sviluppatori hanno la possibilità di utilizzare Docker per creare un ambiente sulla loro workstation locale che rispecchia un ambiente server live, in modo che possano sviluppare applicazioni all'interno di container e avere la certezza che verranno effettivamente eseguite una volta che tali applicazioni vengono spostate sul server. Docker è la piattaforma che fornisce funzionalità di pacchetto, spedizione ed esecuzione per i tuoi sviluppatori. Una volta terminato lo sviluppo, il pacchetto contenitore può essere consegnato all'amministratore di sistema, che avvia i contenitori che eseguiranno l'applicazione e lo distribuisce di conseguenza. Lo sviluppatore non conosce o non si preoccupa dell'infrastruttura host del contenitore e l'amministratore non conosce o non si preoccupa del processo di sviluppo o della compatibilità con i propri server.

Contenitori Linux

È in corso un aggiornamento importante quando si discute delle funzionalità di cui dispone Windows Server 2019 per interagire con diversi tipi di contenitori. In precedenza, in Server 2016, un server host di contenitori Windows poteva eseguire solo contenitori basati su Windows, perché i contenitori di Windows Server condividono il kernel con il sistema operativo host, quindi non era possibile avviare un contenitore Linux su un host Windows.

I tempi stanno cambiando e ora abbiamo alcune nuove funzionalità creative in Server 2019 per gestire scenari come i contenitori Linux. Sebbene queste funzionalità siano ancora in fase di perfezionamento, ci sono alcune nuove opzioni, chiamate Moby VM e LCOW, che consentiranno ai container Linux di funzionare su un host container di

Windows Server, anche in esecuzione fianco a fianco con i container di Windows!

Questo è tutto abbastanza nuovo e ancora in fase di costruzione che ulteriori dettagli sono in arrivo, ma visita questo link per controllare lo stato corrente di queste nuove funzionalità se sei interessato a eseguire contenitori Linux: https: //documenti.microsoft.com /en-noi/virtualizzazione / windowscontainers /schierarecontenitori /linux-contenitori.

Docker Hub

Quando lavori con i contenitori, crei immagini di contenitori utilizzabili su qualsiasi istanza del server che esegue lo stesso sistema operativo host: questa è l'essenza di ciò che i contenitori ti consentono di fare. Quando fai girare nuove istanze di contenitori, stai semplicemente estraendo nuove copie di quell'immagine esatta, che è all-inclusive. Questo tipo di mentalità di imaging standardizzato si presta bene a una comunità condivisa di immagini, un deposito, per così dire, di immagini che le persone hanno costruito che potrebbero beneficiare gli altri. Docker è open source, dopotutto.
Esiste una risorsa di condivisione di questo tipo, che puoi visitare per prendere i file di immagine del contenitore per il test o anche per caricare le immagini che hai creato e condividerle con il mondo? Assolutamente! Si chiama Docker Hub ed è disponibile all'indirizzohttps://hub.docker.com.

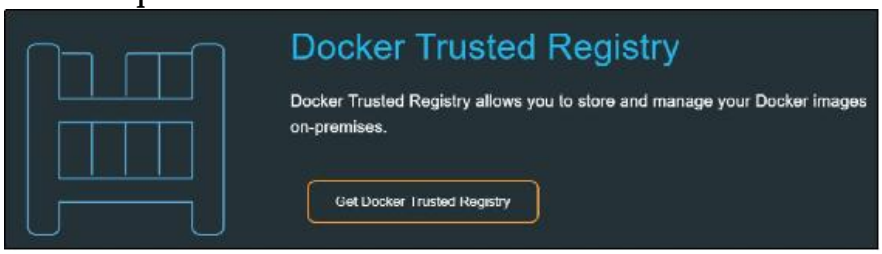
Visita questo sito e crea un login e avrai immediatamente accesso a migliaia di immagini di base del contenitore che la comunità ha creato e caricato. Questo può essere un modo rapido per far funzionare un laboratorio con contenitori e molte di queste immagini di contenitori potrebbero anche essere utilizzate per sistemi di produzione, eseguendo le applicazioni che le persone qui hanno preinstallato per te all'interno di queste immagini di contenitori. Oppure puoi utilizzare Docker Hub per caricare e archiviare le tue immagini del contenitore:


docker hub
Search for great content (e.g., mysql)
Explore
Repositories
Organizations
Get Help
jordankrause
Welcome to Docker Hub
Here are a few things to get you started.
Create a Repository
Push container images to Docker Hub
Create an Organization
Manage Docker Hub repositories with your team

In effetti, dovresti davvero andare avanti e creare un account per Docker Hub ora, perché se vuoi seguire più avanti nel capitolo e testare l'implementazione di un container con Docker, avrai bisogno di un accesso per farlo.

Registro affidabile Docker

Se sei come me, pensi che l'idea di Docker Hub sia fantastica: un posto pulito dove archiviare immagini e persino per condividerle tra la comunità. Tuttavia, la mia prossima inclinazione è guardarla attraverso un cannocchiale dell'Enterprise, che cambia rapidamente la mia prospettiva
da pulito a non protetto. In altre parole, potresti non sentirti a tuo agio nel posizionare le immagini in questo archivio pubblico. Certamente non immagini che contengono qualcosa di sensibile alla tua organizzazione, comunque.



Qui è dove Docker Trusted Registry potrebbe essere qualcosa da esaminare. Docker Trusted Registry è un sistema di repository di immagini del contenitore, simile a Docker Hub, ma è qualcosa che puoi contenere all'interno della tua rete, dietro i tuoi firewall e sistemi di sicurezza. Questo ti dà un sistema di repository di immagini del contenitore senza il rischio di condividere informazioni sensibili con il resto del mondo.

Kubernetes

Mentre Docker è la nostra interfaccia principale per la creazione e l'hosting di container, permettendoci di creare piattaforme all'interno

delle quali possiamo ospitare applicazioni in questo modo nuovo ed entusiasmante, la vera magia arriva dopo aver finito con la configurazione del container. Diamo uno sguardo al futuro e supponiamo che tu abbia un'applicazione ora ospitata con successo all'interno di un contenitore. Questo contenitore può essere avviato su un server host del contenitore nel tuo ambiente o persino spostato facilmente su un host contenitore di Azure. Ciò fornisce una facile interazione con l'infrastruttura necessaria per essere in grado di scalare senza problemi questa applicazione verso l'alto o verso il basso, ma c'è un pezzo mancante in questa scalabilità: l'orchestrazione.

Kubernetes è una soluzione di orchestrazione dei contenitori. Ciò significa che Kubernetes orchestra o facilita il modo in cui vengono eseguiti i contenitori. È lo strumento che consente a molti contenitori di funzionare insieme, in armonia, come se fossero un'unica grande applicazione. Se intendi utilizzare contenitori per creare applicazioni di ridimensionamento che hanno la capacità di avviare nuovi contenitori ogni volta che sono necessarie risorse aggiuntive, dovrai assolutamente disporre di un agente di orchestrazione dei contenitori e Kubernetes è attualmente il migliore e il più popolare.

Microsoft ha riconosciuto questa popolarità e ha adottato misure per garantire che Kubernetes sia completamente supportato su Windows Server 2019.

Come con qualsiasi software, Kubernetes non è l'unico nome nel gioco. In effetti, Docker ha una propria piattaforma di orchestrazione, chiamata Docker Swarm. Sebbene possa avere senso che Docker e Docker Swarm funzionino insieme meglio di Docker e qualsiasi altro orchestratore, i numeri non mentono. Un recente rapporto mostra che l'82% delle aziende che utilizzano applicazioni di ridimensionamento nel cloud utilizza Kubernetes per l'orchestrazione dei contenitori.

Come accennato in precedenza, strumenti come contenitori, Docker e Kubernetes fanno parte di un file
visione cloud-first. Sebbene l'utilizzo dei container per la maggior parte delle aziende inizierà in loco, utilizzando i propri server e infrastrutture per l'hosting dei container, questa è una tecnologia che è già in grado di estendersi al cloud. Poiché i contenitori stessi sono così standardizzati e fluidi, il che li rende facili da espandere e spostare, è facile farli scorrere in un ambiente cloud.

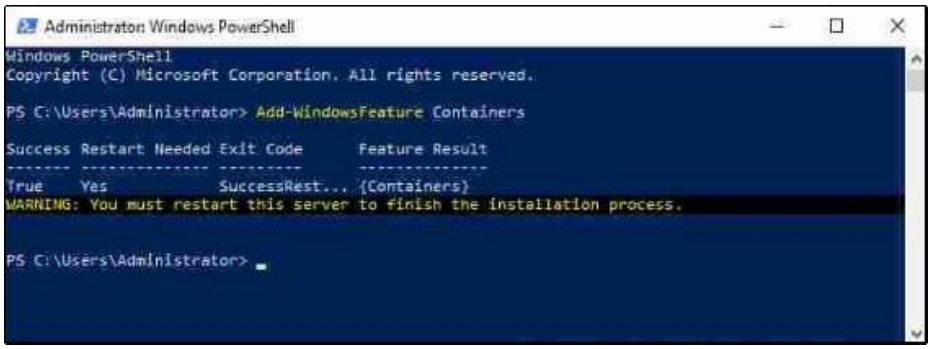
Lavorare con i contenitori

Ci sono molti pezzi in movimento che lavorano insieme per rendere i contenitori una realtà nel tuo ambiente, ma non è davvero troppo difficile iniziare. Esaminiamo la configurazione iniziale per trasformare Windows Server 2019 in una mega macchina in esecuzione su container.

Installazione del ruolo e della funzionalità

La quantità di lavoro che devi svolgere qui dipende dal fatto che tu voglia eseguire contenitori di Windows Server, contenitori Hyper-V o entrambi. La funzionalità principale di cui hai bisogno per assicurarti di installare è Contenitori, che possono essere installati utilizzando il collegamento Aggiungi ruoli e funzionalità dall'interno di Server Manager o emettendo il seguente comando di PowerShell:

```
Contenitori Add-WindowsFeature
```



Inoltre, se intendi eseguire contenitori Hyper-V, devi assicurarti che i componenti Hyper-V sottostanti siano installati anche sul server host del contenitore. A tale scopo, installare il ruolo Hyper-V e gli strumenti di gestione associati su questo stesso server.

Come indicato in seguito all'installazione di ruoli e funzionalità, assicurati di riavviare il server dopo queste modifiche.

A questo punto, ti starai chiedendo: "Se il mio server host contenitore deve avere installato il ruolo Hyper-V, non significa che deve essere un server fisico? Non puoi installare il ruolo Hyper-V su un server virtuale macchina, giusto? " Sbagliato. Windows Server 2019 supporta qualcosa chiamato virtualizzazione annidata, che è stata aggiunta ai fini dei contenitori. Vedete, la richiesta di hardware fisico sta diventando un fattore limitante per i reparti IT in questi giorni, poiché quasi tutto viene eseguito da macchine virtuali. È logico che le aziende vogliano distribuire container, ma potrebbero anche volere che i loro server host container siano VM, con più container in esecuzione all'interno di quella VM. Pertanto, per renderlo possibile, era necessaria la virtualizzazione annidata. Se stai utilizzando un server hypervisor fisico di Windows Server 2019, e una macchina virtuale Windows Server 2019 all'interno di quel server, ora scoprirai che sei in grado di installare correttamente il ruolo Hyper-V direttamente su quella VM. Ti ho detto che le macchine virtuali erano popolari, tanto che ora vengono utilizzate per eseguire altre macchine virtuali!

Ricorda che possiamo anche ospitare ed eseguire container sui nostri computer Windows 10! Per preparare un client Win10 a questo scopo, è sufficiente aggiungere la funzionalità di Windows denominata Contenitori, proprio come nel sistema operativo del server

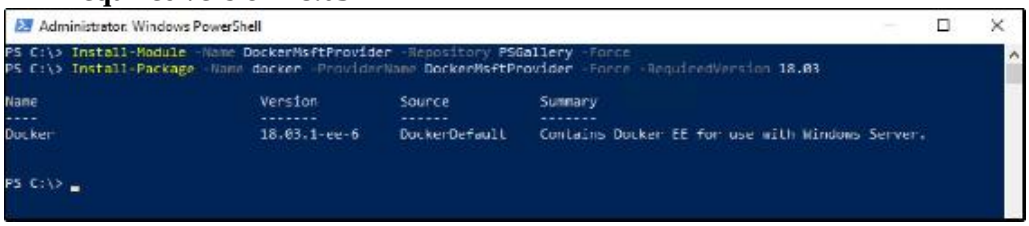
Installazione di Docker per Windows

Ora che il nostro server host del contenitore è preparato con i componenti Windows necessari, dobbiamo prendere Docker per Windows da Internet. L'interfaccia Docker ci fornirà tutti i comandi necessari per iniziare a costruire e interagire con i nostri container.

Questo è il punto in cui l'accesso a Docker Hub diventa importante. Se stai lavorando per testare i contenitori sulla tua workstation e devi installare Docker Desktop per Windows sul tuo client Win10, il modo più semplice è visitare Docker Hub, accedere e cercare il software client Docker. Ecco un collegamento a quel software (questo è lo strumento che devi utilizzare se stai installando su Windows 10):https: //centro.docker.com /edizioni / Comunit à /docker-ce-desktopfinestre.

Tuttavia, poiché sono seduto su un Windows Server 2019, la mia licenza per il server include anche la licenza per Docker Enterprise, che può essere ritirata senza dover visitare Docker Hub. Se apro un prompt di PowerShell con privilegi elevati ed eseguo i seguenti due comandi, il mio server raggiungerà Docker Enterprise e lo installerà sul mio server:

Modulo di installazione -Nome DockerMsftProvider -Repository PSGallery -Force
Install-Package -Nome docker -ProviderName DockerMsftProvider -Force -RequiredVersion 18.03



Al termine dell'installazione del pacchetto, Docker è ora configurato sul tuo server come servizio, ma quel servizio deve essere avviato con il seguente comando:

Finestra mobile Avvia servizio

Comandi Docker

Una volta che Docker è installato sul tuo sistema, che tu stia lavorando con un computer Windows Server 2019 o Windows 10, ora hai il Docker Engine in esecuzione sul tuo computer ed è pronto ad accettare alcuni comandi per iniziare a lavorare con i contenitori. Se c'è una sola parola da ricordare quando si tratta di lavorare con i contenitori, è Docker. Questo perché ogni comando emesso per interagire con i contenitori inizierà con la parola docker. Diamo un'occhiata ad alcuni dei comandi comuni con cui lavorerai.

docker --help

Questo è ordinario come l'emissione di docker / ?, se fosse un vero comando. La funzione di aiuto per Docker genererà un elenco dei possibili comandi Docker disponibili per l'esecuzione. Questo è un buon punto di riferimento quando inizi.

immagini docker

Dopo aver scaricato alcune immagini del contenitore da un repository (lo faremo da soli nella prossima sezione di questo capitolo), è possibile utilizzare il comando docker images per visualizzare tutte le immagini disponibili sul sistema locale.

ricerca docker

Utilizzando il la funzione di ricerca ti consente di cercare nei repository del contenitore (come Docker Hub) le immagini del contenitore di base che potresti voler utilizzare nel tuo ambiente. Ad esempio, per cercare e trovare immagini fornite dall'interno del repository Docker Hub di Microsoft, emettere quanto segue:

```
docker search microsoft
```

docker pull

Possiamo usare docker pull per tirare giù immagini del contenitore a partire dal in linea archivi. Là sono più repository da cui è possibile ottenere immagini del contenitore. Molto spesso, lavorerai con immagini da Docker Hub, da cui estrarremo a breve un'immagine del contenitore. Tuttavia, esistono altri repository online da cui è possibile ottenere immagini del contenitore, come il registro pubblico dei contenitori di Microsoft, noto come MCR.

Di seguito sono riportati alcuni comandi pull di Docker di esempio che mostrano come eseguire il pull delle immagini del contenitore da Docker Hub, oltre a MCR:

docker pull Microsoft \ nanoserver
docker pull Microsoft \ windowsservercore
pull dell'immagine docker mcr.microsoft.com/windows/servercore:1809
pull dell'immagine docker mcr.microsoft.com/windows/nanoserver:1809

docker run

Questo è il comando per avviare un nuovo contenitore da un'immagine di base. Scoprirai che puoi conservare più immagini del contenitore nel tuo repository locale che sono tutte basate sulla stessa immagine del contenitore. Ad esempio, quando aggiungi nuove cose ai tuoi contenitori o aggiorni l'applicazione all'interno dei tuoi contenitori, potresti creare nuove immagini del contenitore che ora sono un sottoinsieme di un'immagine del contenitore esistente. Ad esempio, potresti avere numerose immagini del contenitore che sono tutte denominate windowsservercore. In questo caso, i tag del contenitore diventano molto importanti, poiché i tag ti aiutano a distinguere tra le diverse versioni di quelle immagini del contenitore. Ad esempio, ecco un comando che avrebbe avviato un contenitore basato su un'immagine windowsservercore per la quale avevo associato il tag ltsc2019:

docker run -it --rm Microsoft \ windowsservercore: ltsc2019

Nel precedente il comando -it crea una shell da cui possiamo interagire con un container, utile per costruire e testare container, ma generalmente non avresti bisogno di questo switch per lanciare container di produzione che erano pronti al 100% per servire applicazioni. --rm è un'opzione di pulizia, il che significa che una volta che questo particolare contenitore è uscito, il contenitore e il suo filesystem verranno automaticamente cancellati.

docker ps -a

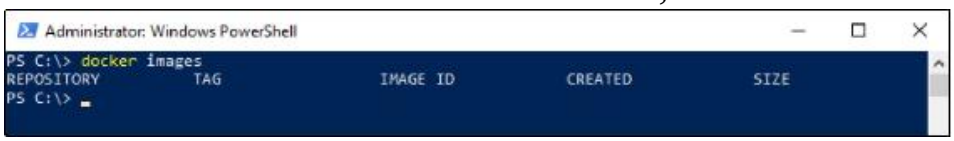
voi utilizzare docker ps quando si desidera visualizzare i contenitori attualmente in esecuzione sul sistema.

informazioni docker

Questo riepilogherà il tuo ambiente Docker, incluso il numero di contenitori in esecuzione e ulteriori informazioni sulla piattaforma host stessa.

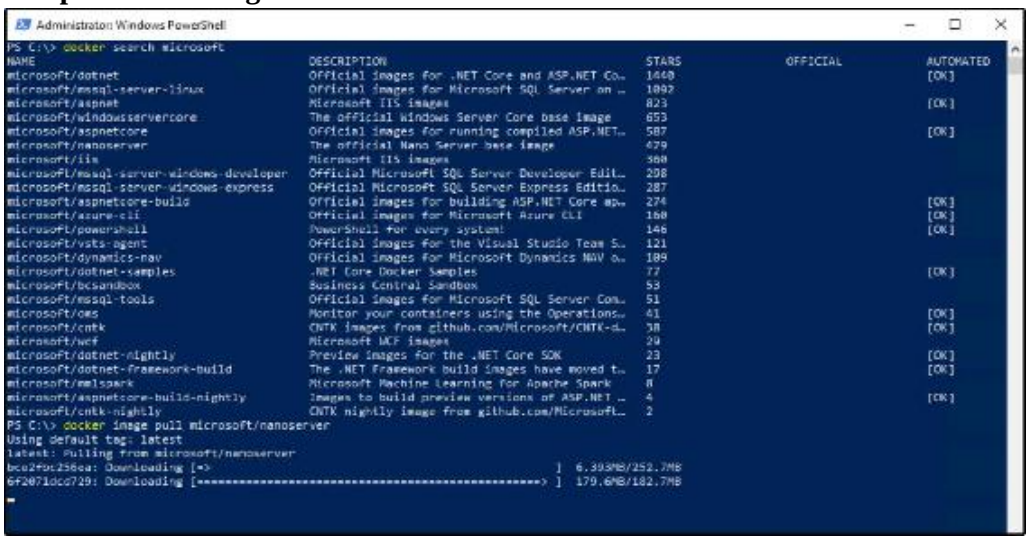
Download di un'immagine del contenitore

Il primo comando che eseguiremo sul nostro host container appena creato è docker images, che ci mostra tutte le immagini container che attualmente risiedono sul nostro sistema; non ce ne sono:



Ovviamente non ci sono ancora immagini del contenitore, poiché non ne abbiamo scaricate nessuna. Prendiamone un paio in modo da poterlo testare. Esiste un file di immagine del contenitore di esempio fornito da Team .NET che mostra l'esecuzione di un'applicazione .NET all'interno di un contenitore Nano Server: questo
uno suona come un modo divertente per iniziare a verificare che posso eseguire correttamente i contenitori su questo nuovo server host. Innanzitutto, possiamo utilizzare la ricerca docker per controllare le immagini del contenitore correnti che risiedono nel repository Docker Hub di Microsoft. Una volta trovata l'immagine che vogliamo scaricare, usiamo docker pull per scaricarla sul nostro server:

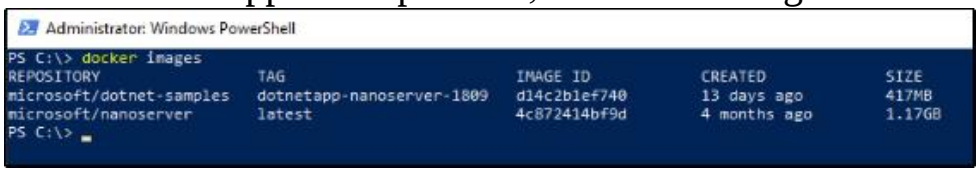
docker search microsoft
pull dell'immagine docker microsoft / nanoserver



Il comando precedente ha scaricato una copia dell'immagine di base standard di Nano Server, ma vogliamo che il nostro contenitore faccia qualcosa alla fine, quindi ecco un comando che scaricherà anche quell'immagine di esempio .NET:

pull dell'immagine docker microsoft / dotnet-samples: dotnetapp-nanoserver-1809

Dopo che i download sono terminati, l'esecuzione delle immagini Docker ancora una volta ci mostra il file immagine del contenitore di Nano Server appena disponibile, nonché l'immagine di esempio .NET:



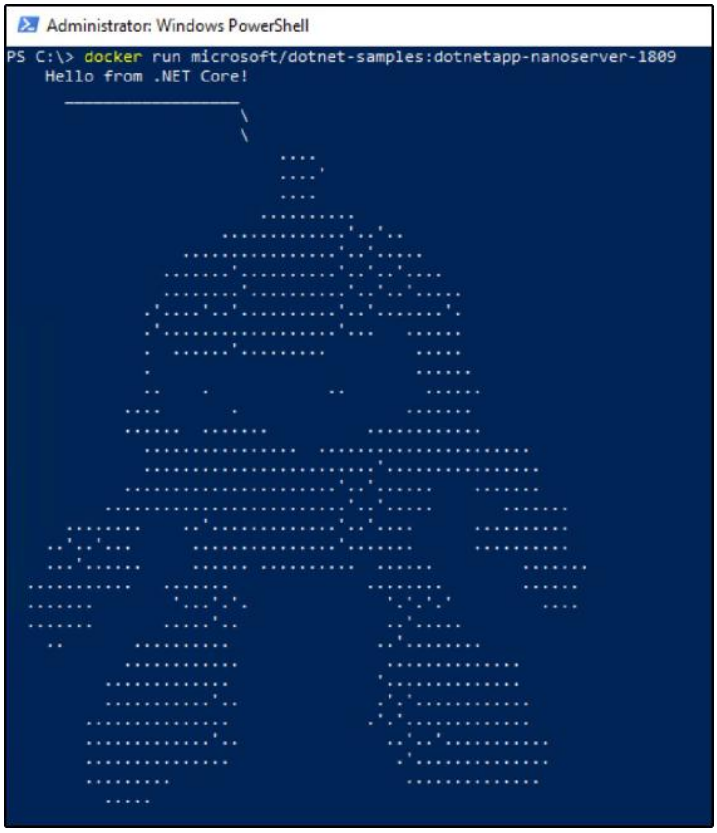
Da queste immagini di base siamo ora in grado di lanciare ed eseguire un vero e proprio container.

Gestire un container

Siamo così vicini ad avere un container in esecuzione sul nostro host! Ora che abbiamo installato il servizio, implementato Docker, importato il modulo Docker nel nostro prompt di PowerShell e scaricato un'immagine del contenitore di base, possiamo finalmente emettere un comando per avviare un contenitore da quell'immagine. Eseguiamo il contenitore .NET che abbiamo scaricato in precedenza:

docker esegue microsoft / dotnet-samples: dotnetapp-nanoserver-1809

Il contenitore si avvia ed esegue il codice incluso e vediamo alcuni output divertenti:



Questo contenitore mostra che tutti i componenti necessari per l'esecuzione di questa applicazione .NET sono inclusi all'interno del contenitore. Questo contenitore è basato su Nano Server, il che significa che ha un ingombro incredibilmente ridotto. In effetti, guardando indietro di alcune pagine all'ultimo comando di immagini Docker che abbiamo eseguito, posso vedere che questa immagine del contenitore è di soli 417 MB! Che risparmio di risorse, rispetto all'esecuzione di questa applicazione su un server Web IIS tradizionale.

La risorsa principale per la documentazione Microsoft sui contenitori è https://aka.ms/windowscontainers. Gli strumenti utilizzati per interagire con i contenitori cambiano costantemente, comprese le modifiche a Docker e Kubernetes. Assicurati di controllare il sito di Microsoft Docs per trovare le best practice più recenti e il percorso di installazione approvato per la preparazione dei server host del contenitore.

Sommario

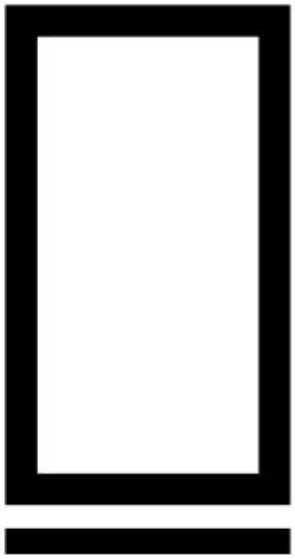
I container rivoluzioneranno il modo in cui costruiamo e ospitiamo applicazioni moderne. Contenendo le app, saremo in grado di eseguire molte più applicazioni su ciascun server fisico, perché sono in grado di essere completamente isolate l'una dall'altra.
Inoltre, la mentalità del contenitore consente lo sviluppo di applicazioni in modo molto più fluido. Gli sviluppatori di app possono creare le loro applicazioni all'interno di contenitori in esecuzione sui propri laptop e, una volta terminate, semplicemente consegnarle al team dell'infrastruttura per far scorrere l'immagine del contenitore su un server host del contenitore di produzione. Quel server host potrebbe essere in sede o anche nel cloud. Strumenti di orchestrazione come Kubernetes possono quindi essere sfruttati per scalare tale applicazione, aumentando o diminuendo la capacità delle risorse e il numero di contenitori necessari in base al carico o ad altri fattori. L'usabilità dei container nel mondo reale è stata notevolmente ampliata dal progetto Docker. I ragazzi di Docker sono chiaramente i primi in questo spazio, tanto che Microsoft ha deciso di incorporare l'uso di Docker - un progetto open source sviluppato da Linux! - direttamente in Windows Server 2019. Ora possiamo utilizzare sia il motore Docker per eseguire container sui nostri server Windows, sia il set di strumenti client Docker per gestire e manipolare i container all'interno di Windows nello stesso modo in cui possiamo lavorare con i container nel mondo Linux .

I contenitori Linux e i contenitori Windows Server hanno molto in comune e funzionano sostanzialmente allo stesso modo. L'idea geniale di Microsoft di creare un ulteriore ambito di container, il container Hyper-V, offre una solida risposta a molte domande di sicurezza comuni che si presentano quando ci si avvicina all'idea di container in generale. Tutti usano pesantemente le macchine virtuali in questi giorni; Non credo che nessuno possa essere in disaccordo con questo. Supponendo che l'uso dei contenitori si evolva in qualcosa di facile da implementare e amministrare, prevedo che i contenitori Hyper-V sostituiranno molte delle nostre macchine virtuali Hyper-V esistenti nei prossimi anni. Ciò consentirà di risparmiare tempo, denaro e spazio sul server.

Parlando di Hyper-V, oggi è diventato una parte integrante di tante delle nostre reti aziendali. Nel prossimo e ultimo capitolo, impareremo di più su questa straordinaria tecnologia di virtualizzazione.

Domande

1. Un contenitore di Windows Server può eseguire un sistema operativo di base di due tipi diversi, cosa sono?
2. Rispetto a un contenitore di Windows Server, quale tipo di contenitore offre livelli di isolamento ancora maggiori?
3. Vero o falso: in Windows Server 2016 era possibile eseguire contenitori sia Windows che Linux sulla stessa piattaforma host Windows Server.
4. Qual è il comando Docker per visualizzare un elenco di immagini del contenitore sul tuo sistema locale?
5. Qual è attualmente il software di orchestrazione dei contenitori più popolare che si integra con Windows Server 2019?
6. Vero o falso: gli sviluppatori possono installare Docker sulle loro workstation Windows 10 per iniziare a creare applicazioni all'interno dei container.



Virtualizzazione del tuo data center con Hyper-V

Sono sempre stato un ragazzo di campagna. Guidare strade sterrate, lavorare sulle auto e cacciare tendono a riempire il mio tempo libero. Viaggiare in città, e in particolare un recente viaggio a Hong Kong, mi colpisce sempre con un po 'di shock culturale. Tutti quei grattacieli e palazzi alti hanno però uno scopo importante e servono a realizzare la mia metafora: se non c'è abbastanza terra per crescere verso l'esterno, devi costruire. L'ascensione verticale delle grandi città è simile a ciò che abbiamo visto accadere nei nostri data center negli ultimi dieci anni. Le città hanno bisogno di sempre più posti per le persone e le imprese, proprio come noi abbiamo bisogno di ospitare sempre più server ogni anno. Piuttosto che un'espansione orizzontale, con enormi sale server piene di rack e rack di hardware, stiamo abbracciando la mentalità del grattacielo e virtualizzando tutto. Costruiamo un numero

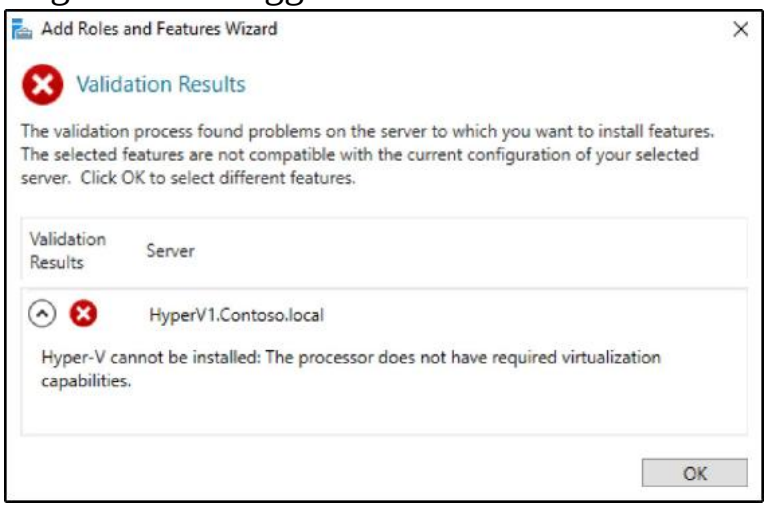
considerevolmente inferiore di server, ma li rendiamo incredibilmente potenti. Quindi, in cima a questi super computer, possiamo eseguire dozzine, se non centinaia, di server virtuali. La tecnologia che fornisce questo livello hypervisor, la capacità di eseguire macchine virtuali (VM) nei negozi incentrati su Microsoft, è il ruolo Hyper-V in Windows Server. Questo è uno dei ruoli più critici da comprendere come amministratore di server, perché se la tua organizzazione non sta ancora utilizzando la virtualizzazione del server, fidati di me quando dico che lo sarà presto. La virtualizzazione è la via del futuro. Di seguito sono riportati alcuni argomenti che esploreremo in modo da poter acquisire familiarità con le funzionalità di virtualizzazione fornite da Microsoft in Windows Server 2019: di server virtuali. La tecnologia che fornisce questo livello hypervisor, la capacità di eseguire macchine virtuali (VM) nei negozi incentrati su Microsoft, è il ruolo Hyper-V in Windows Server. Questo è uno dei ruoli più critici da comprendere come amministratore di server, perché se la tua organizzazione non sta ancora utilizzando la virtualizzazione del server, fidati di me quando dico che lo sarà presto. La virtualizzazione è la via del futuro. Di seguito sono riportati alcuni argomenti che esploreremo in modo da poter acquisire familiarità con le funzionalità di virtualizzazione fornite da Microsoft in Windows Server 2019: di server virtuali. La tecnologia che fornisce questo livello hypervisor, la capacità di eseguire macchine virtuali (VM) nei negozi incentrati su Microsoft, è il ruolo Hyper-V in Windows Server. Questo è uno dei ruoli più critici da comprendere come amministratore di server, perché se la tua organizzazione non sta ancora utilizzando la virtualizzazione del server, fidati di me quando dico che lo sarà presto. La virtualizzazione è la via del futuro. Di seguito sono riportati alcuni argomenti che esploreremo in modo da poter acquisire familiarità con le funzionalità di virtualizzazione fornite da Microsoft in Windows Server 2019: perché se la tua organizzazione non utilizza ancora la virtualizzazione dei server, fidati di me quando dico che sarà presto. La virtualizzazione è la via del futuro. Di seguito sono riportati alcuni argomenti che esploreremo in modo da poter acquisire familiarità con le funzionalità di virtualizzazione fornite da Microsoft in Windows Server 2019: perché se la tua organizzazione non utilizza ancora la virtualizzazione dei server, fidati di me quando dico che sarà presto. La

virtualizzazione è la via del futuro. Di seguito sono riportati alcuni argomenti che esploreremo in modo da poter acquisire familiarità con le funzionalità di virtualizzazione fornite da Microsoft in Windows Server 2019:

- Progettazione e implementazione del server Hyper-V utilizzando switch virtuali
- Implementazione di un nuovo server virtuale Gestione di un server virtuale VM schermate
- Integrazione con Linux
- **File system resiliente** (ReFS) deduplicazione Hyper-V Server 2019

Progettare e implementare il tuo server Hyper-V

Creare il tuo server Hyper-V è in genere piuttosto semplice: crea un server, installa il ruolo Hyper-V e sei pronto per iniziare. In effetti, puoi persino installare il ruolo Hyper-V su un computer Windows 10 Pro o Enterprise, se devi eseguire alcune macchine virtuali dal tuo desktop. Mentre la maggior parte dell'hardware che viene creato in questi giorni supporta pienamente l'idea di essere un provider di hypervisor, alcuni di voi potrebbero provare a installare il ruolo Hyper-V solo per finire con il seguente messaggio di errore:

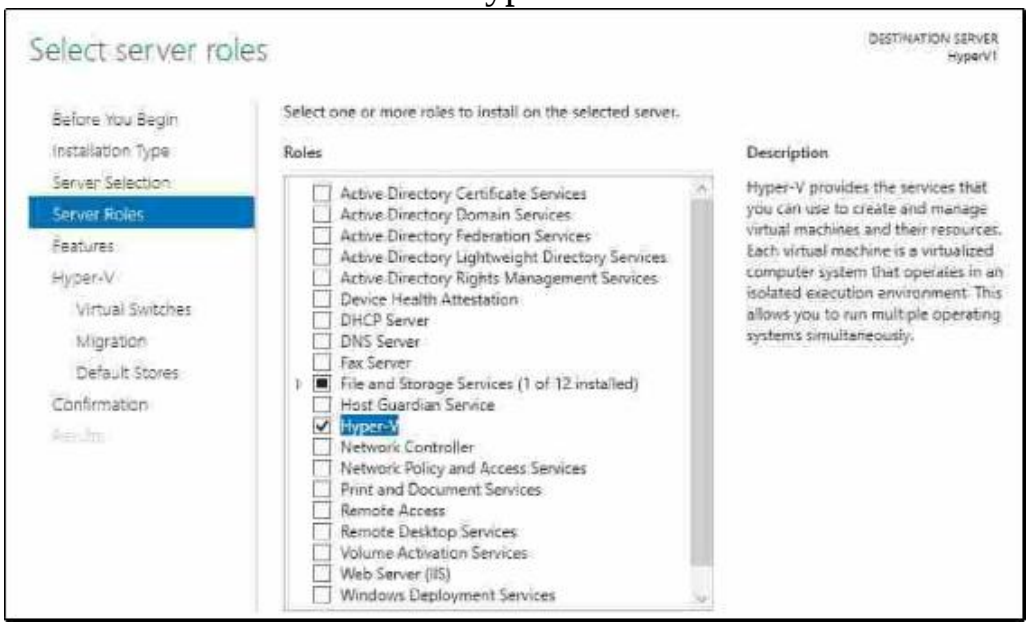


Oh oh, non va bene. Ciò significa una delle due cose: o la mia CPU non supporta davvero la virtualizzazione, o semplicemente ho alcune impostazioni disattivate all'interno del BIOS sul mio server che ne impediscono il funzionamento. Ci sono tre considerazioni che dovresti controllare sul tuo server per assicurarti che sia pronto per eseguire Hyper-V. Innanzitutto, è necessario eseguire un processore basato su x64. Questo è un dato di fatto, dal momento che Windows Server 2019 è comunque disponibile solo a 64 bit. Se non hai un processore x64, non sarai in grado di installare il sistema operativo in primo luogo. In secondo luogo, le CPU devono essere in grado di eseguire la virtualizzazione assistita dall'hardware. Questo è in genere chiamato Intel Virtualization Technology (Intel VT) o AMD Virtualization (AMD-V). Ultimo ma non meno importante, è necessario disporre di Protezione esecuzione programmi (DEP) disponibile e abilitata sul sistema. Se hai esaminato l'hardware stesso e sembra che sia in grado di virtualizzare, ma non funziona ancora, è probabile che tu abbia DEP attualmente disabilitato all'interno del BIOS di quel sistema.
Avvia le impostazioni del BIOS e abilita DEP, insieme a qualsiasi altra impostazione con nome più intuitivo che potrebbe indicare che attualmente sta bloccando la tua capacità di eseguire macchine virtuali.

Finché i tuoi processori sono felici di eseguire macchine virtuali, puoi trasformare qualsiasi dimensione di hardware in un hypervisor installando il ruolo Hyper-V. Non è importante pensare ai requisiti minimi di sistema perché si desidera che l'hardware di sistema sia il più grande possibile in un server Hyper-V. Più core della CPU, RAM e spazio su disco rigido puoi fornire, più VM sarai in grado di eseguire. Anche i server Hyper-V più piccoli che ho visto negli ambienti di produzione eseguono hardware come due processori Xeon, 96 GB di RAM e molti terabyte di spazio di archiviazione. Mentre 96 GB di RAM possono sembrare molti per un singolo sistema, se la build del server del carico di lavoro standard include 8 GB di RAM, che è un numero piuttosto basso, e desideri eseguire 12 server sul tuo server Hyper-V, sei già oltre le capacità di un server Hyper-V con solo 96 GB di RAM. 8 per 12 fa 96 e non hai lasciato memoria da usare per il sistema operativo host! Quindi la morale della storia? Andare Grande o andare a casa!

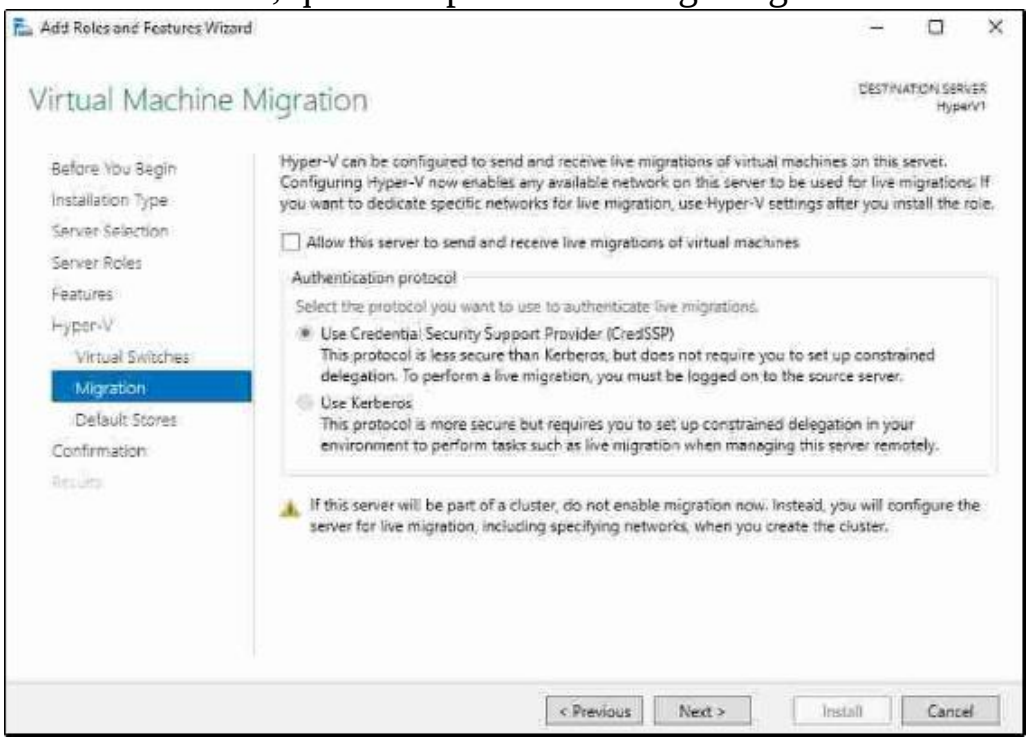
Installazione del ruolo Hyper-V

Hyper-V è solo un altro ruolo in Windows Server 2019, ma durante l'installazione di quel ruolo, ti verranno poste alcune domande ed è importante capire cosa stanno chiedendo, in modo da poter essere sicuro del tuo nuovo Hyper-V Server è costruito per durare e per funzionare in modo efficiente. Prima di tutto, dovrai avere Windows Server 2019 già installato e utilizzare la funzione Aggiungi ruoli e funzionalità per installare il ruolo chiamato Hyper-V:



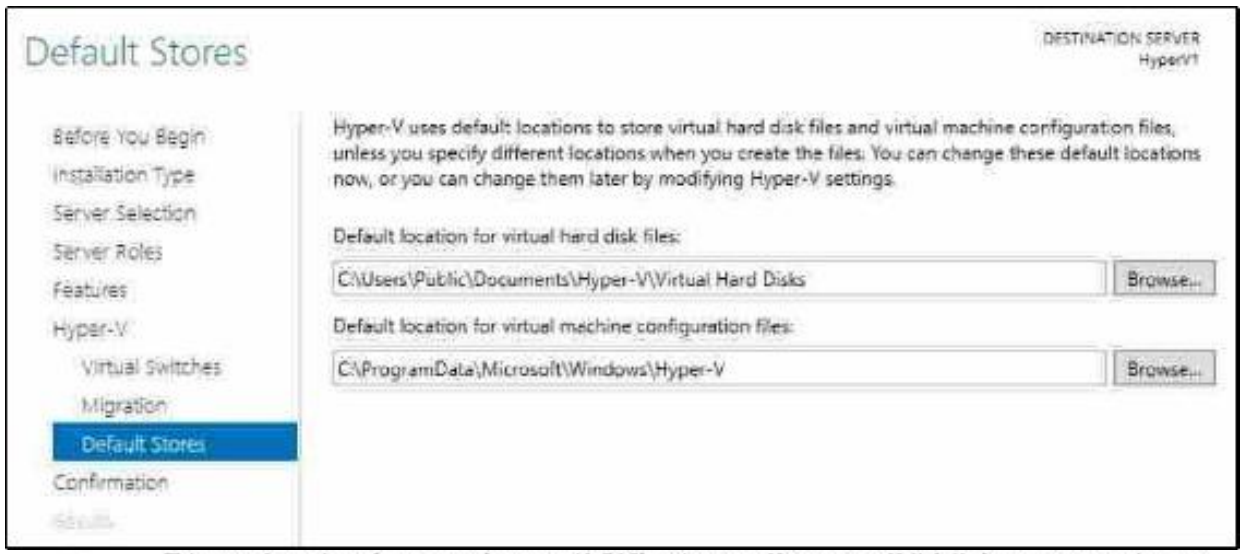
Mentre continui a lavorare attraverso la procedura guidata per installare il ruolo, ti imbatti in una schermata denominata Crea switch virtuali. Discuteremo un po 'più di rete in Hyper-V nella prossima sezione di questo capitolo, ma ciò che è importante qui è che tu possa definire quale delle schede NIC fisiche del tuo server sarà collegata a Hyper-V e disponibile per il tuo computer virtuale macchine da utilizzare. È consigliabile che ogni server Hyper-V disponga di più schede di rete. Si desidera una scheda NIC dedicata all'host stesso, che non si selezionerà in questa schermata. Lascialo da solo per le comunicazioni dell'hypervisor. Oltre a quella NIC, ti servirà almeno una scheda di rete in grado di collegare le VM alla rete aziendale. Questo lo selezioneresti, come puoi vedere nello screenshot imminente. Se ospiterete molte VM diverse su questo server,

Dopo aver definito le schede di rete, dobbiamo decidere se questo server Hyper-V sarà in grado di gestire la migrazione in tempo reale delle macchine virtuali. La migrazione delle VM in tempo reale è la capacità di spostare una VM da un host Hyper-V a un altro, senza alcuna interruzione del servizio su quella VM. Come puoi vedere nello screenshot seguente, ci sono un paio di modi diversi in cui puoi configurare il server per prepararlo per la gestione delle migrazioni in tempo reale e prendi nota del testo in basso che ti dice di lasciare questa opzione da sola per ora se si prevede di rendere questo server Hyper-V parte di un cluster. Negli ambienti cluster, queste impostazioni vengono gestite a un livello diverso:



L'ultima schermata che volevo sottolineare è la definizione delle posizioni di archiviazione per i dati della VM. Dopo aver creato le VM e aver analizzato il loro aspetto a livello del disco rigido (guardando i file effettivi che vengono creati per VM), vedrai che ci sono due aspetti chiave di una VM: il file del disco rigido virtuale, Virtual Disco rigido (VHD) o VHDX e una cartella che contiene i file di configurazione per quella VM.

Come puoi vedere nello screenshot imminente, le posizioni predefinite per la memorizzazione di questi elementi sono qualcosa che ti aspetteresti da un'applicazione client che stavi installando su un laptop, ma non ti aspetteresti che qualcosa di pesante come Hyper-V memorizzi il suo core in una cartella Documenti utente condivisa. Suppongo che dal momento che Microsoft non conosce la configurazione del tuo server, non può fare ipotesi reali su dove vuoi davvero memorizzare quei dati, e quindi imposta l'impostazione predefinita per essere qualcosa che funzionerebbe tecnicamente, ma probabilmente dovrebbe essere modificato come una questione di migliori pratiche. Molti server Hyper-V avranno uno spazio di archiviazione dedicato, anche se solo un disco rigido separato, su cui è prevista l'archiviazione di questi file. Assicurati di dedicare un minuto a questa schermata e modificare le posizioni di archiviazione predefinite dei file della VM:

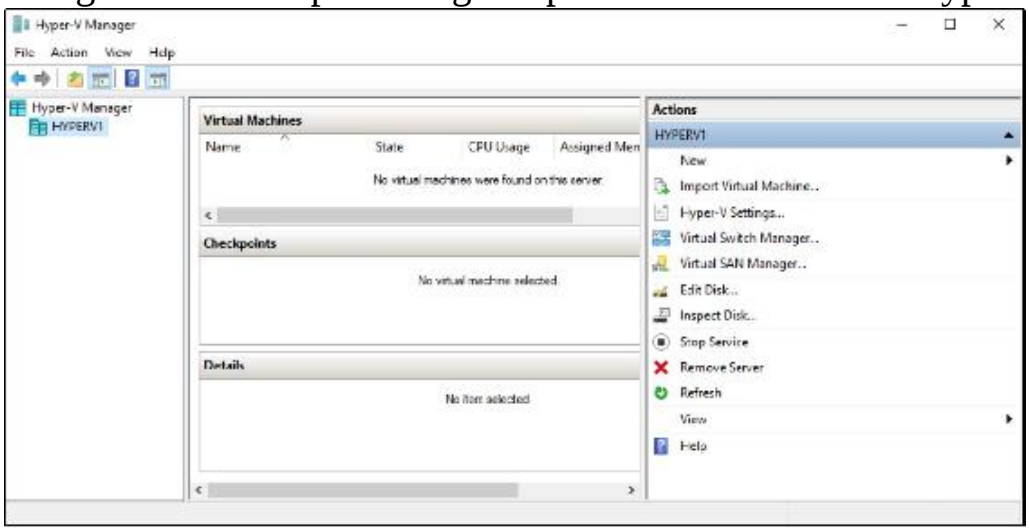


Ricorda che la versione di Windows Server 2019 in esecuzione determina il numero di VM che potrai eseguire su questo host. Server 2019 Standard ti limita a eseguire due VM, mentre l'edizione Datacenter ti consente di avviarne quante ne puoi inserire nell'hardware

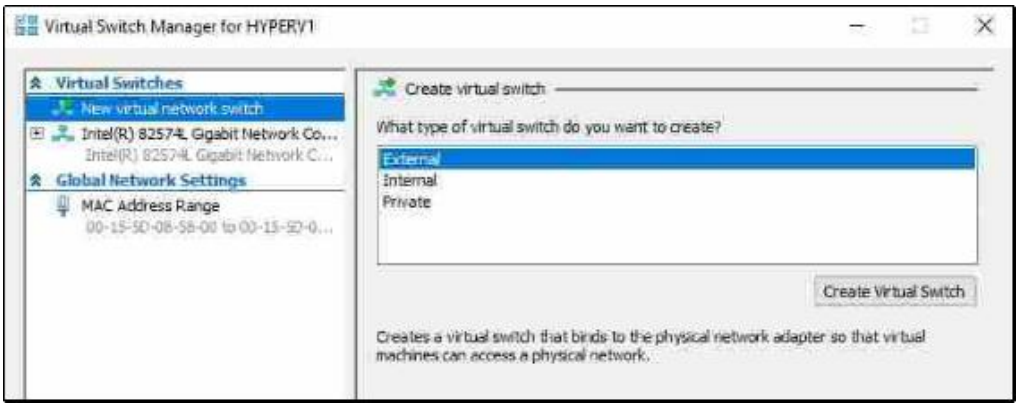
Utilizzo di interruttori virtuali

Al termine dell'installazione del ruolo Hyper-V, la tua prima inclinazione potrebbe essere quella di saltare subito e iniziare a creare VM, ma dovresti davvero dedicare un minuto per assicurarti che le capacità di rete del tuo server Hyper-V siano adeguate alle tue esigenze . Durante il processo di installazione del ruolo, abbiamo selezionato le NIC fisiche che devono essere passate in Hyper-V e quella schermata ci ha detto che avrebbe stabilito uno switch virtuale per ciascuna di queste NIC. Ma che aspetto ha all'interno della console? E quali opzioni abbiamo per stabilire una rete tra le nostre macchine virtuali?

Per rispondere a queste domande, dobbiamo aprire l'interfaccia di gestione per Hyper-V. Come con qualsiasi strumento di amministrazione di un ruolo Windows, controlla nel menu Strumenti di Server Manager e ora che il ruolo è stato installato, vedrai un nuovo elenco per Hyper-V Manager. Avvialo e ora stiamo esaminando la piattaforma principale da cui gestirai e manipolerai ogni aspetto del tuo ambiente Hyper-V:



Al momento abbiamo molto spazio vuoto in questa console, perché non abbiamo ancora nessuna VM in esecuzione. Sul lato destro di Hyper-V Manager, puoi vedere un collegamento che dice**Virtual Switch Manager.** Vai avanti e fai clic su quel link per essere portato nelle impostazioni per
i nostri switch virtuali e networking:

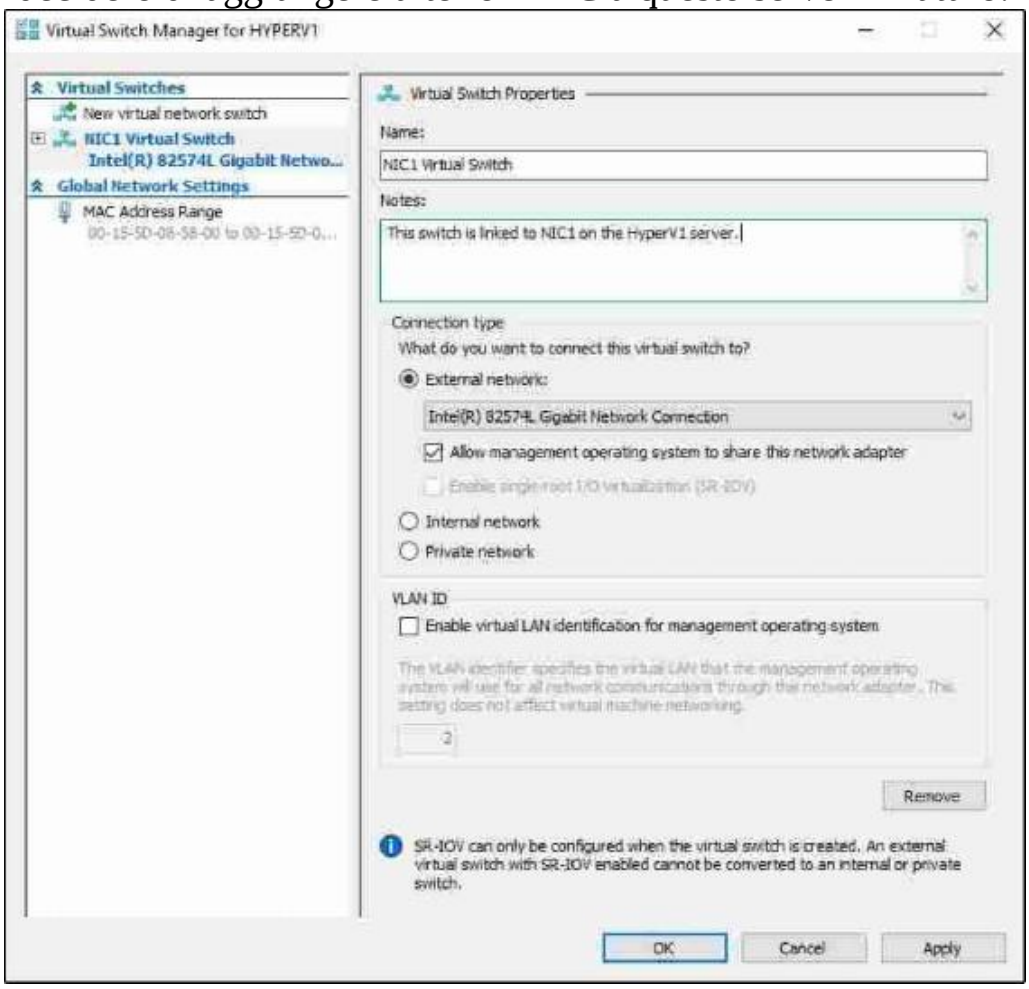


Verso sinistra, viene visualizzato un elenco degli attuali switch virtuali. Sul mio server, al momento è elencato un solo switch, che prende il nome dalla scheda di rete fisica a cui è connesso. Questo è lo switch virtuale che il processo di installazione del ruolo ha creato per noi quando abbiamo selezionato la NIC da includere in Hyper-V. Se hai selezionato più NIC durante l'installazione del ruolo, avrai più switch virtuali disponibili qui, ciascuno corrispondente a una singola NIC fisica. Ogni VM che crei avrà una o più NIC virtuali e presto vedrai che hai la possibilità di scegliere dove connettere ciascuna di quelle NIC virtuali. Se sono presenti cinque diverse reti fisiche che le tue VM potrebbero dover contattare, puoi utilizzare cinque NIC fisiche nel server Hyper-V, collegare ciascuna di esse a una rete diversa,

Come puoi vedere nello screenshot precedente, abbiamo un pulsante chiamato Crea interruttore virtuale, che si spiega da sé. Ovviamente, è qui che andiamo per creare nuovi interruttori, ma ci sono tre diversi tipi di interruttori che puoi creare. Prendiamo solo un minuto per discutere le differenze tra loro.

L'interruttore virtuale esterno

Lo switch virtuale esterno è il tipo più comune da utilizzare per tutte le VM che devono contattare una rete di produzione. Ogni switch virtuale esterno si associa a una scheda NIC fisica installata nel server Hyper-V. Se fai clic su un interruttore virtuale esterno, puoi vedere che hai alcune opzioni per configurare questo interruttore e che puoi persino cambiare un tipo di interruttore. Nello screenshot seguente, ho rinominato il mio switch virtuale esterno in modo che sia più facile identificarlo quando deciderò di aggiungere ulteriori NIC a questo server in futuro:



L'interruttore virtuale interno

Gli switch virtuali interni non sono associati a una scheda NIC fisica, quindi se crei uno switch virtuale interno e ci colleghi una VM, quella macchina virtuale non sarà in grado di contattare una rete fisica esterna al server Hyper-V stesso. È una sorta di intermediario tra gli altri due tipi di switch; l'utilizzo di uno switch virtuale interno è utile quando si desidera che il traffico della macchina virtuale rimanga all'interno dell'ambiente Hyper-V, ma fornisce comunque la connettività di rete tra le macchine virtuali e l'host Hyper-V stesso. In altre parole, le VM connesse a uno switch virtuale interno potranno parlare tra loro e parlare con il server Hyper-V, ma non oltre.

Lo switch virtuale privato

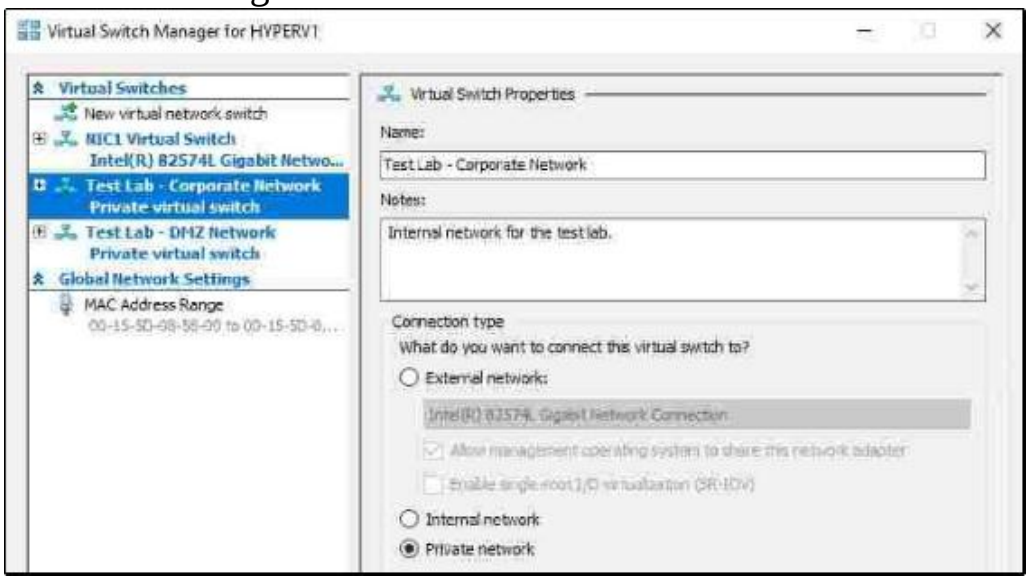
Lo switch virtuale privato è proprio quello che suggerisce il nome: privato. Le VM collegate allo stesso switch virtuale privato possono comunicare tra loro, ma non oltre. Anche il server host Hyper-V non dispone di connettività di rete a uno switch virtuale privato. I laboratori di test sono un ottimo esempio di un caso d'uso per switch virtuali privati, di cui parleremo immediatamente dopo questo testo, quando creeremo un nostro nuovo switch virtuale.

Creazione di un nuovo switch virtuale

Quello che segue è un esempio che uso spesso. Sto eseguendo un nuovo server Hyper-V, che è connesso fisicamente alla mia rete aziendale, quindi posso avviare nuove VM, collegarle al mio switch virtuale esterno e farle comunicare direttamente con la rete aziendale. Ciò mi consente di unirmi al dominio e di interagire con loro come farei con qualsiasi server sulla mia rete. Forse ho bisogno di creare alcune VM con cui voglio essere in grado di parlare tra loro, ma non voglio che siano in grado di comunicare con la mia rete di produzione. Un buon esempio di questo scenario nel mondo reale è quando si costruisce un laboratorio di test. In effetti, sto adottando questo approccio esatto per tutti i server che abbiamo utilizzato in questo libro. Il mio server Hyper-V fisico si trova sulla mia rete di produzione, ma l'intera rete Contoso e tutte le VM in esecuzione al suo interno si trovano sulla propria rete separata, che è completamente separato dalla mia rete reale. L'ho fatto creando un nuovo switch virtuale privato.

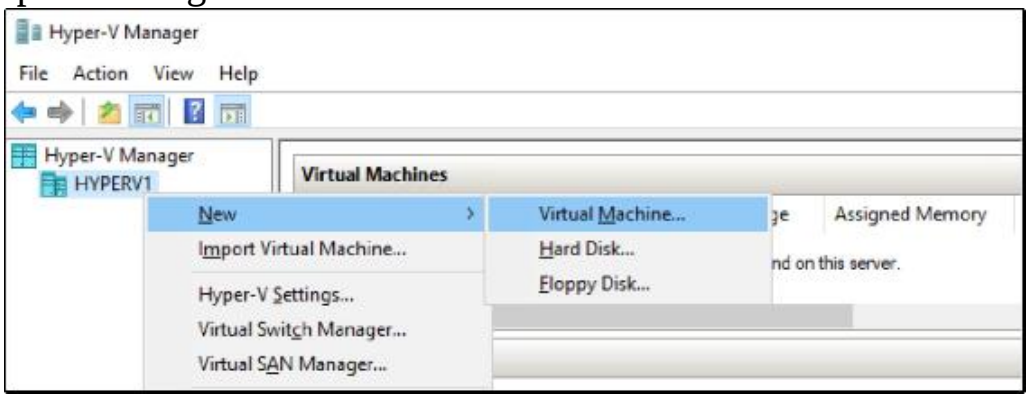
Ricordare dalla descrizione che quando si collegano le VM a questo tipo di switch, possono comunicare con altre VM collegate allo stesso switch virtuale, ma non possono comunicare oltre tale switch.

All'interno del Virtual Switch Manager, tutto quello che devo fare è scegliere il tipo di switch virtuale che voglio creare, privato in questo caso, e fare clic sul pulsante Crea switch virtuale. Posso quindi fornire un nome per il mio nuovo switch e sono immediatamente in grado di connettere le VM a questo switch. Nella schermata seguente puoi vedere che ho creato due nuovi switch virtuali privati: uno per collegare le schede di rete interne della VM del mio laboratorio di test e un altro switch che fungerà da rete DMZ del mio laboratorio di test:

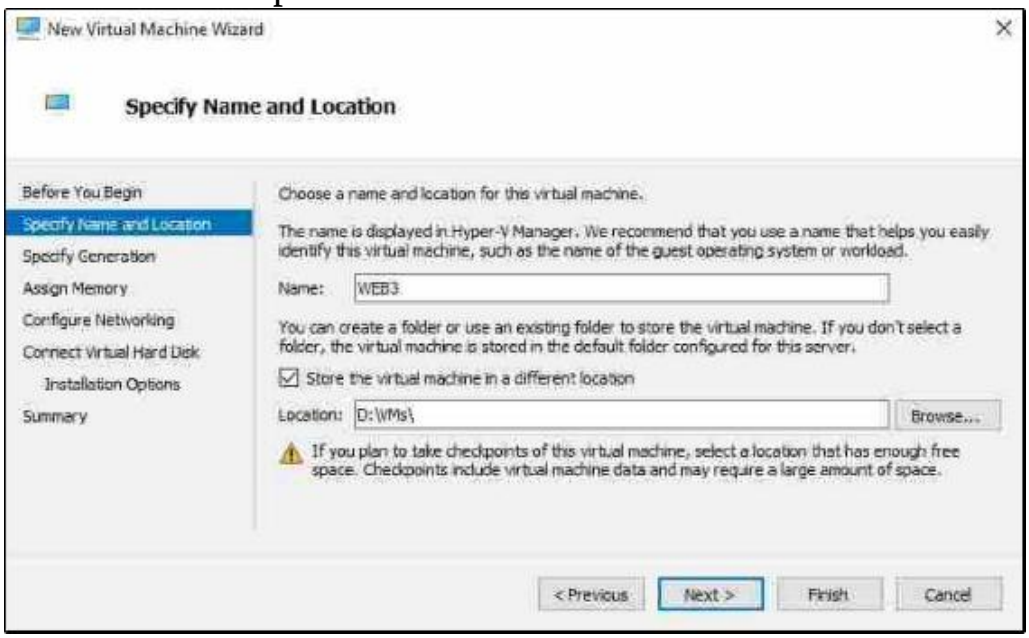


Implementazione di un nuovo server virtuale

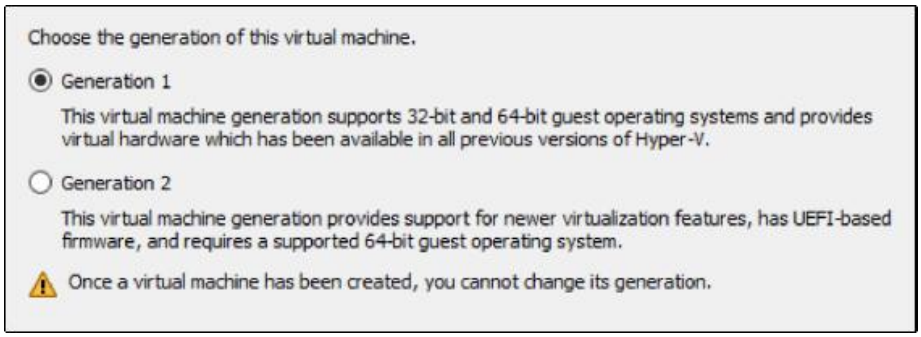
Ora siamo pronti per avviare il nostro primo server virtuale! Simile alla creazione di nuovi switch virtuali, il processo per la creazione di una nuova VM è abbastanza semplice, ma ci sono alcuni passaggi lungo il percorso che potrebbero richiedere qualche spiegazione se non l'hai mai fatto prima. Partiamo dalla stessa interfaccia di gestione da cui facciamo tutto nel mondo Hyper-V. Apri Hyper-V Manager e fai clic con il pulsante destro del mouse sul nome del tuo file
Server Hyper-V. Vai a Nuovo | Macchina virtuale ... per avviare la procedura guidata:



La prima schermata in cui dobbiamo prendere alcune decisioni è Specifica nome e posizione. Crea un nome per la tua nuova VM, è abbastanza facile. Ma poi hai anche la possibilità di archiviare la tua VM in una nuova posizione. Se si imposta una buona posizione predefinita per le macchine virtuali durante l'installazione del ruolo Hyper-V, è probabile che non sia necessario modificare questo campo. Ma nel mio caso, ho scelto le opzioni predefinite quando ho installato il ruolo, quindi avrei posizionato la mia VM da qualche parte in C: \ ProgramData, e l'aspetto non mi piaceva. Quindi ho selezionato questa casella e ho scelto una posizione che mi piace per la mia VM. Puoi vedere che sto usando un disco dedicato per archiviare le mie VM, che generalmente è una buona pratica. Una pratica ancora migliore in una rete più ampia sarebbe quella di utilizzare lo spazio su disco resiliente a cui si accede attraverso la rete,

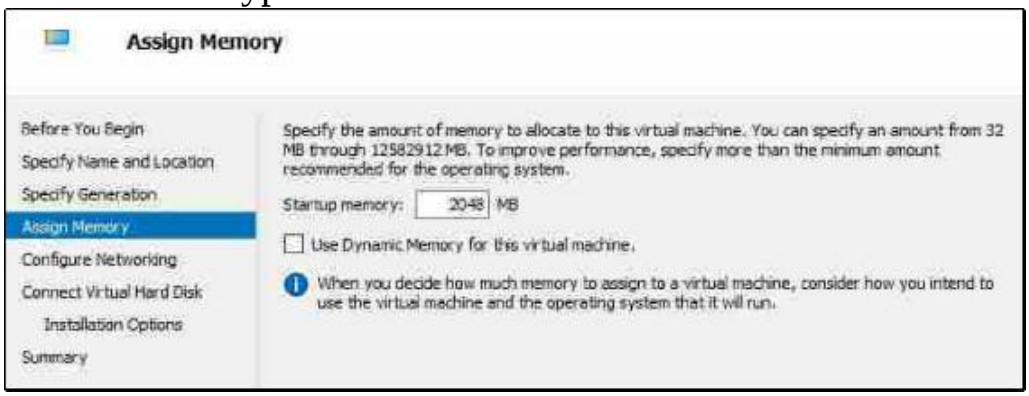


Successivamente, devi decidere se stai creando una VM di prima o seconda generazione. Non abbiamo bisogno di discuterne in dettaglio, perché le spiegazioni dei due sono chiaramente indicate nella pagina e nello screenshot seguente. Se la tua VM eseguirà un sistema operativo precedente, dovresti probabilmente utilizzare la prima generazione per garantire la compatibilità.
In alternativa, se stai pianificando di installare un sistema operativo recente su questa nuova VM, selezionare la seconda generazione è probabilmente nel tuo migliore interesse da una nuova prospettiva di funzionalità e sicurezza:

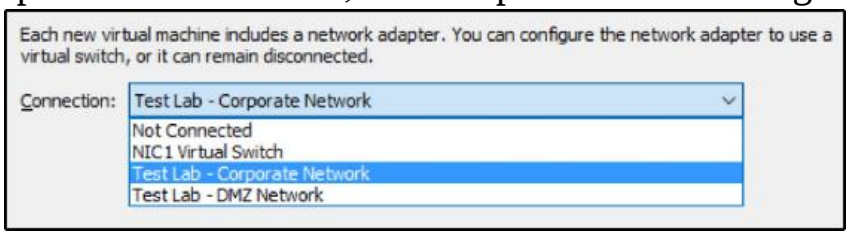


Ora, definisci quanta memoria vuoi assegnare a questa particolare VM. Tieni presente che questa è un'impostazione che puoi modificare in futuro su questo server, quindi non devi pianificare troppo duramente per questo. La quantità di RAM che dedichi a questa macchina virtuale dipenderà dalla quantità di RAM che hai a disposizione nel sistema host Hyper-V e da quanta memoria è richiesta per eseguire i ruoli e i servizi che intendi installare su questa VM. È possibile specificare qualsiasi quantità di memoria in questo campo. Ad esempio, se volessi circa 2 GB, potrei digitare circa 2.000 MB. Tuttavia, quello che trovo sul campo è che la maggior parte delle persone si attacca ancora alla quantità effettiva di MB, perché è quello che abbiamo sempre fatto con l'hardware. Quindi, invece di arrotondare a 2.000, imposterò la mia VM da 2 GB su 2 GB effettivi o 2.048 MB.

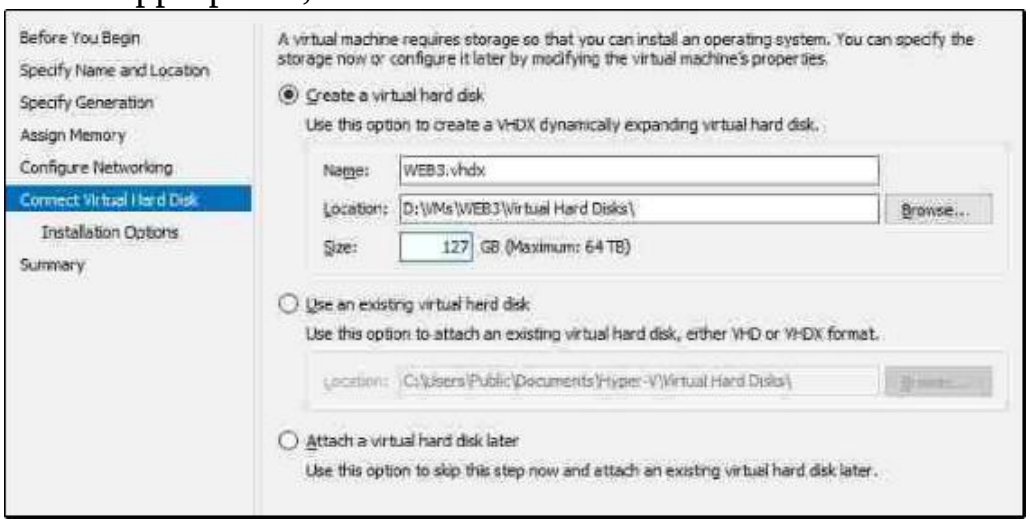
Lasciando deselezionata la casella per la memoria dinamica, Hyper-V dedicherà 2.048 MB effettivi della sua RAM fisicamente disponibile a questa specifica VM. Indipendentemente dal fatto che la VM utilizzi 2.048 MB o 256 MB in un dato momento, tutti i 2.048 MB saranno dedicati alla VM e saranno inutilizzabili dal resto del server Hyper-V. Se selezioni Usa memoria dinamica per questa macchina virtuale, la VM sottrae all'host Hyper-V solo ciò che sta effettivamente utilizzando. Se lo imposti a 2.048 MB, ma la VM è inattiva e consuma solo 256 MB, verrà tassato solo Hyper-V con un carico di 256 MB:



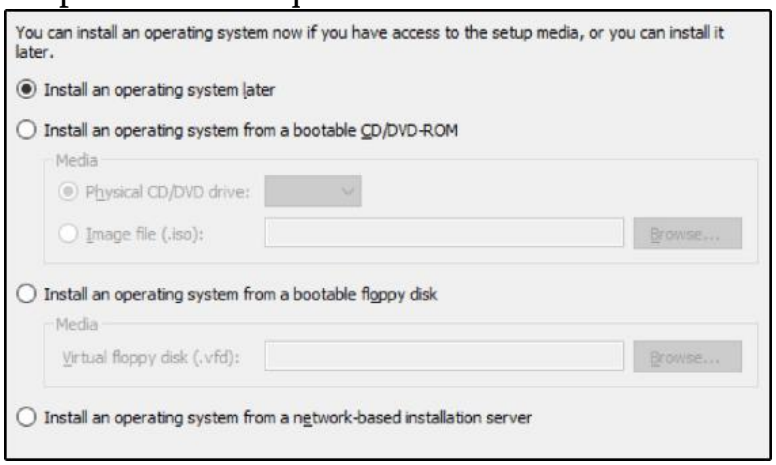
Configurare la rete è la schermata successiva che ci viene presentata, e qui stiamo semplicemente scegliendo a quale switch virtuale deve essere collegata la NIC della nostra VM. Abbiamo la possibilità di aggiungere ulteriori NIC a questa VM in un secondo momento, ma per ora otteniamo una singola NIC standard durante la creazione della nostra nuova VM e dobbiamo solo scegliere dove deve essere collegata. Per il momento, questo nuovo server web che sto costruendo sarà connesso alla rete aziendale interna del mio Test Lab, in modo che io possa costruire la mia web app e testarla, prima di introdurla in una vera rete di produzione. Se faccio scorrere un elenco di connessioni disponibili qui, vedrai che il mio switch virtuale esterno originale, così come i due nuovi switch virtuali privati che ho creato, sono disponibili tra cui scegliere:



Sono necessari anche alcuni dettagli in modo che questa nuova VM possa avere un disco rigido. Più comunemente, utilizzerai l'opzione in alto qui in modo che la nuova VM ottenga un disco rigido nuovo di zecca. Esistono anche opzioni per utilizzare un disco rigido virtuale esistente se si esegue l'avvio da un file esistente o per collegare un disco in un secondo momento se non si è ancora preparati a prendere questa decisione. Consentiremo alla procedura guidata di generare un nuovo disco rigido virtuale e la dimensione predefinita è 127 GB. Posso impostarlo su quello che voglio, ma è importante sapere che non consuma tutti i 127 GB di spazio. La dimensione del disco sarà grande quanto quella effettivamente utilizzata sul disco, quindi verrà utilizzata solo una frazione di quei 127 GB. Lo menziono per sottolineare che il numero che specifichi qui è più di una dimensione massima, quindi assicurati di pianificare i tuoi dischi in modo appropriato,

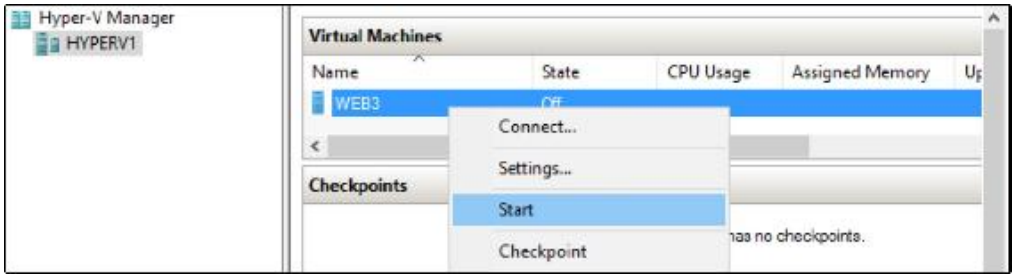


La nostra ultima schermata di opzioni nella procedura guidata ci consente di definire le specifiche del sistema operativo su cui verrà eseguita la nostra nuova VM. O meglio, da dove verrà installato quel sistema operativo. Lasceremo intenzionalmente questo set su Installa un sistema operativo in seguito, perché questa è l'opzione predefinita e ci darà la possibilità di vedere cosa succede quando non specifichi alcuna impostazione in questa schermata:

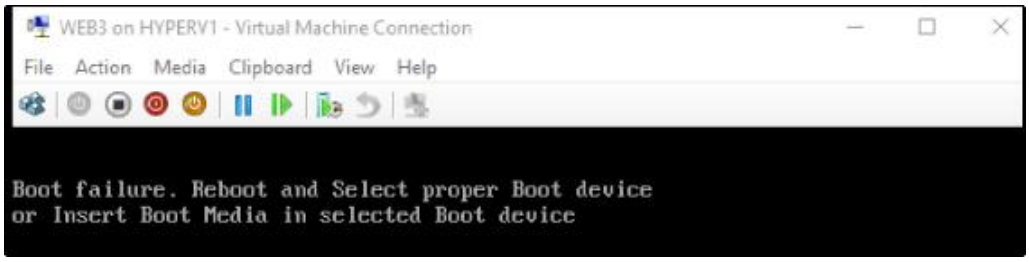


Avvio e connessione alla VM

Ora abbiamo creato una VM, che puoi vedere all'interno della console di Hyper-V Manager. L'avvio della VM è semplice come fare clic con il pulsante destro del mouse su di essa e quindi selezionare Avvia. Dopo aver selezionato l'opzione per avviare la VM, fare nuovamente clic con il pulsante destro del mouse e fare clic su**Collegare.** Questo aprirà un file
finestra della console dalla quale puoi guardare il processo di avvio del tuo nuovo server:



Ora che la nostra nuova VM è stata avviata, cosa possiamo aspettarci di vedere all'interno della finestra della console? Un errore di avvio fallito, ovviamente:

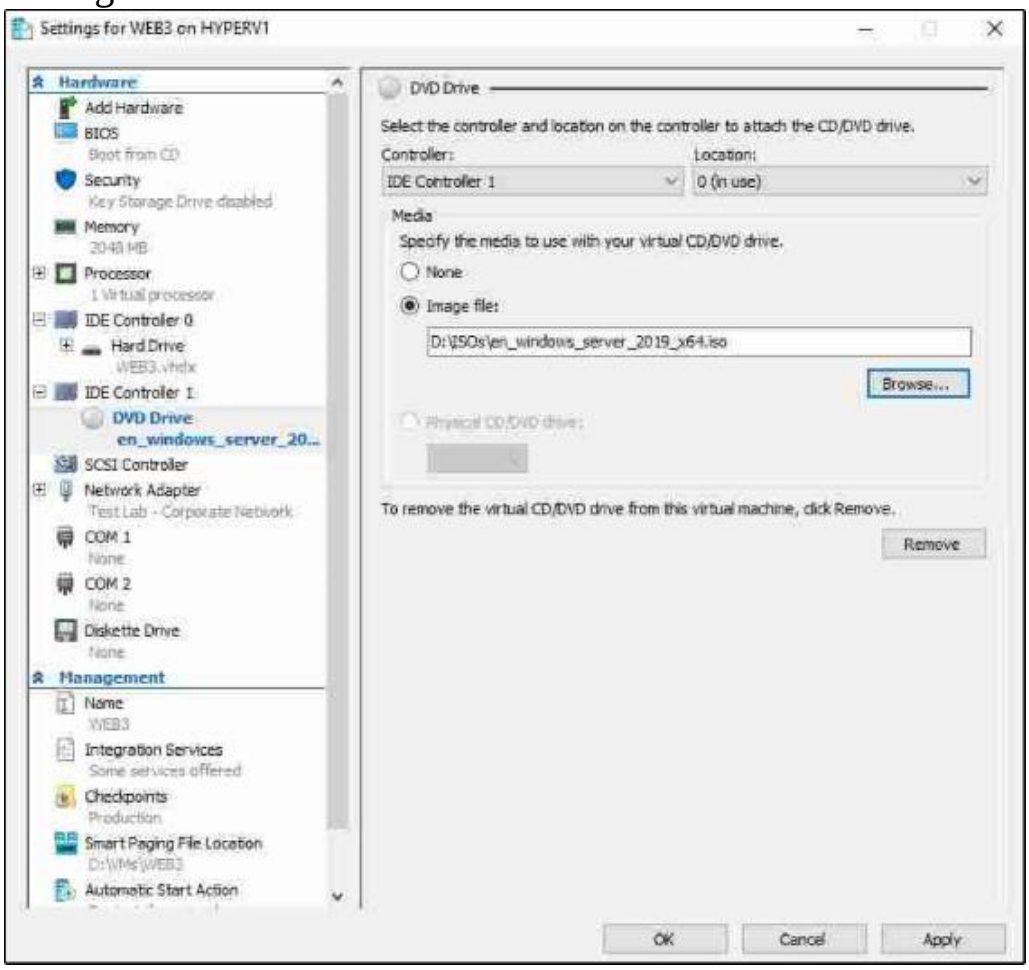


Installazione del sistema operativo

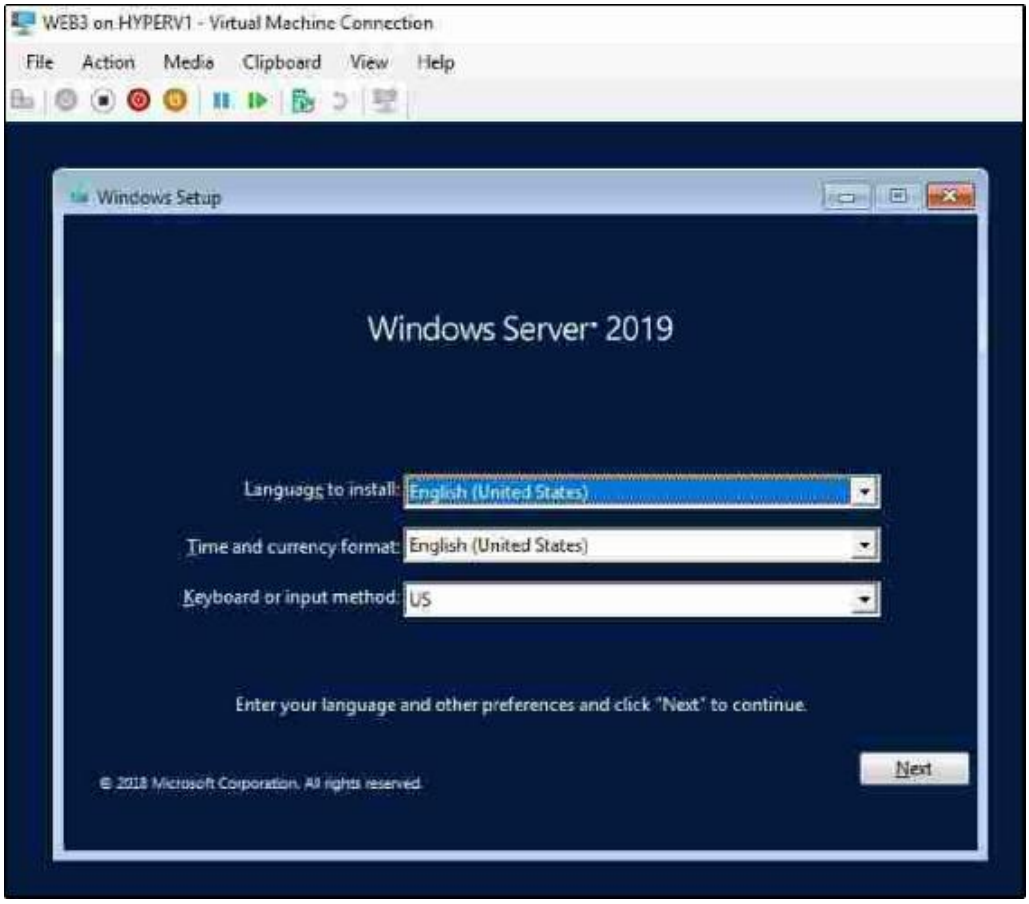
Riceviamo un messaggio di errore di avvio perché non abbiamo specificato alcun supporto del sistema operativo durante la nostra procedura guidata, quindi Hyper-V ha creato la nostra VM e il nostro nuovo disco rigido, ma proprio come quando costruisci un nuovo server con un nuovo hardware, tu è necessario che il software sia installato su quel disco rigido in modo che possa fare qualcosa. Fortunatamente, installare un sistema operativo su una VM è ancora più semplice che installarlo su un server fisico. Tornando alla console di Hyper-V Manager, fai clic con il pulsante destro del mouse sul nome della tua nuova VM e vai su Impostazioni ...

All'interno delle impostazioni, vedrai che questa VM ha un'unità DVD automaticamente elencata in IDE Controller 1. Se fai clic su DVD Drive, puoi facilmente dirle di montare qualsiasi ISO su quell'unità. Copia il file ISO del programma di installazione del sistema operativo che desideri eseguire sul disco rigido del tuo server Hyper-V.

In genere inserisco tutte le mie ISO all'interno di una cartella dedicata chiamata ISO, proprio accanto alla mia cartella VM, quindi sfoglia ... da questa schermata. La connessione di una ISO alla tua VM è come se collegassi un DVD di installazione fisica a un server fisico:



Dopo aver montato il supporto, riavvia la VM e vedrai che il programma di installazione del nostro sistema operativo si avvia automaticamente:

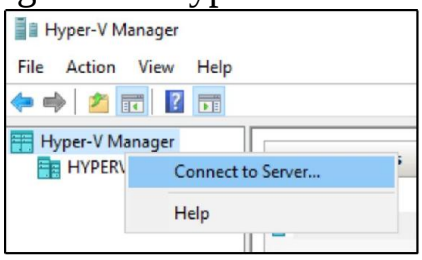


Gestire un server virtuale

Abbiamo utilizzato Hyper-V Manager per gestire i nostri switch virtuali e per creare una macchina virtuale. Questo strumento è onnipotente quando si tratta di manipolare le VM e mi ritrovo ad accedervi frequentemente nel mio lavoro quotidiano. Diamo un'occhiata ad alcune delle altre cose che puoi fare all'interno di Hyper-V Manager, oltre a discutere altri metodi che possono essere utilizzati per lavorare con le nuove macchine virtuali che vengono create sul tuo server Hyper-V.

Hyper-V Manager

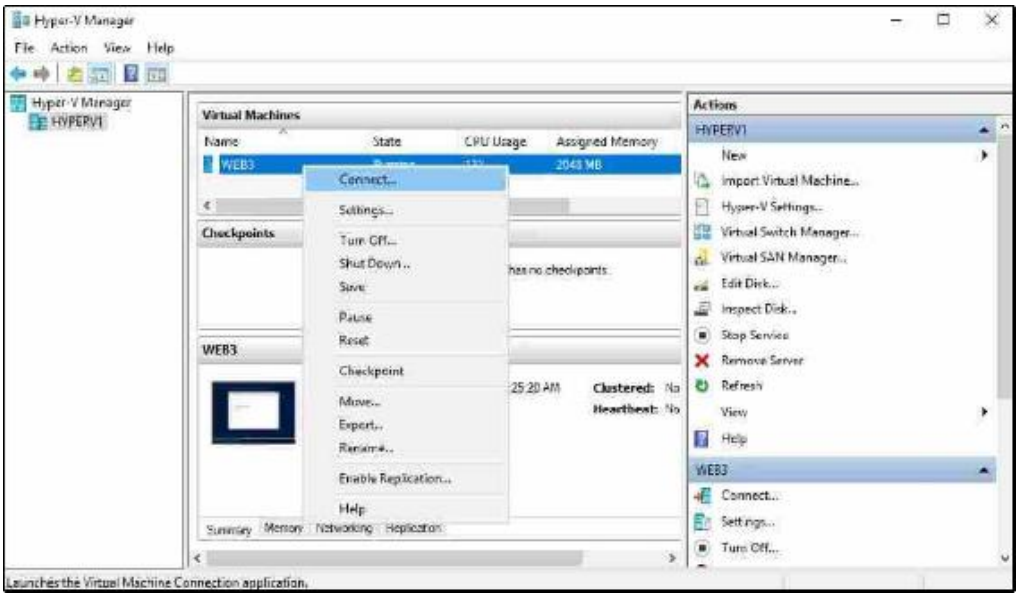
Come saprai, Hyper-V Manager è lo strumento principale per la gestione di un server Hyper-V. È una bella console che ti offre uno stato rapido delle tue macchine virtuali e ti consente di gestire quelle VM in una varietà di modi. Qualcosa che non abbiamo trattato, perché ho un solo server Hyper-V in esecuzione, è che puoi gestire più server Hyper-V da una singola console Hyper-V Manager. Proprio come qualsiasi console in stile MMC nel mondo Microsoft, puoi fare clic con il pulsante destro del mouse sulle parole Hyper-V Manager vicino all'angolo in alto a sinistra dello schermo e selezionare un'opzione che dice Connetti**al server.** Usando questa funzione, puoi estrarre le informazioni da altri server Hyper-V nella stessa console di gestione Hyper-V:



Inoltre, ciò consente di eseguire il software Hyper-V Manager su un computer client. È possibile installare il ruolo Hyper-V su una macchina Windows 10, che installerà anche questa console, quindi utilizzare la copia locale di Hyper-V Manager in esecuzione sul desktop di Windows

10 per gestire i server Hyper-V, senza la necessità per accedere direttamente a quei server.

Alcune delle azioni più utili all'interno di Hyper-V Manager sono elencate lungo il lato destro della console nel riquadro Azioni, funzionalità come Virtual Switch Manager e la possibilità di creare una nuova VM. Una volta che le VM sono attive e in esecuzione, troverai molte funzioni utili elencate nel menu contestuale che appare quando fai clic con il tasto destro su una VM, come puoi vedere nello screenshot seguente:

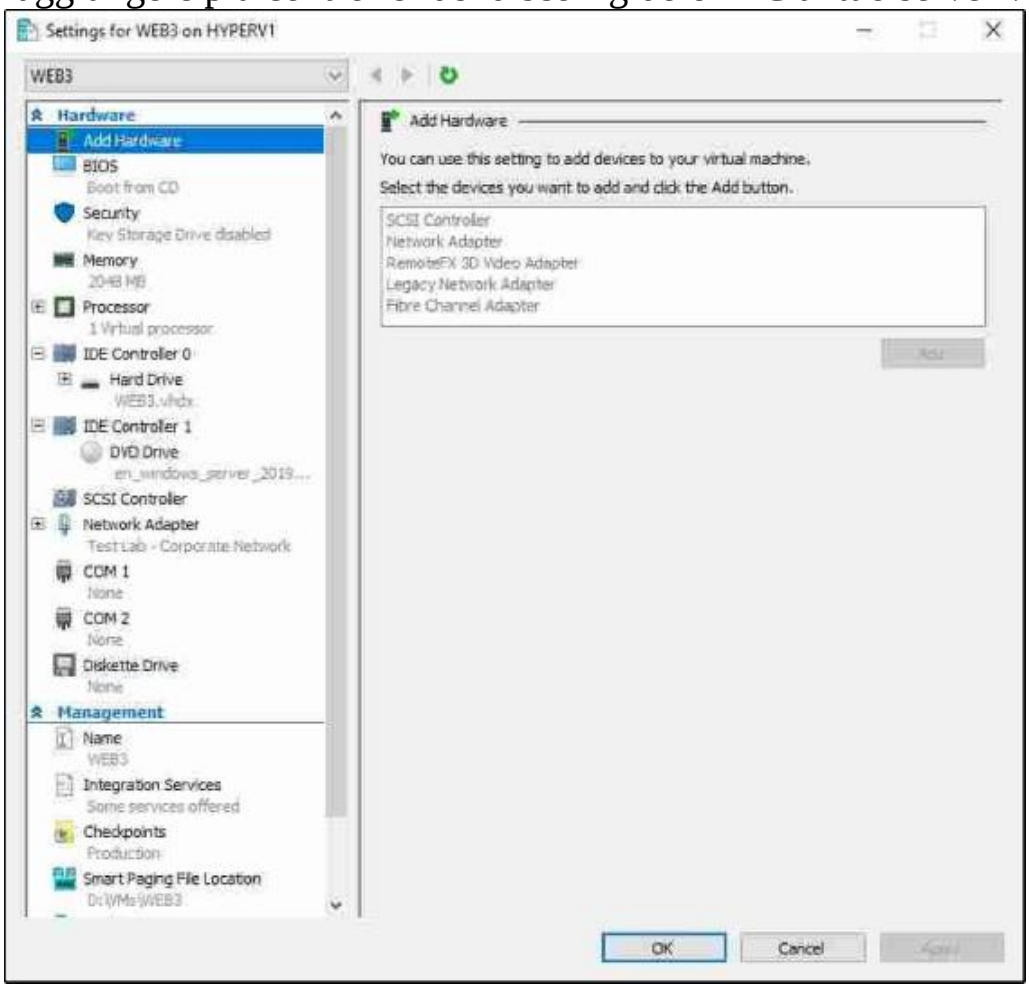


Alcuni di questi sono autoesplicativi e con alcuni vale la pena giocarci. Abbiamo già utilizzato Connect ... per connetterci alla console della nostra VM. Impostazioni ... apre un sacco di possibilità e daremo un'occhiata più da vicino al menu Impostazioni subito dopo questo testo. Uno dei motivi più comuni per cui apro questo menu di scelta rapida è per le funzioni di alimentazione sulle mie VM. Puoi vedere che hai la possibilità di spegnere ... o spegnere ... la tua VM. Spegnerlo è come premere il pulsante di accensione su un server: interrompe immediatamente l'alimentazione a quel server e causerà un po 'di dolore a Windows quando lo fa. La funzione di spegnimento, d'altra parte, avvia uno spegnimento pulito, almeno quando si utilizzano sistemi operativi Microsoft sulle VM. Chiudere un server non è un grosso problema, ma il vero potere qui deriva dal fatto che è possibile arrestare più VM contemporaneamente. Ad esempio, se eseguissi una dozzina di VM diverse tutte per i miei laboratori di test e decidessi che il mio laboratorio sta occupando troppe risorse e sta causando problemi sul mio server Hyper-V, potrei selezionare tutte le mie VM contemporaneamente , fai clic con il pulsante destro del mouse su di essi, quindi fai clic su Spegni ... solo una volta e avvierà immediatamente il processo di spegnimento su tutte le VM che avevo selezionato. Una volta che una VM è stata arrestata o spenta, fare clic con il tasto destro su quella VM ti darà una funzione di avvio; puoi anche selezionare molti server e avviarli tutti in

una volta utilizzando questo menu di scelta rapida. e ho deciso che il mio laboratorio stava occupando troppe risorse e stava causando problemi sul mio server Hyper-V, potevo selezionare tutte le mie VM contemporaneamente, fare clic con il tasto destro su di esse, quindi fare clic su Spegni ... solo una volta e avrebbe immediatamente avviato il processo di arresto su tutte le VM che avevo selezionato. Una volta che una VM è stata arrestata o spenta, fare clic con il tasto destro su quella VM ti darà una funzione di avvio; puoi anche selezionare molti server e avviarli tutti in una volta utilizzando questo menu di scelta rapida. e ho deciso che il mio laboratorio occupava troppe risorse e causava problemi sul mio server Hyper-V, potevo selezionare tutte le mie VM contemporaneamente, fare clic con il tasto destro su di esse, quindi fare clic su Spegni ... solo una volta e avrebbe immediatamente avviato il processo di arresto su tutte le VM che avevo selezionato. Una volta che una VM è stata arrestata o spenta, fare clic con il tasto destro su quella VM ti darà una funzione di avvio; puoi anche selezionare molti server e avviarli tutti in una volta utilizzando questo menu di scelta rapida.

Il menu Impostazioni

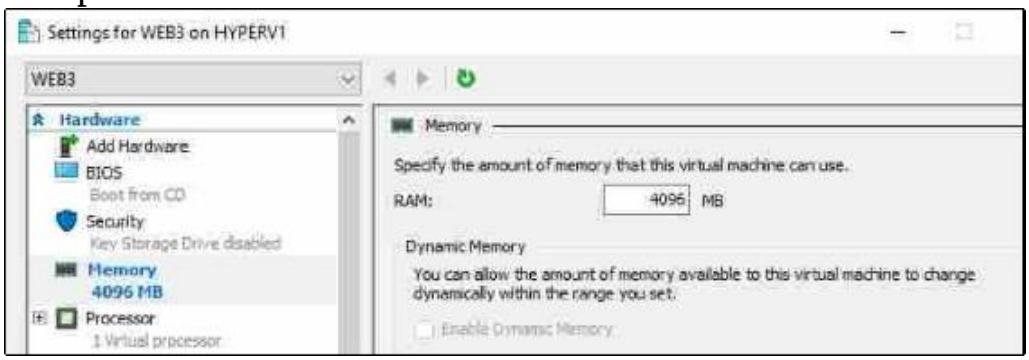
Apportare modifiche approfondite a una qualsiasi delle VM in genere significa fare clic con il pulsante destro del mouse su quella VM e quindi passare a Impostazioni ... per quella particolare VM. All'interno delle impostazioni, puoi regolare qualsiasi aspetto dell'hardware della tua VM, che è il motivo più comune per visitare questa schermata. Immediatamente dopo l'apertura delle impostazioni, hai la possibilità di aggiungere hardware alla tua VM. Questo è il posto dove andresti per aggiungere più controller del disco rigido o NIC al tuo server virtuale:



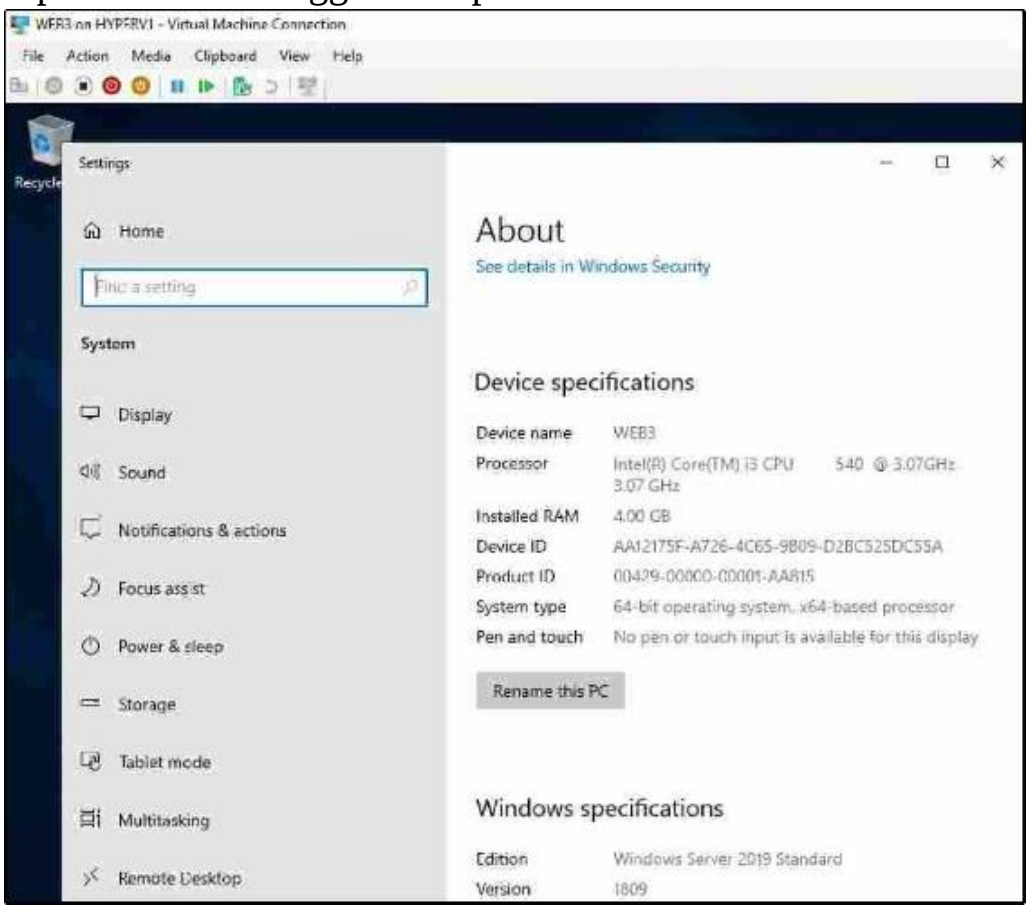
Non so se puoi dirlo dallo screenshot precedente, ma il pulsante Aggiungi è attualmente disattivato. Questo è importante. Molte funzioni all'interno delle impostazioni possono essere manipolate al volo, mentre la VM è in esecuzione. Alcune funzioni non possono essere eseguite a meno che la VM non sia spenta. L'aggiunta di hardware è una di quelle funzioni. Se desideri aggiungere un nuovo disco rigido o NIC alla tua VM, dovrai spegnere quel server prima di poterlo fare.

Successivamente, dovremmo parlare della schermata Memoria. Questo è abbastanza semplice, giusto? Basta inserire la quantità di RAM che si desidera che questa VM abbia a disposizione. Il motivo per cui voglio segnalarlo è che è stato apportato un notevole miglioramento a questa funzionalità. A partire da Windows Server 2016 Hyper-V, ora puoi regolare la quantità di RAM di cui dispone una VM mentre è in esecuzione! Nelle versioni precedenti di Hyper-V, era necessario arrestare le VM per modificare la loro allocazione di memoria, ma anche se il mio server WEB3 è attualmente in esecuzione e serve gli utenti, posso entrare qui e aumentare la RAM a piacimento.

Diciamo che i miei 2 GB non tengono il passo con il carico delle attività e voglio aumentarlo a 4 GB. Lascio il server in esecuzione, apro le impostazioni di Hyper-V Manager per la VM e aggiusto l'impostazione relativa a 4.096 MB:



La quantità di memoria si adatta immediatamente e se apro le proprietà di sistema all'interno del server WEB3, posso vedere che il sistema operativo è stato aggiornato per riflettere i 4 GB di RAM ora installati:

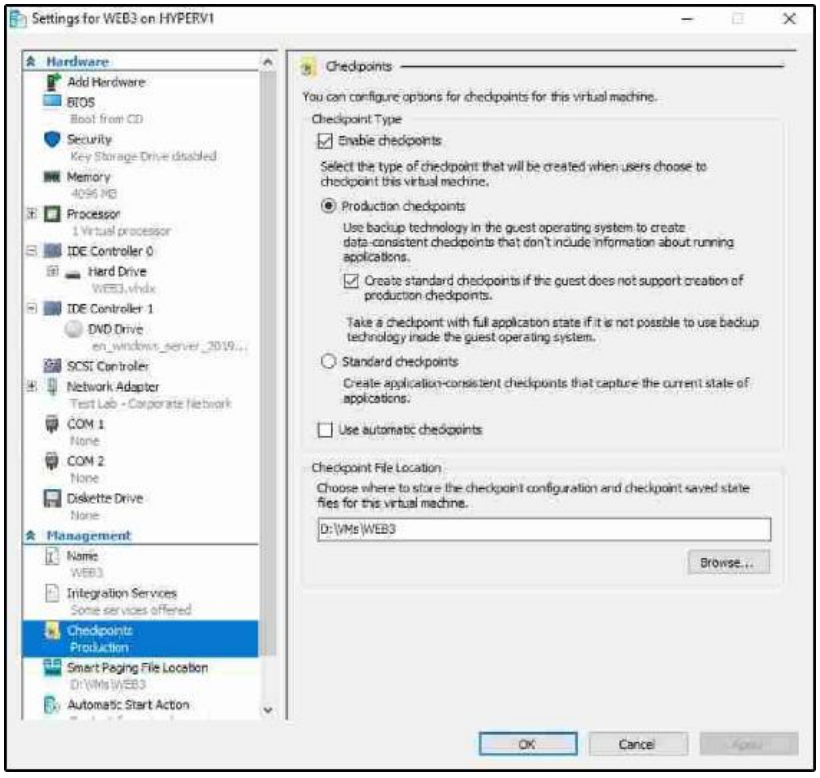


Le altre schermate di impostazioni utili sono le sezioni Processore e Adattatore di rete. Hai la possibilità di definire il numero di processori virtuali attualmente assegnati alla VM e i pesi delle prestazioni associati a questi processori. Nella schermata dell'adattatore di rete, puoi modificare lo switch virtuale a cui sono collegate le tue schede NIC virtuali. Mi ritrovo ad accedere spesso a questa sezione mentre sposto i server da una posizione all'altra.

Checkpoint

L'ultima parte del menu Impostazioni di cui voglio parlare si chiama checkpoint. In precedenza erano chiamate istantanee, il che penso abbia un po 'più senso per la maggior parte di noi.
I checkpoint sono una funzione che puoi richiamare da Hyper-V Manager facendo clic con il pulsante destro del mouse su una o più VM. In sostanza, crea un'istantanea in tempo per la VM. Un altro modo per esaminare i checkpoint è che stanno creando punti di rollback per i tuoi server. Se si crea un checkpoint martedì e mercoledì qualcuno apporta una modifica alla configurazione su quel server che causa problemi, è possibile ripristinare il checkpoint da martedì e riportare la VM allo stato di quel giorno.

Ci sono un paio di modi diversi in cui i checkpoint possono essere eseguiti e il menu Impostazioni è dove definiamo quei particolari. È sufficiente fare clic con il pulsante destro del mouse su qualsiasi VM, visitare la schermata Impostazioni, quindi fare clic sull'attività di gestione denominata Checkpoint. Puoi vedere le opzioni nella seguente schermata:

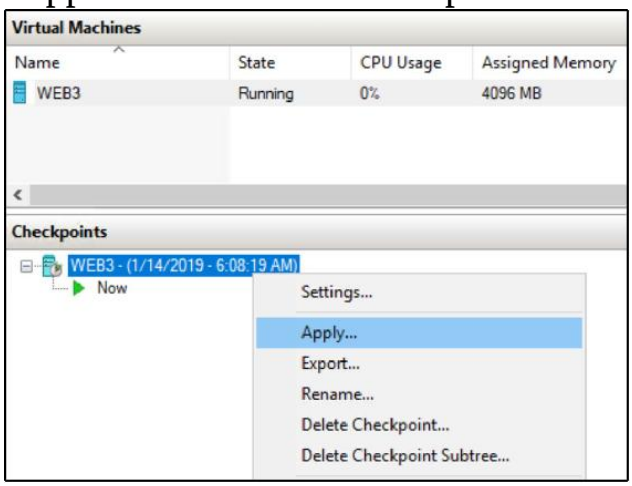


Queste impostazioni sono individuali per ogni VM in esecuzione; ad esempio, potresti trattare i checkpoint per WEB1 in modo diverso da WEB2. Il modo predefinito per gestire queste istantanee nel tempo è chiamato checkpoint di produzione. Questo è generalmente il metodo preferito per creare queste immagini rapide dei tuoi server, poiché è il metodo più pulito. Quando si sceglie di generare un checkpoint di produzione, Hyper-V richiama le funzioni di backup di Windows all'interno del sistema operativo della VM, al fine di creare un backup di quel server. Sarebbe simile all'accesso a quella VM e all'avvio manuale di un'attività di backup del sistema operativo. Tieni presente che, quando lo fai, e quindi quando Hyper-V lo fa per te, non è un backup identico blocco per blocco della VM mentre è in esecuzione in questo momento, ma piuttosto un file di backup che può essere ripristinato in futuro per riportare i file del sistema operativo a questo punto nel tempo. In altre parole, un checkpoint di produzione riporta Windows allo stato precedente, ma tutte le applicazioni e i dati che cambiano costantemente sul server non vengono acquisiti.

In alternativa, l'opzione Checkpoint standard fa proprio questo. Ciò richiede più di un'acquisizione rapida e sporca della VM, un po 'come fare clic con il pulsante destro del mouse sul file del disco rigido VHDX e scegliere di copiarlo e quindi incollarlo da qualche altra parte. Il ripristino dei checkpoint standard può essere un processo più complicato, perché se il tuo checkpoint è stato creato mentre un'applicazione sul server si trovava nel mezzo di una funzione importante, il ripristino lo riporterebbe direttamente all'applicazione che si trova nel mezzo della stessa importante funzione. Per qualcosa come la scrittura di un database, ciò potrebbe diventare complicato.

Dopo aver preso la decisione su quale tipo di checkpoint è il migliore per la tua VM, invocare i checkpoint è molto semplice. Torna alla schermata principale in Hyper-V Manager, fai semplicemente clic con il pulsante destro del mouse sulla tua VM e seleziona Checkpoint. Dopo aver eseguito questa attività, vedrai il pannello centrale di Hyper-V Manager ricevere alcune nuove informazioni in una sezione che potresti non aver nemmeno notato prima: Checkpoint.

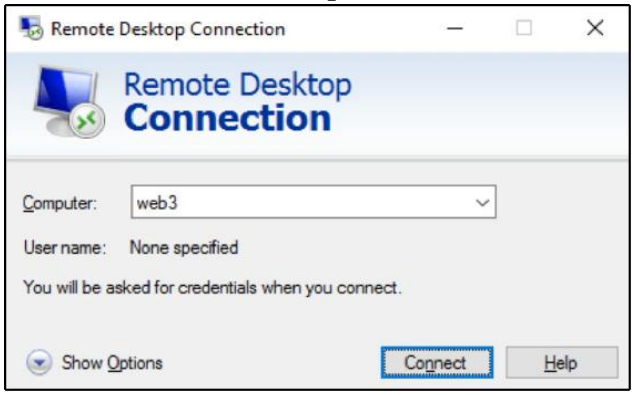
Il nuovo checkpoint che abbiamo appena creato è ora seduto qui, in attesa di essere ripristinato in caso di necessità. In futuro, facendo clic con il pulsante destro del mouse su questo checkpoint e scegliendo Applica ... verrà avviato il processo di ripristino:



Console Hyper-V, protocollo RDP (Remote Desktop Protocol) o PowerShell

Sebbene le modifiche hardware alle VM debbano essere effettuate tramite Hyper-V Manager, la tua interazione quotidiana con queste VM in esecuzione come server nel tuo ambiente non significa necessariamente che devi accedere al tuo Hyper-V Server. Se ti trovi comunque all'interno di Hyper-V Manager, puoi utilizzare in modo rapido e semplice la funzione Connect per interagire con la console dei tuoi server, tramite lo strumento Hyper-V Console. L'accesso ai server in questo modo è vantaggioso se è necessario vedere qualcosa nel BIOS o in altro modo al di fuori del sistema operativo Windows in esecuzione su quella VM, ma non è spesso necessario questo livello di accesso alla console.

Quando hai server Windows in esecuzione come VM, è molto più comune interagire con questi server nello stesso modo in cui interagiresti con i server fisici sulla tua rete. Mentre accedo al mio server WEB3 tramite la console Hyper-V in questo capitolo, ora che ho Windows Server 2019 installato su WEB3 e ho abilitato le funzionalità RDP su di esso, non c'è motivo per cui non potrei semplicemente aprirlo MSTSC e accedi a WEB3 in questo modo, direttamente dal mio desktop:



Lo stesso vale per PowerShell o qualsiasi altro modo tradizionale di accedere in remoto ai servizi su qualsiasi altro server. Poiché questa VM è completamente online e ha il sistema operativo del server installato, posso utilizzare PowerShell remoting per manipolare anche il mio server WEB3, da un altro server o dal mio computer desktop. Una volta terminata la creazione dell'hardware e l'installazione del sistema operativo su una VM, è raro che sia effettivamente necessario utilizzare la console Hyper-V per interagire con quel server. I motivi principali per aprire Hyper-V Manager per raggiungere una macchina virtuale sono apportare modifiche a livello di hardware su quel server, ad esempio l'aggiunta di un disco rigido, la regolazione della RAM o lo spostamento di una connessione di rete da uno switch a un altro.

Windows Admin Center (WAC)

Abbiamo visto WAC sparsi in questo libro, e per una buona ragione. WAC è il nuovissimo super-strumento che Microsoft vuole che gli amministratori di server inizino a utilizzare per interagire e gestire quasi tutti i loro server. I server VM ospitati in Hyper-V non fanno eccezione; è

possibile utilizzare il set di strumenti WAC per amministrare i server in esecuzione sugli host Hyper-V e utilizzare WAC per gestire i server host stessi.

VM schermate

Se il tuo lavoro quotidiano non include il lavoro con Hyper-V, è possibile che tu non abbia mai sentito parlare di VM schermate. Il nome spiega bene questa tecnologia a un livello di base. Se una VM è una macchina virtuale, allora una VM schermata deve essere una macchina virtuale schermata o protetta in qualche modo, giusto?

Una VM schermata è essenzialmente una VM crittografata. Piuttosto, il file del disco rigido stesso (il VHDX) viene crittografato, utilizzando BitLocker. Sembra semplice, ma ci sono alcuni requisiti decenti per farlo accadere. Affinché la crittografia BitLocker funzioni correttamente, la VM viene iniettata con un chip TPM (Trusted Platform Module) virtuale. I TPM stanno rapidamente diventando comuni a livello hardware, ma in realtà il loro utilizzo è ancora una misteriosa scatola nera per la maggior parte degli amministratori. Le VM schermate possono anche essere bloccate in modo che possano essere eseguite solo su server host integri e approvati, il che è un vantaggio straordinario per chi è attento alla sicurezza. Questa capacità è fornita da un paio di diverse opzioni di attestazione, di cui parleremo a breve.

Per spiegare i vantaggi offerti dalle VM schermate, esamineremo un esempio di ciò che accade quando le VM non sono schermate. Tieni presente che l'idea di VM schermate è un po 'più importante quando pensi che nel contesto dei server ospitati nel cloud in cui non hai accesso al back-end o ospitati da qualche altra divisione all'interno della tua azienda, come all'interno di un cloud privato. A meno che tu non abbia già impiegato del tempo per implementare tutte le VM schermate nel tuo ambiente, quello che sto per mostrarti è attualmente possibile su qualsiasi delle tue VM esistenti.

Sai già che sto eseguendo un server host Hyper-V e su quell'host ho una macchina virtuale chiamata WEB3. Ora, facciamo finta che io sia un provider di cloud hosting e che WEB3 sia un server web che appartiene a uno dei miei inquilini. Ho fornito al mio tenant uno switch virtuale privato per la rete, in modo che possa gestire la rete di quel server e non ho

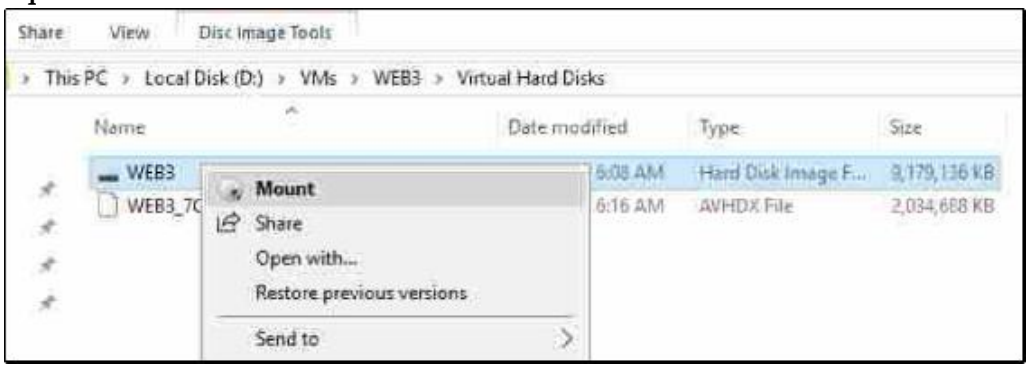
accesso a quella VM a livello di rete. Inoltre, è un dato di fatto che questo server WEB3 è unito al dominio e alla rete del mio tenant e io come host cloud non ho assolutamente accesso alle credenziali di dominio o qualsiasi altro mezzo che posso utilizzare per accedere effettivamente a quel server.

Finora suona abbastanza bene, giusto? Tu, come tenant, certamente non vorresti che il tuo provider cloud fosse in grado di curiosare all'interno delle tue macchine virtuali ospitate in quel cloud. Inoltre, non vorresti che altri tenant che potrebbero avere VM in esecuzione sullo stesso host cloud siano in grado di vedere i tuoi server in alcun modo. Questa stessa mentalità vale anche nei cloud privati. Se si ospita un cloud privato e si consente a varie società o divisioni di un'azienda di avere VM segregate in esecuzione nello stesso fabric, è opportuno assicurarsi che tali divisioni abbiano livelli di sicurezza reali tra le VM e tra le VM e l'host.

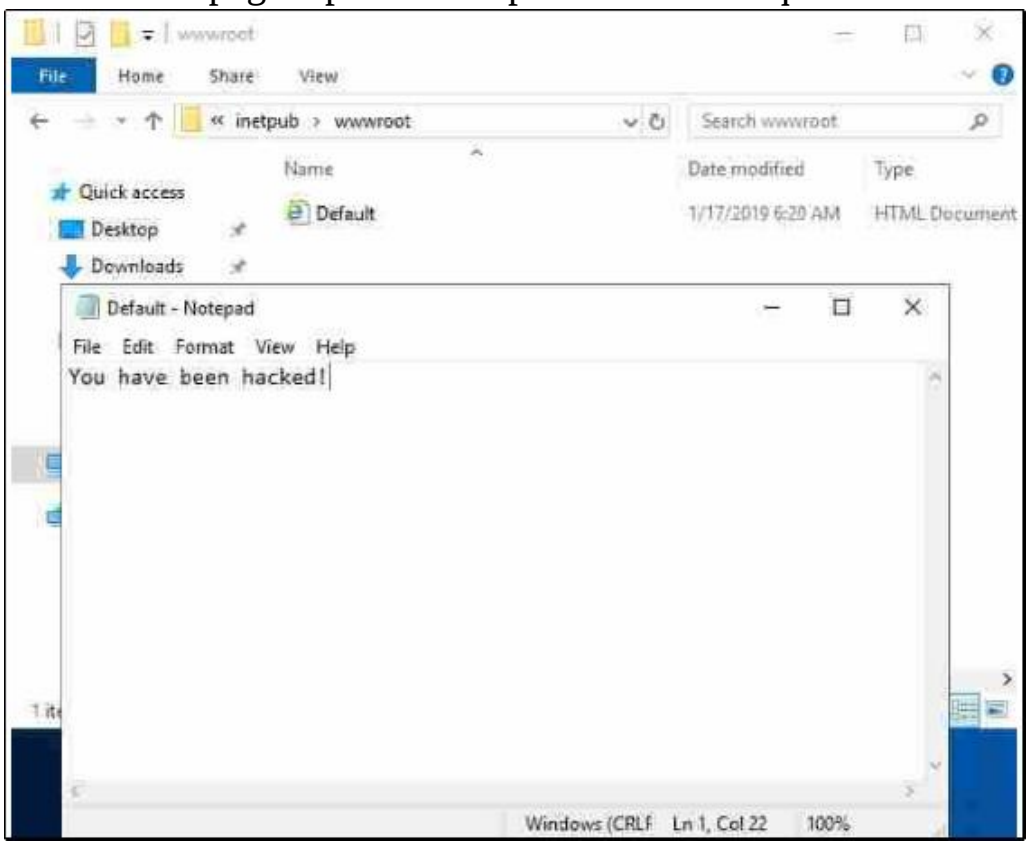
Ora, divertiamoci un po 'e trasformiamoci in un cattivo. Sono un dipendente di cloud host canaglia e decido che farò dei danni prima di uscire dalla porta. Sarebbe facile per me uccidere completamente quel server WEB3, dato che ho accesso alla console di amministrazione dell'host. Tuttavia, ciò probabilmente genererebbe una bandiera da qualche parte e l'inquilino dovrebbe semplicemente avviare un nuovo server Web o ripristinarlo da un backup. Quindi, anche meglio che rompere la VM, la lascerò in esecuzione e poi cambierò il contenuto del sito stesso. Diamo ai clienti di questa azienda qualcosa di cui parlare!

Per manipolare il sito Web del mio inquilino in esecuzione su WEB3, non ho bisogno di alcun accesso reale alla VM stessa, perché ho accesso diretto al file del disco rigido virtuale. Tutto quello che devo fare è attingere a quel file VHD, modificare il sito Web e posso fare in modo che il sito Web visualizzi tutte le informazioni che voglio.

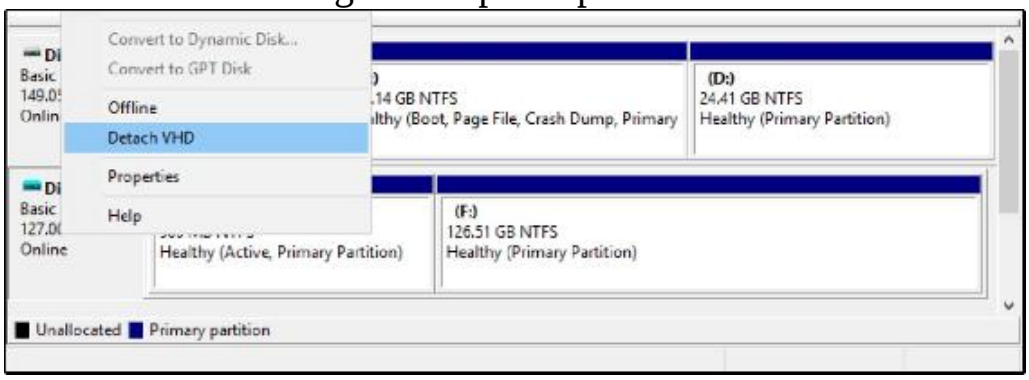
Innanzitutto, accedo al server Hyper-V (ricorda, questo è di mia proprietà poiché sono l'host) e navigo fino alla posizione del file VHD che WEB3 sta utilizzando. Questo è tutto sul back-end, quindi non ho bisogno di credenziali di tenant per arrivare qui. Inoltre, non viene registrato nulla con queste azioni e l'inquilino non avrà modo di sapere che lo sto facendo. Faccio semplicemente clic con il pulsante destro del mouse su quel VHD e seleziono Mount:



Ora che il VHD è stato montato direttamente sul sistema operativo del server host, posso sfogliare il disco rigido di quella VM come se fosse una delle mie unità. Passa alla cartella wwwroot per trovare i file del sito web e cambia la pagina predefinita per visualizzare quello che vuoi:



Quando ho finito di giocare con il sito Web, posso aprire Gestione disco, fare clic con il pulsante destro del mouse su quel disco montato e selezionare Scollega VHD per coprire le mie tracce:



E poi, solo per il gusto di farlo, copio l'intero file VHD su una USB in modo da poterlo portare con me e scherzare con esso più tardi.

Cosa ne pensi dell'hosting di macchine virtuali nel cloud adesso? Questo esempio va al nocciolo del motivo per cui così tante aziende hanno paura di compiere il primo passo verso l'hosting nel cloud: esiste un livello sconosciuto di sicurezza per quegli ambienti. Per fortuna, Microsoft sta adottando misure per alleviare questa falla nella sicurezza con una nuova tecnologia chiamata VM schermate.

Crittografia dei dischi rigidi virtuali

L'idea alla base delle VM schermate è abbastanza semplice. Microsoft dispone già di una straordinaria tecnologia di crittografia delle unità, chiamata BitLocker. Le VM schermate sono VM Hyper-V con la crittografia dell'unità BitLocker abilitata. Quando l'intero file VHD è protetto e crittografato con BitLocker, nessuno sarà in grado di ottenere l'accesso backdoor a quell'unità.
Tentare di montare il VHD come abbiamo appena fatto comporterebbe un messaggio di errore e nient'altro:


Location is not available
E:\ is not accessible.
Access is denied.

Ancora meglio è quello; quando si configura la propria infrastruttura per supportare VM schermate, si blocca anche l'accesso della console Hyper-V alle VM schermate. Sebbene questo di per sé non sia un grosso problema come la crittografia delle unità, è comunque abbastanza importante da sottolineare. Se qualcuno ha accesso al server host Hyper-V e apre Hyper-V Manager, generalmente avrà la possibilità di utilizzare la funzione Connect sulle VM tenant per visualizzare ciò che era attualmente sulla console. Molto probabilmente, questo li lascerebbe a fissare una schermata di accesso che, si spera, non sarebbero in grado di violare. Ma se la console di quella VM fosse stata in qualche modo lasciata in uno stato di accesso, avrebbero accesso immediato alla manipolazione della VM, anche se l'unità fosse crittografata. Pertanto, quando crei una VM schermata, non solo crittografa il VHD utilizzando la tecnologia BitLocker,

Questo blocco hardcore ha il potenziale per causare problemi quando si tenta di risolvere legittimamente una VM? Cosa succede se è necessario utilizzare la console Hyper-V per capire perché una VM non si avvia o qualcosa del genere? Sì, questo è un punto valido e che devi considerare. Le VM schermate aumentano la sicurezza delle tue VM. Tanto che potresti, in effetti, impedirti di risolvere i problemi su quel server. Come spesso accade nel mondo IT, stiamo scambiando l'usabilità con la sicurezza.

Requisiti di infrastruttura per VM schermate

Ci sono un paio di pezzi importanti in questo puzzle di cui devi essere a conoscenza se sei interessato a eseguire VM schermate.

Host sorvegliati

Sarà necessario eseguire uno o più server host protetti per ospitare le VM schermate. Gli host sorvegliati sono essenzialmente server Hyper-V

con steroidi. Ospiteranno VM come qualsiasi altro server Hyper-V, ma sono appositamente predisposti e configurati per ospitare queste VM schermate crittografate e per attestare la propria salute come parte di questa strategia di sicurezza complessiva.

Gli host sorvegliati devono eseguire Server 2016 Datacenter o Server 2019 Datacenter e in genere si desidera che vengano avviati tramite UEFI e che contengano un chip TPM 2.0. Sebbene TPM 2.0 non sia un requisito fisso, è sicuramente consigliato.

Questi server host sorvegliati prendono quindi il posto dei tradizionali server Hyper-V. È il loro lavoro ospitare le tue VM.

Host Guardian Service (HGS)

HGS è un servizio che viene eseguito su un server, o più comunemente un cluster di tre server, e gestisce l'attestazione di host sorvegliati. Quando una VM schermata tenta di avviarsi su un server host protetto, tale host deve raggiungere HGS e attestare che è sicuro e protetto. Solo dopo che l'host ha superato l'attestazione HGS e i controlli di integrità, la VM schermata potrà essere avviata.

HGS è fondamentale per far funzionare un tessuto protetto. Se HGS non funziona, nessuna delle tue VM schermate sarà in grado di avviarsi!

Esistono requisiti diversi per HGS, a seconda della modalità di attestazione che utilizzeranno gli host sorvegliati. Impareremo a conoscere queste modalità nella prossima sezione di questo capitolo. HGS dovrà eseguire Server 2016 o Server 2019 e più comunemente si desidera utilizzare server fisici in esecuzione in un cluster a tre nodi per questo servizio.

Voglio anche sottolineare una funzionalità relativa a HGS che è nuova di zecca in Windows Server 2019: la cache di HGS. Una precedente limitazione delle VM schermate Server 2016 era che HGS doveva essere contattato ogni volta che un host sorvegliato desiderava avviare una VM schermata. Questo può diventare problematico se HGS non è disponibile per qualche motivo temporaneo. Una novità di Server 2019 è la cache HGS per le chiavi VM in modo che un host sorvegliato sia in grado di avviare VM approvate in base alle chiavi nella cache, anziché dover sempre eseguire il check-in con un HGS live. Questo può essere utile se HGS è offline (sebbene HGS sia completamente offline probabilmente significa che hai grossi problemi), ma la cache di HGS ha un caso d'uso più valido negli scenari di succursali in cui un host sorvegliato potrebbe avere una connessione di rete scarsa a HGS.

Attestati host

L'attestazione degli host sorvegliati è il segreto per utilizzare VM schermate. Questa è la base della sicurezza nel voler andare avanti con

una tale soluzione nel proprio ambiente. La possibilità per i tuoi host di attestare la loro salute e identità ti dà la tranquillità di sapere che quegli host non vengono modificati o manipolati a tua insaputa e garantisce che un dipendente host malintenzionato non possa copiare tutti i file del disco rigido della VM su un USB, portali a casa e avviali. Quelle VM schermate inizieranno sempre e solo sugli host sorvegliati nel tuo ambiente, da nessun'altra parte.

Esistono due diverse modalità che gli host sorvegliati possono utilizzare per superare l'attestazione con HGS. In realtà ce ne sono tre, ma uno è già stato deprecato. Dedichiamo un minuto per descrivere in dettaglio le diverse modalità che possono essere utilizzate tra i tuoi host sorvegliati e il tuo HGS.

Attestazioni attendibili da TPM

Questo è il modo migliore! I chip TPM sono chip fisici installati sulle schede madri del server che contengono informazioni univoche. Ancora più importante, queste informazioni non possono essere modificate o violate dal sistema operativo Windows. Quando i tuoi server host sorvegliati sono dotati di chip TPM 2.0, questo apre le porte per eseguire un'attestazione host incredibilmente potente. L'host utilizza l'avvio protetto e alcuni controlli di integrità del codice archiviati all'interno del TPM per verificare che sia integro e non sia stato modificato. HGS esegue quindi un controllo incrociato delle informazioni inviate dal TPM con le informazioni di cui è a conoscenza quando l'host sorvegliato è stato inizialmente configurato, per garantire che l'host richiedente sia effettivamente uno degli host sorvegliati approvati e che non sia stato manomesso. Se stai configurando nuovi server Hyper-V,

Attestazioni chiave host

Se i TPM non fanno per te o sono al di là delle tue capacità hardware, possiamo eseguire un'attestazione della chiave host più semplice. La possibilità per i tuoi host sorvegliati di generare una chiave host che può essere conosciuta e verificata da HGS è una novità di Windows Server 2019. Questo utilizza la tecnologia di coppia di chiavi asimmetrica per convalidare gli host sorvegliati. Fondamentalmente, creerai una nuova coppia di chiavi host o utilizzerai un certificato esistente, quindi invierai la parte pubblica di quella chiave o certificato a HGS. Quando gli host sorvegliati desiderano avviare una VM schermata, contattano per attestare con HGS e tale attestazione viene approvata o negata in base a questa coppia di chiavi.

Questo è certamente un modo più veloce e più semplice per rendere le VM schermate una realtà nella tua rete, ma non è sicuro come un'attestazione affidabile TPM.

Attestazione attendibile dall'amministratore: deprecata nel 2019

Se il tuo ambiente è nuovo e basato su Server 2019, non prestare attenzione a questo. Tuttavia, ci sono persone che eseguono VM schermate all'interno di un'infrastruttura di Windows Server 2016 e, in quel caso, c'era un'opzione aggiuntiva per l'attestazione. Comunemente noto come attestazione attendibile dall'amministratore, questo era un modo molto semplice (e non molto sicuro)
affinché i tuoi host attestino a HGS che sono stati approvati. Fondamentalmente, hai creato un gruppo di sicurezza di Active Directory (AD), hai aggiunto i tuoi host protetti in quel gruppo e quindi HGS ha considerato qualsiasi host che faceva parte di quel gruppo da proteggere e approvato per eseguire VM schermate.

Integrazione con Linux

Molte aziende utilizzano Linux in un modo o nell'altro. L'uso di Linux potrebbe effettivamente essere destinato a fare un ingresso più ampio nel mondo di Windows Server ora che abbiamo questo livello di integrazione più elevato possibile all'interno di Windows Server 2019. Ci sono modi in cui il tuo Server 2019 può ora essere utilizzato per interagire con VM Linux:

- **In esecuzione in Hyper-V**: Le macchine virtuali ospitate su un server Hyper-V erano limitate ai sistemi operativi basati su Windows. Non è più così. L'ambito dell'host di virtualizzazione Hyper-V è stato ora ampliato per consentire l'esecuzione di VM basate su Linux in Hyper-V Manager. C'è anche una buona integrazione con la tastiera e il mouse!
- **VM schermate Linux**: Ora sai come eseguire VM schermate in Hyper-V e sai anche come eseguire VM basate su Linux all'interno di Hyper-V. Ciò significa che possiamo combinare queste due idee ed eseguire una VM Linux anch'essa schermata? Perché sì, certamente possiamo. Questa funzionalità è stata introdotta in Windows Server 1709 ed è presente anche nella versione più recente di LTSC di Windows Server 2019.
- **Correndo in container**: Sebbene la maggior parte degli amministratori di server e Hyper-V non mordicheranno il bit per installare Linux sui loro sistemi perché semplicemente non hanno motivo di farlo, ci saranno sicuramente molti più discorsi su Linux da chiunque su DevOps lato della casa IT. Quando si creano applicazioni scalabili destinate al cloud, si parla spesso di eseguire queste applicazioni all'interno di container. In passato, ospitare contenitori su un server Windows significava che il contenitore stesso doveva eseguire Windows, ma non di più. È ora possibile ospitare contenitori basati su Linux su Windows Server 2019. Ciò consente una grande flessibilità al processo di sviluppo delle applicazioni e sarà una considerazione importante per il futuro dei contenitori.

Deduplicazione ReFS

Sebbene i file system e le funzionalità di deduplicazione siano tecnologie di cui non ci si può aspettare che vengano discusse quando si tratta di Hyper-V, i miglioramenti in Server 2019 relativi a ReFS e alla deduplicazione dei dati comportano alcuni enormi vantaggi per i server Hyper-V. Nel caso in cui si tratti di termini sconosciuti, dedichiamo un minuto alla definizione di ReFS e deduplicazione.

ReFS

Chiunque abbia lavorato su computer per un po 'riconoscerà FAT, FAT32 e NTFS. Questi sono file system che possono essere utilizzati durante la formattazione dei dischi rigidi. Le diverse versioni dei filesystem si traducono in diverse capacità di come puoi utilizzare quel disco rigido. Per diversi anni, NTFS è stato lo standard de facto per tutti i dischi rigidi collegati a macchine Windows.

Cioè, fino a quando non è arrivato Windows Server 2016. Ora abbiamo una nuova opzione del file system chiamata ReFS. Anche se lavori in un reparto IT ogni giorno, potresti non aver mai sentito parlare di ReFS perché finora non viene utilizzato molto. Viene utilizzato principalmente nei server coinvolti con Storage Spaces Direct (S2D). Se è l'ultimo e il più grande filesystem di Microsoft, perché non viene utilizzato come opzione predefinita su nessun nuovo sistema? Principalmente perché ReFS non è un filesystem avviabile. Ciò annulla immediatamente la capacità dei sistemi con un singolo disco rigido di eseguire ReFS sull'intera unità. Ciò che implica è che ReFS è per volumi secondari su server, forse volumi destinati a contenere grandi quantità di dati.

In quei casi in cui formatti un secondo volume come ReFS e memorizzi i dati su di esso, ci sono alcuni grandi vantaggi in termini di resilienza e prestazioni nell'utilizzo di ReFS invece di NTFS. Questi vantaggi sono stati progettati per far funzionare meglio le implementazioni S2D.

Deduplicazione dei dati

La deduplicazione dei dati è semplicemente la capacità di un sistema informatico di rilevare più bit di dati su un'unità identici e pulirli. Se ci fossero sei copie dello stesso identico file su un sistema, la deduplicazione potrebbe eliminarne cinque, conservandone una ai fini di tutte e sei le posizioni. Questa idea consente un notevole risparmio di spazio. La deduplicazione dei dati in sé non è una novità; abbiamo avuto alcune funzionalità introdotte nel lontano Server 2012 in merito a questo.

Windows Server 2019 è la prima piattaforma in cui è possibile abilitare la deduplicazione dei dati su un volume formattato tramite ReFS.

Perché questo è importante per Hyper-V?

La deduplicazione dei dati può essere incredibilmente vantaggiosa da eseguire su un volume che archivia i file del disco rigido della VM Hyper-V perché, come puoi immaginare, ci saranno un sacco di informazioni che vengono duplicate più e più volte quando esegui dozzine di VM . Pensa a tutti quei file del sistema operativo Windows che saranno identici tra tutte le tue VM in esecuzione sull'host Hyper-V. È abbastanza ovvio il motivo per cui sarebbe utile abilitare la deduplicazione dei dati su un volume che memorizza i file VHDX.

ReFS ha una grande resilienza e vantaggi in termini di prestazioni rispetto a NTFS, quindi è anche ovvio che i file VHDX sarebbero meglio serviti se archiviati su un volume ReFS.

Windows Server 2019 è la prima piattaforma in cui puoi avere la tua torta e mangiarla anche tu. Ora abbiamo la possibilità di creare un volume ReFS per l'archiviazione dei dischi rigidi delle macchine virtuali e abilitare anche la deduplicazione dei dati sullo stesso volume.

Server Hyper-V 2019

È molto facile entusiasmarsi per la virtualizzazione. Crea hardware, installa Windows Server 2019, implementa il ruolo Hyper-V e bam! Sei pronto per iniziare a distribuire centinaia e centinaia di VM nel tuo ambiente ... giusto?

Non necessariamente. Non abbiamo ancora parlato di licenze e troppo spesso la nostra abilità tecnologica è limitata dai requisiti di licenza. Lo stesso vale con Hyper-V. Ovviamente, ogni macchina virtuale che si avvia deve avere la propria licenza del sistema operativo. Questo requisito ha senso. Ciò che non è così ovvio, tuttavia, è il fatto che puoi eseguire solo un certo numero di VM sul tuo server Hyper-V, a seconda dello SKU che usi per il sistema operativo host stesso.

Il problema principale è che l'utilizzo di Windows Server 2019 Standard Edition come Hyper-V Server ti consentirà di eseguire due VM. Due! Questo è tutto, non di più. Sarai in grado di avviare un paio di macchine virtuali e quindi non sarà più possibile eseguirle. Chiaramente, lo SKU Standard Edition non è progettato per essere utilizzato come server Hyper-V.

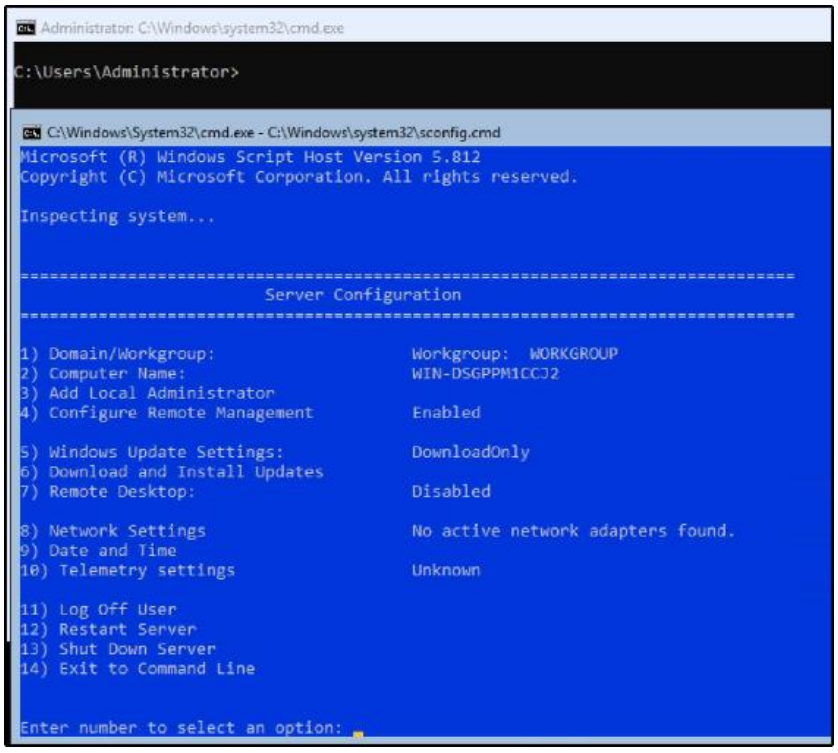
Questo ti lascia con Windows Server 2019 Datacenter Edition. Fortunatamente, Datacenter ti consente di eseguire VM illimitate! Questa è un'ottima notizia! Tranne una cosa: l'edizione Datacenter di solito costa molte migliaia di dollari. Questo è un fattore molto limitante per le distribuzioni di server Hyper-V.

Tutto questo parlare di licenze e di quanto possa essere disordinato o costoso porta a uno
punto: Hyper-V Server 2019. Aspetta un attimo, non è di questo che tratta l'intero capitolo? Non è solo Windows Server 2019 con il ruolo Hyper-V installato? No, per niente.

Hyper-V Server 2019 è il suo animale. Ha il suo programma di installazione e un'interfaccia utente completamente diversa da un server tradizionale. L'installazione di Hyper-V Server 2019 su un componente hardware si tradurrà in un server in grado di ospitare un numero illimitato di VM Hyper-V, ma nient'altro. Non è possibile utilizzarlo come server generico per ospitare altri ruoli o servizi. Hyper-V Server inoltre non dispone di un'interfaccia utente grafica.

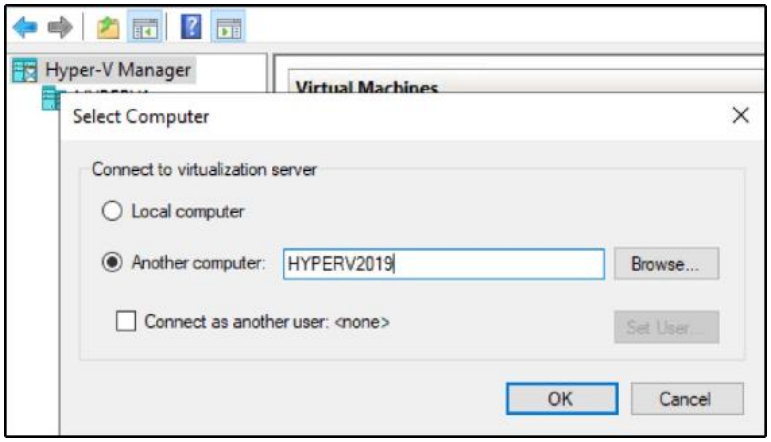
Hyper-V Server 2019 ha un enorme vantaggio: è GRATUITO. Sei ancora responsabile delle licenze su ciascuna delle VM stesse, ovviamente, ma per avere un sistema operativo host gratuito in grado di eseguire un numero illimitato di VM, ora questo è qualcosa che il mio portafoglio può davvero ottenere.

Ho masterizzato il programma di installazione ISO per Hyper-V Server 2019 su un DVD (per fortuna questo è abbastanza piccolo da adattarsi effettivamente!) E ho appena finito di installarlo sul mio hardware. L'installazione del sistema operativo stesso era completamente familiare: tutte le schermate e le opzioni di installazione erano le stesse come se stessi installando la versione completa di Windows Server 2019. Tuttavia, ora che il programma di installazione è terminato e ho avviato il sistema operativo del mio Hyper-V Server 2019, tutto sembra completamente diverso:


Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>
C:\Windows\System32\cmd.exe - C:\Windows\system32\sconfig.cmd
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.
Inspecting system...
Server Configuration
1) Domain/Workgroup: Workgroup: WORKGROUP
2) Computer Name: WIN-DSGPPM1CCJ2
3) Add Local Administrator
4) Configure Remote Management Enabled
5) Windows Update Settings: DownloadOnly
6) Download and Install Updates
7) Remote Desktop: Disabled
8) Network Settings No active network adapters found.
9) Date and Time
10) Telemetry settings Unknown
11) Log Off User
12) Restart Server
13) Shut Down Server
14) Exit to Command Line
Enter number to select an option:

Ci viene presentato solo un prompt dei comandi e al suo interno è stato avviato automaticamente un'utilità di configurazione chiamata SConfig. Usando la tastiera qui, posso fare cose come impostare il nome host di questo server, unirlo a un dominio e modificare le impostazioni di rete. Una volta che hai finito di utilizzare questa interfaccia CLI per impostare i requisiti di base sul server e farlo comunicare con la rete, non abbiamo davvero bisogno di accedere nuovamente alla console di questo server Hyper-V, a meno che tu non debba tornare indietro e rivisitare questo schermata di configurazione per cambiare qualcosa. Invece, dopo aver configurato il server Hyper-V, è sufficiente utilizzare Hyper-V Manager, o PowerShell, su un altro server o desktop all'interno della rete, per accedere in remoto alla gestione delle VM in esecuzione su questo server Hyper-V.

Nello screenshot seguente, puoi vedere che ho avviato Hyper-V Manager. Sto eseguendo questa istanza di Hyper-V Manager dal mio computer Windows 10 in cui è installato il ruolo Hyper-V. Da qui, faccio clic con il pulsante destro del mouse su Hyper-V Manager e scelgo Connetti**al server.** Quindi inserisco il nome del mio nuovo server Hyper-V e la console crea un file
connessione remota. Da questa connessione remota, ora posso utilizzare tutte le funzionalità all'interno del mio Window 10 Hyper-V Manager come se fossi connesso direttamente al nuovo server Hyper-V:



Analogamente al modo in cui la maggior parte delle attività eseguite su un Server Core o Nano Server vengono gestite in remoto, tramite l'uso di console remote o PowerShell, tutti gli interventi di manutenzione e

amministrazione in corso di questo server Hyper-V avvengono da una console Hyper-V Manager remota .

Hyper-V Server offre i vantaggi in termini di sicurezza di un'interfaccia senza GUI, combinati con i vantaggi di flessibilità dell'hosting di un numero illimitato di macchine virtuali, a un prezzo con cui nessuno può discutere!

Sommario

Non ho numeri ufficiali, ma correrò il rischio e dirò che oggi ci sono già più server virtuali in esecuzione che server fisici, per mantenere il nostro mondo online. Mentre la battaglia continua a imperversare tra quale piattaforma hypervisor è la migliore - in genere l'argomento è diviso tra Hyper-V o VMware - non puoi ignorare il fatto che la virtualizzazione è la via del futuro. Microsoft investe grandi quantità di tempo e risorse per assicurarsi che Hyper-V rimanga sempre un passo avanti rispetto alla concorrenza e per introdurre sempre più funzionalità a ogni versione in modo che tu possa mantenere la tua infrastruttura virtualizzata sempre perfettamente funzionante. La capacità di virtualizzazione del cloud è ancora più potente del server Hyper-V in sede? Direi di si, perché l'infrastruttura che è in atto presso un provider di servizi cloud sarà l'onnipotente Oz rispetto a ciò che una singola azienda può fornire nel proprio data center. Questo significa che puoi dimenticarti del tutto di Hyper-V e utilizzare solo server forniti dal cloud? Forse un giorno, ma la maggior parte non è ancora pronta a fare quel salto. La necessità di server e servizi in sede è ancora immensa e alcuni settori semplicemente non consentiranno mai che i propri dati e le proprie applicazioni siano ospitati da terze parti. Comprendere le capacità di Hyper-V ed essere in grado di costruire questa infrastruttura da zero ti darà un grande vantaggio quando cerchi un lavoro tecnologico in un'organizzazione incentrata su Microsoft. Questo significa che puoi dimenticarti del tutto di Hyper-V e utilizzare solo server forniti dal cloud? Forse un giorno, ma la maggior parte non è ancora pronta a fare quel salto. La necessità di server e servizi in sede è ancora immensa e alcuni settori semplicemente non consentiranno mai che i propri dati e le proprie applicazioni siano ospitati da terze parti. Comprendere le capacità di Hyper-V ed essere in grado di costruire questa infrastruttura da zero ti darà un grande vantaggio quando cerchi un lavoro tecnologico in un'organizzazione incentrata su Microsoft. Questo significa che puoi dimenticarti del tutto di Hyper-V e utilizzare solo server forniti dal cloud? Forse un giorno, ma la maggior parte non è ancora pronta a fare quel salto. La necessità di server e servizi in sede è ancora immensa e alcuni settori semplicemente non consentiranno mai

che i propri dati e le proprie applicazioni siano ospitati da terze parti. Comprendere le capacità di Hyper-V ed essere in grado di costruire questa infrastruttura da zero ti darà un grande vantaggio quando cerchi un lavoro tecnologico in un'organizzazione incentrata su Microsoft.

Questo ci porta alla fine della nostra storia sul nuovo Windows Server 2019. Molti degli argomenti che abbiamo discusso potrebbero riempire interi libri e spero che le idee fornite in questo volume siano sufficienti per spingerti ad approfondire le tecnologie che tu piano con cui lavorare. La tecnologia Microsoft regna sovrana nella maggior parte dei data center in tutto il mondo. Le funzionalità nuove e aggiornate all'interno di Windows Server 2019 garantiranno che questa tendenza continui a lungo nel futuro.

Domande

1. Quali sono i tre tipi di switch virtuali all'interno di Hyper-V?
2. Se avessi bisogno di creare una macchina virtuale che si avviava utilizzando UEFI, quale generazione di VM avresti bisogno di creare?
3. Vero o falso: in Windows Server 2019 Hyper-V, è necessario arrestare una macchina virtuale per modificare la quantità di memoria allocata (RAM).
4. Vero o falso: l'unico modo per interagire con una macchina virtuale è tramite la console Hyper-V.

5. Qual è il nome della tecnologia all'interno di Hyper-V che consente di acquisire immagini istantanee di macchine virtuali, che possono essere successivamente ripristinate?
6. Quando si eseguono VM schermate nel proprio ambiente, qual è il nome del ruolo che gestisce l'attestazione dei server host Hyper-V?
7. Qual è il metodo di attestazione più completo per le VM schermate: attestazione della chiave host, attestazione attendibile TPM o attestazione attendibile dell'amministratore?

Valutazioni

Capitolo 1: Introduzione a Windows Server 2019

1. Fare clic con il pulsante destro del mouse sul pulsante Start e selezionare Windows PowerShell (amministratore) dal menu delle attività di amministrazione rapide
2. WinKey + X
3. Microsoft Azure
4. Standard e Datacenter 5. 2
6. Server Core
7. Canale di manutenzione a lungo termine (LTSC)
8. Entrambi, sebbene le impostazioni di Windows siano il metodo preferito per la maggior parte delle opzioni di configurazione

Capitolo 2: Installazione e gestione di Windows Server 2019

1. Windows Admin Center (WAC).
2. Falso. Windows Server 2019 può essere installato su hardware fisico o come istanza di macchina virtuale.
3. Falso. L'opzione predefinita per Windows Server 2019 è Server Core, che non dispone di un'interfaccia utente grafica.
4. Get-WindowsFeature | Dove installato .
5. Vero.
6. Strumenti di amministrazione remota del server (RSAT).
7. Al momento della stesura di questo documento, Microsoft Edge e Google Chrome. Tieni presente che Internet Explorer non è supportato.

Capitolo 3: Servizi di infrastruttura di base

1. Unità organizzativa (UO)
2. Prestaging dell'account
3. Siti e servizi di Active Directory
4. Controller di dominio di sola lettura (RODC)
5. Il criterio di dominio predefinito
6. Record AAAA (quad A)
7. DSA.MSC

Capitolo 4: Certificati in Windows Server 2019

1. Autorità di certificazione
2. CA radice aziendale
3. No, questo non è uno scenario consigliato
4. Il nuovo modello di certificato deve essere pubblicato
5. Registrazione automatica del certificato
6. Chiave privata
7. Richiesta di firma del certificato (CSR)

Capitolo 5: Rete con Windows Server 2019

1. 128 bit.
2. 2001: ABCD: 1: 2 :: 1.
3. PERCORSO.
4. Falso. Ciò causerà problemi di routing. Dovresti sempre avere un solo indirizzo gateway predefinito su un sistema, indipendentemente dal numero di schede NIC che ha.
5. New-NetRoute
6. Windows Server 2019, 2016 e 2012 R2.

Capitolo 6: Abilitazione della forza lavoro mobile

1. Sempre su VPN
2. IKEv2 e SSTP
3. Windows 10 1607
4. Quando desideri utilizzare il tunnel dei dispositivi AOVPN
5. No, la tua rete interna può essere completamente IPv4
6. Network Location Server (NLS)
7. Il WAP può essere implementato come proxy ADFS

Capitolo 7: rafforzamento e sicurezza

1. Windows Defender Antivirus
2. Il profilo di dominio
3. Pubblico e privato
4. ICMPv4
5. Politica di gruppo
6. VM schermata
7. Analisi avanzata delle minacce

Capitolo 8: Server Core

1. Vero
2. Falso, il passaggio avanti e indietro non è possibile in Windows Server 2019
3. Prompt dei comandi
4. Get-NetIPConfiguration
5. Rinomina computer
6. PowerShell, Server Manager, RSAT e Windows Admin Center
7. Sconfig.exe

Capitolo 9: Ridondanza in Windows Server 2019

1. Bilanciamento del carico di rete
2. Indirizzo IP dedicato e indirizzo IP virtuale
3. IGMP unicast, multicast e multicast
4. NLB è una caratteristica
5. Hyper-V e servizi di file
6. Una chiavetta USB
7. Falso, puoi utilizzare qualsiasi tipo di disco rigido con S2D

Capitolo 10: PowerShell

1. Digita semplicemente la parola powershell e premere Invio
2. Get-Command
3. Enter-PSSession
4. .PS1
5. RemoteSigned
6. *Tab*
7. Il servizio WinRM

Capitolo 11: Contenitori e Nano Server

1. Server Core o Nano Server
2. Contenitore Hyper-V
3. Falso, la possibilità di eseguire contenitori Windows e Linux è una novità di Windows Server 2019
4. immagini docker
5. Kubernetes
6. Vero

Capitolo 12: Virtualizzazione del data center con Hyper-V

1. Esterno, interno e privato
2. Seconda generazione
3. Falso, puoi regolare al volo il conteggio della RAM di una VM
4. Falso, una volta installato il sistema operativo della tua VM, puoi interagire con esso tramite qualsiasi altro metodo di amministrazione tradizionale, come RDP
5. Checkpoint
6. Servizio guardiano host
7. Attestazione attendibile TPM