Beschreiben von Azure Compute- und Azure-Netzwerkdiensten

1 Std. 8 Min.Modul14 Einheiten

Feedback

Anfänger Administrator Entwickler DevOps-Techniker Lösungsarchitekt Azure

Der Schwerpunkt dieses Moduls liegt auf einigen der Computer- und Netzwerkdienste, die in Azure verfügbar sind.

Lernziele

Nach Abschluss dieses Moduls beherrschen Sie Folgendes:

- Vergleichen von Computetypen, einschließlich Containerinstanzen, VMs und Funktionen
- Beschreiben von Optionen für VMs, einschließlich VMs, Virtual Machine Scale Sets, Verfügbarkeitsgruppen und Azure Virtual Desktop
- Beschreiben der für VMs erforderlichen Ressourcen
- Beschreiben der Optionen für das Anwendungshosting, einschließlich Azure Web-Apps, Containern und VMs
- Beschreiben von virtuellen Netzwerken, einschließlich des Zwecks von Azure Virtual Networks, virtuellen Azure-Subnetzen, Peering, Azure DNS, VPN Gateway und ExpressRoute
- Definieren von öffentlichen und privaten Endpunkten

Beschreiben von Azure-VMs

6 Minuten

100 XP

Azure Virtual Machines ermöglicht Ihnen, VMs in der Cloud zu erstellen und zu verwenden. VMs stellen IaaS (Infrastructure-as-a-Service) in Form eines virtualisierten Servers zur Verfügung und können auf viele unterschiedliche Arten verwendet werden. Genau wie bei einem physischen Computer können Sie die gesamte Software anpassen, die auf Ihrer VM ausgeführt wird. VMs sind eine ideale Wahl, wenn Sie Folgendes benötigen:

- Vollständige Kontrolle über das Betriebssystem
- Die Möglichkeit, benutzerdefinierte Software auszuführen
- Die Möglichkeit, benutzerdefinierte Hostingkonfigurationen zu verwenden

Ein virtueller Azure-Computer bietet Ihnen die Flexibilität der Virtualisierung, ohne Zeit und Geld für den Kauf und die Verwaltung der Hardware aufwenden zu müssen, mit der der virtuelle Computer betrieben wird. Sie müssen die auf der VM ausgeführte Software jedoch noch immer konfigurieren, aktualisieren und verwalten, da es sich um ein IaaS-Angebot handelt.

Sie können sogar ein bereits erstelltes Image erstellen oder verwenden, um VMs noch schneller bereitzustellen. Innerhalb weniger Minuten können Sie eine VM erstellen, wenn Sie ein vorkonfiguriertes VM-Image verwenden. Ein Image ist eine Vorlage, die zum Erstellen einer VM verwendet wird. Es kann bereits ein Betriebssystem und andere Software wie z. B. Entwicklungstools oder Webhostingumgebungen enthalten.

Skalieren virtueller Computer in Azure

Sie können einzelne VMs für Test-, Entwicklungs- oder kleinere Aufgaben ausführen. Außerdem können Sie VMs gruppieren, um Hochverfügbarkeit, Skalierbarkeit und Redundanz zu gewährleisten. Azure kann auch die Gruppierung von VMs für Sie mit Features wie Skalierungsgruppen und Verfügbarkeitssätzen verwalten.

VM-Skalierungsgruppen

Mit VM-Skalierungsgruppen können Sie eine Gruppe von identischen virtuellen Computern mit Lastenausgleich erstellen und verwalten. Wenn Sie einfach mehrere VMs mit demselben Zweck erstellt haben, müssen Sie sicherstellen, dass sie alle gleich konfiguriert wurden und dann Parameter für das Netzwerkrouting einrichten, um die Effizienz zu gewährleisten. Sie müssen auch die Auslastung überwachen, um festzustellen, ob Sie die Anzahl der VMs erhöhen oder verringern müssen.

Azure hingegen automatisiert den größten Teil dieser Arbeit mit VM-Skalierungsgruppen. Mit Skalierungsgruppen können Sie eine große Anzahl von VMs innerhalb weniger Minuten zentral verwalten, konfigurieren und aktualisieren. Die Anzahl von VM-Instanzen kann als Reaktion auf die Nachfrage oder einen definierten Zeitplan automatisch erhöht oder verringert werden. VM-Skalierungsgruppen stellen auch automatisch einen Lastenausgleich bereit, über den sichergestellt wird, dass Ihre Ressourcen effizient genutzt werden. Mit VM-Skalierungsgruppen können Sie umfassende Dienste für Bereiche wie Compute, Big Data und Containerworkloads erstellen.

VM-Verfügbarkeitsgruppen

Verfügbarkeitsgruppen sind ein weiteres Tool, mit dem Sie eine robustere, hoch verfügbare Umgebung erstellen können. Verfügbarkeitsgruppen sind so konzipiert, dass Updates der VMs verschoben werden und dass Stromversorgung und Netzwerkverbindungen unabhängig sind, um zu verhindern, dass Sie beim einem Ausfall eines einzelnen Netzwerks oder bei einem Stromausfall alle Ihre VMs verlieren.

Die Verfügbarkeit erreicht diese Ziele, indem VMs auf zwei Arten gruppiert werden: Aktualisieren der Domäne und Fehlerdomäne.

- **Updatedomäne:** In der Updatedomäne werden VMs gruppiert, die gleichzeitig neu gestartet werden können. Diese Einrichtung ermöglicht es Ihnen Updates anzuwenden und gleichzeitig sicher zu sein, dass nur eine Gruppe in einer Updatedomäne gleichzeitig offline ist. Alle Computer in einem Updatedomänenupdate. Wenn eine Updategruppe den Updateprozess durchläuft, werden ihr 30 Minuten Zeit für die Wiederherstellung gewährt, bevor die Wartung in der nächsten Updatedomäne gestartet wird.
- **Fehlerdomäne:** In einer Fehlerdomäne werden VMs mit einer gemeinsamen Stromquelle und einem gemeinsamen Netzwerkswitch gruppiert. Standardmäßig werden Ihre VMs in einer Verfügbarkeitsgruppe auf bis zu drei Fehlerdomänen aufgeteilt. Dies hilft beim Schutz vor einem physischen Stromversorgungs- oder Netzwerkfehler, da Ihre VMs sich in verschiedenen Fehlerdomänen befinden (und daher mit verschiedenen Stromversorgungs- und Netzwerkressourcen verbunden sind).

Und das Beste daran ist, dass für die Konfiguration einer Verfügbarkeitsgruppe keine zusätzlichen Kosten anfallen. Sie bezahlen nur für die VM-Instanzen, die Sie erstellen.

Anwendungsbeispiele für virtuelle Computer

Einige allgemeine Beispiele oder Anwendungsfälle für VMs:

- **Während Tests und Entwicklung:** VMs bieten eine schnelle und einfache Möglichkeit, verschiedene Betriebssystem- und Anwendungskonfigurationen zu erstellen. Test- und Entwicklungsmitarbeiter können die VMs dann einfach löschen, wenn sie diese nicht mehr benötigen.
- **Beim Ausführen von Anwendungen in der Cloud:** Durch die Möglichkeit zur Ausführung bestimmter Anwendungen in der öffentlichen Cloud, statt eine herkömmliche Infrastruktur für deren Ausführung erstellen zu müssen, können Sie erheblich Kosten einsparen. Beispielsweise muss eine Anwendung möglicherweise schwankenden Nachfragen verarbeiten. Wenn Sie VMs herunterfahren, wenn Sie sie nicht benötigen, oder sie schnell wieder hochfahren, um einem plötzlichen Anstieg der Nachfrage zu begegnen, zahlen Sie nur für die genutzten Ressourcen.
- **Bei der Erweiterung Ihres Rechenzentrums in die Cloud:** Ein Unternehmen kann die Funktionen des eigenen lokalen Netzwerks erweitern, indem es ein virtuelles Netzwerk in Azure erstellt und diesem virtuellen Netzwerk VMs hinzufügt. Anwendungen wie SharePoint können dann auf einem virtuellen Azure-Computer anstatt lokal ausgeführt werden. Dadurch ist der Einsatz einfacher bzw. kostengünstiger als in einer lokalen Umgebung.
- **Bei der Notfallwiederherstellung:** Wie beim Ausführen bestimmter Anwendungstypen in der Cloud und beim Erweitern eines lokalen Netzwerks in die Cloud erreichen Sie auch durch die Verwendung eines IaaS-basierten Ansatzes zur Notfallwiederherstellung erhebliche Kosteneinsparungen. Bei einem Ausfall eines primären Rechenzentrums können Sie in Azure ausgeführte VMs erstellen, die Ihre wichtigen Anwendungen ausführen, und diese wieder herunterfahren, sobald das primäre Rechenzentrum wieder betriebsbereit ist.

Wechseln in die Cloud mit virtuellen Computern

Virtuelle Computer sind ebenfalls eine gute Wahl, wenn Sie von einem physischen Server in die Cloud wechseln (als „Lift and Shift“ bezeichnet). Sie können ein Image des physischen Servers erstellen und dieses auf einer VM mit wenigen oder gar keinen Änderungen hosten. Sie müssen die VM genauso wie einen physischen lokalen Server verwalten: Sie sind verantwortlich für die Wartung des installierten Betriebssystems und der Software.

VM-Ressourcen

Wenn Sie eine VM bereitstellen, können Sie auch die Ressourcen auswählen, die dieser VM zugeordnet sind, einschließlich:

- Größe (Zweck, Anzahl der Prozessorkerne und Menge von RAM)
- Speicherdatenträger (Festplatten, SSD-Laufwerke usw.)
- Netzwerk (virtuelles Netzwerk, öffentliche IP-Adresse und Portkonfiguration)

Beschreiben von Azure Virtual Desktop

100 XP

5 Minuten

Ein anderer VM-Typ ist Azure Virtual Desktop. Azure Virtual Desktop ist ein in der Cloud ausgeführter Dienst für die Desktop- und Anwendungsvirtualisierung. Er ermöglicht Ihnen, eine in der Cloud gehostete Version von Windows von jedem Standort aus zu verwenden. Azure Virtual Desktop funktioniert über Geräte und Betriebssysteme hinweg, mit Apps, über die Sie auf Remotedesktops zugreifen können, sowie mit den meisten modernen Browsern.

Im folgenden Video erhalten Sie eine Übersicht über Azure Virtual Desktop:

Erhöhen der Sicherheit

Azure Virtual Desktop bietet zentralisierte Sicherheitsverwaltung für die Desktops von Benutzer*innen mit Microsoft Entra ID. Sie können die mehrstufige Authentifizierung (Multi-Factor Authentication, MFA) zum Sichern von Benutzeranmeldungen aktivieren. Sie können den Zugriff auf Daten auch schützen, indem Sie Benutzern differenzierte rollenbasierte Zugriffssteuerung zuweisen.

Bei Azure Virtual Desktop werden die Daten und Apps von der lokalen Hardware getrennt. Der eigentliche Desktop und die Apps werden in der Cloud ausgeführt, sodass das Risiko reduziert wird, dass vertrauliche Daten auf einem persönlichen Gerät verbleiben. Darüber hinaus sind Benutzersitzungen sowohl in Umgebungen mit einer Sitzung als auch in Umgebungen mit mehreren Sitzungen isoliert.

Bereitstellung von Windows 10 oder Windows 11 mit mehreren Sitzungen

Mit Azure Virtual Desktop können Sie Windows 10 oder Windows 11 Enterprise für mehrere Sitzungen verwenden, die einzigen clientbasierten Windows-Betriebssysteme, die mehrere gleichzeitige Benutzer*innen auf einer einzelnen VM ermöglichen. Azure Virtual Desktop bietet im Vergleich zu Windows Server-basierten Betriebssystemen außerdem eine konsistentere Umgebung mit breiterer Anwendungsunterstützung.

Beschreiben von Azure-Containern

6 Minuten

100 XP

Obwohl virtuelle Computer eine ausgezeichnete Möglichkeit sind, die Kosten im Vergleich zu den Investitionen zu senken, die für physische Hardware erforderlich sind, sind sie dennoch auf ein einziges Betriebssystem pro virtuellem Computer beschränkt. Container sind eine gute Wahl, wenn Sie mehrere Instanzen einer Anwendung auf einem einzelnen Hostcomputer ausführen möchten.

Was sind Container?

Container sind eine Virtualisierungsumgebung. Ähnlich wie beim Ausführen mehrerer virtueller Computer auf einem einzigen physischen Host können Sie mehrere Container auf einem einzigen physischen oder virtuellen Host ausführen. Im Gegensatz zu virtuellen Computern verwalten Sie das Betriebssystem für einen Container jedoch nicht. VMs scheinen eine Instanz eines Betriebssystems zu sein, mit dem Sie eine Verbindung herstellen und das Sie verwalten können. Aber Container sind schlank und so konzipiert, dass sie dynamisch erstellt, skaliert und beendet werden können. Es ist möglich, VMs zu erstellen und bereitzustellen, wenn die Anwendungsnachfrage steigt, aber Container stellen eine weniger aufwendige, agilere Methode dar. Container sind so konzipiert, dass Sie bei Bedarf auf Änderungen reagieren können. Zudem können Container im Fall eines Absturzes oder einer Hardwareunterbrechung schnell neu gestartet werden. Eine der beliebtesten Containerengines ist Docker, und Azure unterstützt Docker.

Vergleich von virtuellen Computern mit Containern

Im folgenden Video werden einige wichtige Unterschiede zwischen VMs und Containern hervorgehoben:

Azure Container Instances

Azure Container Instances bietet die schnellste und einfachste Möglichkeit, einen Container in Azure auszuführen, ohne VMs verwalten oder zusätzliche Dienste einsetzen zu müssen. Azure Container Instances ist ein PaaS-Angebot (Platform as a Service). Mit Azure Container Instances können Sie Ihre Container hochladen und dann durch den Dienst ausführen lassen.

Azure Container Apps

Azure Container Apps ähnelt in vielerlei Hinsicht einer Containerinstanz. Mit diesem Dienst können Sie sofort loslegen und müssen keine Container verwalten. Zudem handelt es sich um ein PaaS-Angebot. Container Apps hat zusätzliche Vorteile, z. B. die Möglichkeit, Lastenausgleich und Skalierung zu integrieren. Durch diese zusätzlichen Funktionen sind Sie beim Entwerfen flexibler.

Azure Kubernetes Service

Azure Kubernetes Service (AKS) ist ein Containerorchestrierungsdienst. Ein Orchestrierungsdienst verwaltet den Lebenszyklus von Containern. Wenn Sie eine Containerflotte bereitstellen, kann AKS die Flottenverwaltung einfacher und effizienter gestalten.

Verwenden von Containern in Ihren Lösungen

Container werden oft verwendet, um Lösungen mithilfe einer Microservicearchitektur zu erstellen. Bei dieser Architektur teilen Sie Lösungen in kleinere, unabhängige Teile auf. Sie können eine Website beispielsweise in einen Container aufteilen, der Ihr Front-End hostet, einen weiteren, der Ihr Back-End hostet, und einen dritten für den Speicher. Dadurch können Sie einzelne Bestandteile Ihrer App in logische Abschnitte aufteilen, die unabhängig voneinander verwaltet, skaliert oder aktualisiert werden können.

Angenommen, das Back-End Ihrer Website hat die maximale Kapazität erreicht, aber Front-End und Speicher werden nicht so sehr beansprucht. Über Container können Sie das Back-End einzeln skalieren, um die Leistung zu verbessern. Wenn eine solche Änderung erforderlich ist, können Sie auch den Speicherdienst ändern oder das Front-End anpassen, ohne dass sich dies auf andere Komponenten auswirkt.

Beschreiben von Azure Functions

4 Minuten

100 XP

Azure Functions ist eine ereignisgesteuerte, serverlose Computeoption, die keine Wartung von VMs oder Containern erfordert. Wenn Sie eine App mithilfe von VMs oder Containern erstellen, müssen diese Ressourcen ausgeführt werden, damit Ihre App funktioniert. Bei Azure Functions wird die Funktion durch ein Ereignis ausgelöst, sodass Sie keine Ressourcen bereitstellen müssen, wenn keine Ereignisse vorhanden sind.

Serverloses Computing in Azure

Vorteile von Azure Functions

Azure Functions eignet sich ideal, wenn Sie sich nur um den Code zum Ausführen Ihres Diensts und nicht die zugrunde liegende Plattform oder Infrastruktur kümmern möchten. Functions wird häufig verwendet, wenn Sie als Reaktion auf ein Ereignis (häufig über eine REST-Anforderung), einen Timer oder eine Nachricht von einem anderen Azure-Dienst eine Aufgabe ausführen müssen und wenn diese Aufgabe schnell (innerhalb von Sekunden oder schneller) erledigt werden kann.

Functions wird automatisch nach Bedarf skaliert und ist somit eine gute Wahl, wenn der Bedarf variabel ist.

Azure Functions führt Ihren Code aus, wenn er ausgelöst wird, und hebt die Zuteilung von Ressourcen automatisch auf, wenn die jeweilige Funktion beendet wurde. In diesem Modell wird Ihnen nur die CPU-Zeit berechnet, die zum Ausführen Ihrer Funktion benötigt wurde.

Funktionen können entweder zustandslos oder zustandsbehaftet sein. Wenn diese zustandslos sind (Standardeinstellung), verhalten sie sich bei jeder Reaktion auf ein Ereignis so, als wären sie neu gestartet worden. Wenn sie zustandsbehaftet sind (Durable Functions genannt), wird ein Kontext durch die Funktion übergeben, um frühere Aktivitäten zu verfolgen.

Functions ist eine wichtige Komponente beim serverlosen Computing. Zudem ist Functions auch eine allgemeine Computeplattform zum Ausführen beliebiger Codetypen. Wenn sich die Anforderungen der Entwickler-App ändern, können Sie das Projekt in einer Umgebung bereitstellen, die nicht serverlos ist. Dank dieser Flexibilität können Sie Skalierungen vornehmen, in virtuellen Netzwerken arbeiten und die Funktionen sogar vollständig isolieren.

Beschreiben der Optionen zum Anwendungshosting

100 XP

3 Minuten

Wenn Sie Ihre Anwendung in Azure hosten möchten, werden Sie zunächst mit einer VM oder einem Container beginnen. Sowohl VMs als auch Container stellen hervorragende Hostinglösungen dar. VMs bieten Ihnen maximale Kontrolle über die Hostingumgebung und ermöglichen Ihnen, sie genau nach Ihren Wünschen zu konfigurieren. Wenn Sie neu in der Cloud sind, stellen VMs möglicherweise auch die vertrauteste Hostingmethode dar. Container können durch die Möglichkeit, verschiedene Aspekte der Hostinglösung zu isolieren und einzeln zu verwalten, ebenfalls eine robuste und attraktive Option sein.

Es gibt andere Hostingoptionen, die Sie mit Azure verwenden können, einschließlich Azure App Service.

Azure App Service

App Service ermöglicht Ihnen das Erstellen und Hosten von Web-Apps, Hintergrundaufträgen, mobilen Back-Ends und RESTful-APIs in der Programmiersprache Ihrer Wahl, ohne eine Infrastruktur verwalten zu müssen. Dieser Dienst bietet automatische Skalierung und hohe Verfügbarkeit. App Service unterstützt Windows und Linux. Der Dienst ermöglicht automatisierte Bereitstellungen über GitHub, Azure DevOps oder ein beliebiges Git-Repository zur Unterstützung eines Continuous Deployment-Modells.

Azure App Service ist eine robuste Hostingoption, mit der Sie Ihre Apps in Azure hosten können. Mit Azure App Service können Sie sich auf das Erstellen und Verwalten Ihrer App konzentrieren, während Azure die Ausführung der Umgebung sicherstellt.

Azure App Service ist ein HTTP-basierter Dienst zum Hosten von Webanwendungen, REST-APIs und mobilen Back-Ends. Er unterstützt verschiedene Programmiersprachen wie .NET, .NET Core, Java, Ruby, Node.js, PHP und Python. Außerdem unterstützt er Windows- und Linux-Umgebungen.

Typen von App-Diensten

Mit App Service können Sie die meisten App-Dienstformate hosten, einschließlich der folgenden:

- Web-Apps
- API-Apps
- WebJobs
- Mobile Apps

App Service übernimmt die meisten Infrastrukturentscheidungen, die Sie beim Hosting von Apps im Internet treffen:

- Funktionen zur Bereitstellung und Verwaltung sind in die Plattform integriert.
- Endpunkte können gesichert werden.
- Websites lassen sich schnell skalieren, um hohe Datenverkehrslasten zu bewältigen.
- Die integrierten Lastenausgleichs- und Traffic Manager-Funktionen ermöglichen Hochverfügbarkeit.

Alle diese App-Formate werden in derselben Infrastruktur gehostet und profitieren von diesen Vorteilen. Dank dieser Flexibilität wird App Service zur idealen Wahl für das Hosten von

weborientierten Anwendungen.

Web-Apps

App Service bietet vollständige Unterstützung für das Hosten von Web-Apps mit ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP oder Python. Sie können Windows oder Linux als Hostbetriebssystem wählen.

API-Apps

Ähnlich wie beim Hosten einer Website können Sie REST-basierte Web-APIs mit der Sprache und dem Framework Ihrer Wahl erstellen. Sie erhalten vollständige Swagger-Unterstützung sowie die Möglichkeit zum Packen und Veröffentlichen Ihrer API in Azure Marketplace. Die erstellten Apps können von jedem HTTP- bzw. HTTPS-basierten Client genutzt werden.

WebJobs

Mithilfe des WebJobs-Features können Sie ein Programm (EXE, Java, PHP, Python oder Node.js) oder ein Skript (CMD, BAT, PowerShell oder Bash) in demselben Kontext wie eine Web-App, API-App oder mobile App ausführen. Das Programm oder Skript kann geplant oder durch einen Trigger ausgeführt werden. WebJobs wird oft verwendet, um Hintergrundaufgaben im Rahmen Ihrer Anwendungslogik auszuführen.

Mobile Apps

Verwenden Sie das Mobile Apps-Feature von App Service zum schnellen Erstellen eines Back-Ends für iOS- und Android-Apps. Mit nur wenigen Aktionen im Azure-Portal können Sie folgende Aktionen ausführen:

- Speichern von Daten einer mobilen App in einer cloudbasierten SQL-Datenbank
- Authentifizieren Sie Kunden bei gängigen Social Media-Anbietern wie MSA, Google, X und Facebook.
- Senden von Pushbenachrichtigungen
- Ausführen von benutzerdefinierter Back-End-Logik in C# oder Node.js

Auf Seite der mobilen Apps gibt es SDK-Unterstützung für native iOS- und Android-, Xamarin- und React Native-Apps.

Beschreiben virtueller Azure-Netzwerke

100 XP

5 Minuten

Mit virtuellen Azure-Netzwerken und virtuellen Subnetzen können Azure-Ressourcen wie etwa VMs, Web-Apps und Datenbanken untereinander, mit Benutzer*innen im Internet sowie mit Ihren lokalen Clientcomputern kommunizieren. Stellen Sie sich ein Azure-Netzwerk als eine Erweiterung Ihres lokalen Netzwerks von Ressourcen vor, das andere Azure-Ressourcen miteinander verbindet.

Virtuelle Azure-Netzwerke bieten die folgenden wichtigen Netzwerkfunktionen:

- Isolation und Segmentierung
- Internetkommunikation
- Kommunikation zwischen Azure-Ressourcen
- Kommunikation mit lokalen Ressourcen
- Weiterleitung von Netzwerkdatenverkehr
- Filterung von Netzwerkdatenverkehr
- Verbindung virtueller Netzwerke

Virtuelle Azure-Netzwerke unterstützen sowohl öffentliche als auch private Endpunkte, um die Kommunikation zwischen externen oder internen Ressourcen mit anderen internen Ressourcen zu ermöglichen.

- Öffentliche Endpunkte haben eine öffentliche IP-Adresse, auf die von jedem Ort der Welt aus zugegriffen werden kann.
- Private Endpunkte sind in einem virtuellen Netzwerk enthalten und weisen eine private IP-Adresse im Adressraum des virtuellen Netzwerks auf.

Isolation und Segmentierung

Azure Virtual Network ermöglicht die Erstellung mehrerer isolierter virtueller Netzwerke. Wenn Sie ein virtuelles Netzwerk einrichten, definieren Sie einen privaten IP-Adressraum, indem Sie entweder öffentliche oder private IP-Adressbereiche verwenden. Der IP-Adressbereich ist nur innerhalb des virtuellen Netzwerks vorhanden und kann nicht über das Internet geroutet werden. Diesen IP-Adressraum können Sie dann in Subnetze aufteilen und den einzelnen benannten Subnetzen jeweils einen Teil des definierten Adressraums zuordnen.

Für die Namensauflösung können Sie den in Azure integrierten Dienst zur Namensauflösung verwenden. Ferner können Sie das virtuelle Netzwerk so konfigurieren, dass ein interner oder ein externer DNS-Server verwendet wird.

Internetkommunikation

Sie können eingehende Internetverbindungen zulassen, indem Sie einer Azure-Ressource eine öffentliche IP-Adresse zuweisen oder die VM hinter einem öffentlichen Lastenausgleich platzieren.

Kommunikation zwischen Azure-Ressourcen

Es empfiehlt sich, eine sichere Kommunikation zwischen Azure-Ressourcen zu ermöglichen. Dazu haben Sie zwei Möglichkeiten:

- Virtuelle Netzwerke können nicht nur eine Verbindung mit VMs herstellen, sondern auch mit anderen Azure-Ressourcen. Hierzu zählen beispielsweise die App Service-Umgebung für Power Apps, Azure Kubernetes Service und Azure-VM-Skalierungsgruppen.
- Mithilfe von Dienstendpunkten können Sie eine Verbindung mit anderen Azure-Ressourcentypen herstellen (beispielsweise mit Azure SQL-Datenbanken und Speicherkonten). Bei diesem Ansatz können Sie mehrere Azure-Ressourcen mit virtuellen Netzwerken verknüpfen, um die Sicherheit zu erhöhen und ein optimales Routing zwischen Ressourcen sicherzustellen.

Kommunikation mit lokalen Ressourcen

Virtuelle Azure-Netzwerke ermöglichen es Ihnen, Ressourcen in Ihrer lokalen Umgebung und in Ihrem Azure-Abonnement miteinander zu verknüpfen. So können Sie ein Netzwerk erstellen, das sowohl Ihre lokale Umgebung als auch Ihre Cloudumgebung abdeckt. Für diese Konnektivität stehen drei Mechanismen zur Verfügung:

- Point-to-Site-VPN-Verbindungen (Virtual Private Network) bestehen zwischen einem Computer außerhalb Ihrer Organisation zurück in das Unternehmensnetzwerk. In diesem Fall initiiert der Clientcomputer eine verschlüsselte VPN-Verbindung, um den Computer mit dem virtuellen Azure-Netzwerk zu verbinden.
- Site-to-Site-VPNs verbinden Ihr lokales VPN-Gerät oder -Gateway mit dem Azure-VPN-Gateway in einem virtuellen Netzwerk. Dadurch kann der Eindruck entstehen, dass sich die Geräte in Azure tatsächlich im lokalen Netzwerk befinden. Die Verbindung ist verschlüsselt und internetbasiert.
- Azure ExpressRoute bietet dedizierte private Konnektivität mit Azure ohne eine Datenübertragung über das Internet. ExpressRoute ist besonders für Umgebungen geeignet, in denen Sie eine höhere Bandbreite und ein noch höheres Maß an Sicherheit benötigen.

Weiterleitung von Netzwerkdatenverkehr

Azure leitet standardmäßig Datenverkehr zwischen Subnetzen in beliebigen verbundenen virtuellen Netzwerken, lokalen Netzwerken und dem Internet weiter. Sie können das Routing aber auch steuern und die Einstellungen wie folgt überschreiben:

- Mit Routingtabellen können Sie Regeln für die Weiterleitung von Datenverkehr definieren. Sie können benutzerdefinierte Routingtabellen erstellen, die steuern, wie Pakete zwischen Subnetzen weitergeleitet werden.
- Ein Border Gateway Protocol (BGP) kann für Azure-VPN-Gateways, Azure Route Server oder Azure ExpressRoute verwendet werden, um lokale BGP-Routen an virtuelle Azure-Netzwerke weiterzugeben.

Filterung von Netzwerkdatenverkehr

Mit virtuellen Azure-Netzwerken können Sie Datenverkehr zwischen Subnetzen wie folgt filtern:

- Netzwerksicherheitsgruppen sind Azure-Ressourcen, die mehrere Eingangs- und Ausgangssicherheitsregeln enthalten können. Sie können diese Regeln definieren, um Datenverkehr auf der Grundlage von Faktoren wie Quell- und Ziel-IP-Adresse, Port und Protokoll zuzulassen oder zu blockieren.

- Virtuelle Netzwerkgeräte sind spezielle VMs, die mit einem gehärteten Netzwerkgerät vergleichbar sind. Ein virtuelles Netzwerkgerät führt eine bestimmte Netzwerkfunktion aus (beispielsweise eine Firewall oder WAN-Optimierung).

Verbindung virtueller Netzwerke

Virtuelle Netzwerke können mittels Peering miteinander verknüpft werden. Peering ermöglicht eine direkte Verbindung zwischen zwei virtuellen Netzwerken. Der Netzwerkdatenverkehr zwischen Peernetzwerken ist privat und durchläuft das Microsoft-Backbone-Netzwerk, aber nie in das öffentliche Internet. Peering ermöglicht es Ressourcen in den einzelnen virtuellen Netzwerken, miteinander zu kommunizieren. Diese virtuellen Netzwerke können sich in separaten Regionen befinden. Mit diesem Feature können Sie ein globales, miteinander verbundenes Netzwerk über Azure erstellen.

Mit benutzerdefinierten Routen (User-Defined Route, UDR) können Sie die Routingtabellen zwischen Subnetzen innerhalb eines virtuellen Netzwerks oder zwischen virtuellen Netzwerken steuern. Dies ermöglicht eine bessere Kontrolle über den Netzwerkdatenverkehr.

Beschreiben von virtuellen privaten Netzwerken in Azure

100 XP

5 Minuten

Ein virtuelles privates Netzwerk (VPN) verwendet einen verschlüsselten Tunnel in einem anderen Netzwerk. VPNs werden in der Regel bereitgestellt, um zwei oder mehr vertrauenswürdige private Netzwerke über ein nicht vertrauenswürdiges Netzwerk (in der Regel das öffentliche Internet) miteinander zu verbinden. Der Datenverkehr wird bei der Übertragung über das nicht vertrauenswürdige Netzwerk verschlüsselt, um den Verlust von Daten oder andere Angriffe zu verhindern. VPNs können Netzwerken ermöglichen, vertrauliche Informationen sicher und geschützt zu teilen.

VPN-Gateways

Ein VPN-Gateway ist eine Art virtuelles Netzwerkgateway. Instanzen von Azure VPN Gateway werden in einem dedizierten Subnetz des virtuellen Netzwerks bereitgestellt und ermöglichen folgende Verbindungen:

- Verbinden von lokalen Rechenzentren mit virtuellen Netzwerken über eine Verbindung von Standort zu Standort (Site-to-Site-Verbindung).
- Verbinden von einzelnen Geräten mit virtuellen Netzwerken über eine Point-to-Site-Verbindung.
- Verbinden von virtuellen Netzwerken mit anderen virtuellen Netzwerken über eine Netzwerk-zu-Netzwerk-Verbindung.

Alle über das Internet übertragenen Daten werden in einem privaten Tunnel verschlüsselt. Sie können in jedem virtuellen Netzwerk nur ein VPN-Gateway bereitstellen. Sie können aber ein Gateway verwenden, um Verbindungen mit mehreren Standorten herzustellen, einschließlich anderer virtueller Netzwerke oder lokaler Rechenzentren.

Beim Einrichten eines VPN-Gateways müssen Sie den VPN-Typ angeben (richtlinienbasiert oder routenbasiert). Der primäre Unterschied zwischen diesen beiden Typen besteht darin, wie sie bestimmen, welcher Dat
Authentifizierungsmetho

- Richtlinienbasierte
  jeden Tunnel versch
  IP-Adressen aus, u
- Bei Verwendung vo
  Netzwerkschnittste
  IP-Routing (statisch
  welche dieser Tunn
  Routenbasierte VP
  stabiler gegenüber Topologieänderungen, wie etwa der Erstellung neuer Subnetze.

Routenbasiertes VPN-Gateway (Route-based VPN)
Wie funktioniert es?
Bei einem routenbasierten VPN-Gateway geht es darum, dass du Routen definierst, also festlegst, welche Netzwerke miteinander verbunden sind und wie der Verkehr zwischen diesen Netzwerken fließt. Es ist flexibler, weil du größere Netzwerke miteinander verbinden kannst und nicht nur einzelnen Verkehr.

Einfaches Beispiel:
Angenommen, Büro A hat ein gesamtes Netzwerk (z. B. das gesamte Büro mit mehreren Servern und Geräten), und Büro B hat ebenfalls ein Netzwerk. Bei einem routenbasierten VPN-Gateway legst du fest, dass der gesamte Verkehr zwischen Büro A und Büro B über das VPN-Gateway geht, ohne dass du für jede einzelne Verbindung eine Regel erstellen musst. Du definierst einfach eine Route: "Verkehr zu Netzwerk B soll über das VPN gehen."

Einsatzgebiet:
Routengestützte VPN-Gateways sind besser für komplexere Netzwerke geeignet, in denen mehrere Subnetze miteinander verbunden werden müssen. Sie bieten mehr Flexibilität und sind leichter zu verwalten, wenn es viele Verbindungen gibt.

Richtlinienbasiertes VPN-Gateway (Policy-based VPN)
Wie funktioniert es?
Bei einem richtlinienbasierten VPN-Gateway wird der Datenverkehr anhand von vordefinierten Regeln (Richtlinien) gefiltert und weitergeleitet. Jede Regel legt fest, welcher Verkehr von einem Netzwerk zu einem anderen gesendet wird. Du gibst zum Beispiel an, dass nur Verkehr zu einer bestimmten IP-Adresse (z. B. einer Serveradresse) durch das VPN geschickt wird.

Einfaches Beispiel:
Stell dir vor, du hast zwei Büros: Büro A und Büro B. Büro A hat einen Server, der nur für die Buchhaltungsabteilung von Büro B erreichbar sein soll. Bei einem richtlinienbasierten VPN-Gateway würdest du eine Regel einrichten, die nur den Verkehr zur IP-Adresse dieses Servers zulässt, aber den restlichen Verkehr blockiert.

Einsatzgebiet:
Diese Art von VPN wird oft für spezifische Verbindungen zwischen einzelnen Geräten oder Diensten verwendet, die genau festgelegt sind. Es ist weniger flexibel, aber sicherer für bestimmte, gezielte Anwendungen.

Verwenden Sie ein routenbasiertes VPN-Gateway, wenn Sie eine der folgenden Verbindungsarten benötigen:

- Verbindung zwischen virtuellen Netzwerken
- Point-to-Site-Verbindungen
- Verbindungen zwischen mehreren Standorten
- Nutzung parallel zu einem Azure ExpressRoute-Gateway

Eine Point-to-Site-Verbindung (P2S) ist eine Art von VPN-Verbindung, bei der einzelne Geräte (wie Laptops oder Desktops) von einem benutzerspezifischen Endgerät aus eine sichere Verbindung zu einem entfernten Netzwerk (z. B. zu einem Azure-Virtual-Network) herstellen.

Hochverfügbarkeitsszenarien

Wenn Sie ein VPN konfigurieren, um Ihre Informationen zu schützen, möchten Sie auch sicherstellen, dass die VPN-Konfiguration hoch verfügbar und fehlertolerant ist. Es gibt einige Möglichkeiten, die Resilienz Ihres VPN-Gateways zu maximieren.

Aktiv/Standby

Standardmäßig werden VPN-Gateways als zwei Instanzen in einer Aktiv/Standby-Konfiguration bereitgestellt, auch wenn nur eine VPN-Gatewayressource in Azure angezeigt wird. Wirkt sich eine geplante Wartung oder eine ungeplante Unterbrechung auf die aktive Instanz aus, wird die Verwaltung der Verbindungen automatisch ohne Benutzereingriff an die Standbyinstanz übergeben. Verbindungen werden während dieses Failovervorgangs unterbrochen, für eine geplante Wartung aber in der Regel innerhalb weniger Sekunden und für eine ungeplante Unterbrechung innerhalb von 90 Sekunden wiederhergestellt.

Aktiv/Aktiv

Durch die Einführung der Unterstützung des BGP-Routingprotokolls können Sie VPN-Gateways auch in einer Aktiv/Aktiv-Konfiguration bereitstellen. In dieser Konfiguration weisen Sie jeder Instanz eine eindeutige öffentliche IP-Adresse zu. Anschließend erstellen Sie getrennte Tunnel vom lokalen Gerät zu jeder IP-Adresse. Sie können die hohe Verfügbarkeit erweitern, indem Sie ein zusätzliches VPN-Gerät lokal bereitstellen.

ExpressRoute-Failover

Eine weitere Option für Hochverfügbarkeit besteht darin, ein VPN-Gateway als sicheren Failoverpfad für ExpressRoute-Verbindungen zu konfigurieren. ExpressRoute-Verbindungen sind von Haus aus resilient. Sie sind aber nicht immun gegen physische Probleme bei den Kabeln, über die Verbindungen hergestellt werden, oder gegen Ausfälle, die den gesamten ExpressRoute-Standort betreffen. In Szenarios mit Hochverfügbarkeit, bei denen das Risiko eines Ausfalls einer ExpressRoute-Verbindung besteht, können Sie auch ein VPN-Gateway bereitstellen, das das Internet als alternative Verbindungsmethode verwendet. So wird sichergestellt, dass immer eine Verbindung mit den virtuellen Netzwerken besteht.

Zonenredundante Gateways

VPN- und ExpressRoute-Gateways können in Regionen, die Verfügbarkeitszonen unterstützen, in einer zonenredundanten Konfiguration bereitgestellt werden. Diese Konfiguration bringt Resilienz, Skalierbarkeit und eine höhere Verfügbarkeit für die Gateways des virtuellen Netzwerks mit sich. Durch die Bereitstellung von Gateways in Azure-Verfügbarkeitszonen werden die Gateways innerhalb einer Region physisch und logisch getrennt. Gleichzeitig wird die Konnektivität Ihres lokalen Netzwerks mit Azure vor Ausfällen auf Zonenebene geschützt. Für diese Gateways sind verschiedene Gateway-SKUs (Stock Keeping Units) erforderlich, und es werden öffentliche Standard-IP-Adressen anstelle von öffentlichen Basic-IP-Adressen verwendet.

Beschreiben von Azure ExpressRoute

100 XP

4 Minuten

Mit Azure ExpressRoute können Sie Ihre lokalen Netzwerke über eine private Verbindung, die von einem Konnektivitätsanbieter bereitgestellt wird, auf die Cloud von Microsoft ausdehnen. Diese Verbindung wird als ExpressRoute-Leitung bezeichnet. Mit ExpressRoute können Sie Verbindungen mit Microsoft-Clouddiensten herstellen, z. B. Microsoft Azure und Microsoft 365. Mit diesem Feature können Sie Büros, Rechenzentren oder andere Einrichtungen mit der Microsoft-Cloud verbinden. Jeder Standort hätte dabei eine eigene ExpressRoute-Leitung.

Die Konnektivität kann über ein Any-to-Any-Netzwerk (IP VPN), ein Point-to-Point-Ethernet-Netzwerk oder eine virtuelle Querverbindung über einen Konnektivitätsanbieter in einer Co-Location-Einrichtung bereitgestellt werden. ExpressRoute-Verbindungen nutzen nicht das öffentliche Internet. Auf diese Weise können ExpressRoute-Verbindungen gleichmäßige Latenz sowie höhere Sicherheit, größere Zuverlässigkeit und schnellere Geschwindigkeit als herkömmliche Verbindungen über das Internet bieten.

Funktionen und Vorteile von ExpressRoute

Die Verwendung von ExpressRoute als Verbindungsdienst zwischen Azure und Ihren lokalen Netzwerken bietet mehrere Vorteile.

- Verbindung mit Microsoft-Clouddiensten in allen Regionen einer geopolitischen Region.
- Globale Konnektivität mit Microsoft-Diensten in allen Regionen mit ExpressRoute Global Reach
- Dynamisches Routing zwischen Ihrem Netzwerk und Microsoft über das Border Gateway Protocol (BGP)
- Integrierte Redundanz an jedem Peeringort, um eine höhere Zuverlässigkeit zu erzielen.

Verbindung mit Microsoft-Clouddiensten

Über ExpressRoute können Sie in allen Regionen auf die folgenden Dienste direkt zugreifen:

- Microsoft Office 365
- Microsoft Dynamics 365
- Azure Compute Services, wie z. B. Azure Virtual Machines
- Azure Cloud Services, wie z. B. Azure Cosmos DB und Azure Storage

Globale Konnektivität

Sie können ExpressRoute Global Reach zum Austausch von Daten zwischen Ihren lokalen Standorten aktivieren, indem Sie Ihre ExpressRoute-Leitungen verbinden. Angenommen, Sie haben ein Büro in Asien und ein Rechenzentrum in Europa, die beide über ExpressRoute-Leitungen mit dem Microsoft-Netzwerk verbunden sind. Sie können ExpressRoute Global Reach verwenden, um diese beiden Einrichtungen zu verbinden, sodass sie ohne Übertragung von Daten über das öffentliche Internet miteinander kommunizieren können.

Dynamisches Routing

****BGP (Border Gateway Protocol)** ist ein Routing-Protokoll, das dafür sorgt, dass Datenpakete den besten Weg zwischen verschiedenen Netzwerken finden. In Azure wird BGP vor allem in **Site-to-Site VPN-Verbindungen** und **ExpressRoute** verwendet, um automatisch **Routen** zwischen deinem lokalen Netzwerk und Azure zu verwalten. Anstatt dass du jede Route manuell festlegen musst, sorgt BGP dafür, dass das Azure-Gateway dynamisch die besten Verbindungen auswählt und den Verkehr effizient weiterleitet. BGP hilft auch dabei, **Fehlertoleranz** zu bieten, indem es den Datenverkehr bei Ausfällen auf alternative Pfade umleitet, ohne dass du manuell eingreifen musst.**

Bei ExpressRoute wird BGP verwendet. Mit BGP werden Routen zwischen lokalen Netzwerken und in Azure ausgeführten Ressourcen ausgetauscht. Dieses Protokoll ermöglicht ein dynamisches Routing zwischen Ihrem lokalen Netzwerk und Diensten, die in Microsoft Cloud ausgeführt werden.

Integrierte Redundanz

Sämtliche Konnektivitätsanbieter verwenden redundante Geräte, um die Hochverfügbarkeit der über Microsoft erstellten Verbindungen sicherzustellen. Zur Ergänzung dieser Funktion können Sie mehrere Leitungen konfigurieren.

ExpressRoute-Konnektivitätsmodelle

ExpressRoute unterstützt die folgenden vier Modelle, die Sie zum Herstellen einer Verbindung zwischen Ihrem lokalen Netzwerk und der Microsoft-Cloud verwenden können:

- CloudExchange-Housing
- Point-to-Point-Ethernet-Verbindung
- Any-to-Any-Verbindung
- Direkt von ExpressRoute-Standorten

Cloud-Exchange-Colocation

Zusammenstellung bezieht sich auf Ihr Rechenzentrum, Ihr Büro oder eine andere Einrichtung, die sich physisch an einem CloudExchange befinden, z. B. bei einem ISP. Wird Ihre Einrichtung beispielsweise über CloudExchange bereitgestellt, können Sie eine virtuelle Querverbindung mit der Microsoft-Cloud anfordern.

Point-to-Point-Ethernet-Verbindung

Point-to-Point-Ethernetverbindung bezieht sich auf die Verwendung einer Point-to-Point-Verbindung Ihrer Einrichtung mit der Microsoft-Cloud.

Any-to-Any-Netzwerke

Über eine Any-to-Any-Verbindung können Sie Ihr WAN in Azure integrieren, indem Sie Verbindungen mit Ihren Niederlassungen und Rechenzentren bereitstellen. Azure wird in Ihre WAN-Verbindung integriert, um eine Verbindung wie zwischen Ihrem Rechenzentrum und beliebigen Niederlassungen zu bieten.

Direkt von ExpressRoute-Standorten

Sie können sich direkt mit dem globalen Netzwerk von Microsoft verbinden, und zwar an strategisch über die ganze Welt verteilten Peeringstandorten. ExpressRoute Direct bietet duale Konnektivität mit 100 oder 10 GBit/s, die eine Aktiv/Aktiv-Konnektivität nach Maß unterstützt.

Sicherheitshinweise

Mit ExpressRoute werden Ihre Daten nicht über das öffentliche Internet übertragen, wodurch die mit der Internetkommunikation verbundenen Risiken reduziert werden. ExpressRoute ist eine private Verbindung zwischen Ihrer lokalen Infrastruktur und Ihrer Infrastruktur in Azure. Auch mit einer ExpressRoute-Verbindung werden DNS-Abfragen, Überprüfungen der Zertifikatssperrliste und Azure Content Delivery Network-Abfragen (CDN) weiterhin über das öffentliche Internet gesendet.

Beschreiben von Azure DNS

3 Minuten

100 XP

Azure DNS ist ein Hostingdienst für DNS-Domänen, der eine Namensauflösung mittels Microsoft Azure-Infrastruktur bietet. Durch das Hosten Ihrer Domänen in Azure können Sie Ihre DNS-Einträge mithilfe der gleichen Anmeldeinformationen, APIs, Tools und Abrechnung wie für die anderen Azure-Dienste verwalten.

Vorteile von Azure DNS

Azure DNS nutzt den Funktionsumfang und die Skalierung von Microsoft Azure, um zahlreiche Vorteile bereitzustellen, einschließlich:

- Zuverlässigkeit und Leistung
- Sicherheit
- Benutzerfreundlichkeit
- Benutzerdefinierbare virtuelle Netzwerke
- Aliaseinträge

Zuverlässigkeit und Leistung

DNS-Domänen in Azure DNS werden im globalen Azure-Netzwerk von Domänennamenservern gehostet und bieten Resilienz und Hochverfügbarkeit. Für Azure DNS werden Anycast-Netzwerke verwendet, sodass jede DNS-Abfrage jeweils vom am nächsten liegenden verfügbaren DNS-Server beantwortet wird. So erzielen Sie für Ihre Domäne sowohl eine hohe Geschwindigkeit als auch Hochverfügbarkeit.

Sicherheit

Azure DNS basiert auf Azure Resource Manager, wodurch beispielsweise folgende Features zur Verfügung stehen:

- Rollenbasierte Zugriffssteuerung in Azure (Azure RBAC), um zu steuern, wer Zugriff auf bestimmte Aktionen für Ihre Organisation hat
- Aktivitätsprotokolle, um nachzuverfolgen, wie ein Benutzer in Ihrer Organisation eine Ressource geändert hat, oder um im Rahmen der Problembehandlung Fehler zu finden.
- Ressourcensperre, um ein Abonnement, eine Ressourcengruppe oder eine Ressource zu sperren. Eine Sperre verhindert, dass andere Benutzer in Ihrer Organisation versehentlich wichtige Ressourcen löschen oder ändern.

Einfache Bedienung

Azure DNS kann DNS-Einträge für Ihre Azure-Dienste verwalten und außerdem DNS für Ihre externen Ressourcen bereitstellen. Azure DNS ist in das Azure-Portal integriert und verwendet die gleichen Anmeldeinformationen, den gleichen Supportvertrag und die gleiche Abrechnung wie Ihre anderen Azure-Dienste.

Da Azure DNS in Azure ausgeführt wird, können Sie Ihre Domänen und Datensätze über das Azure-Portal, mit Azure PowerShell-Cmdlets und der plattformübergreifenden Azure-Befehlszeilenschnittstelle verwalten. Anwendungen, die eine automatisierte DNS-Verwaltung erfordern, können über die REST-API und SDKs mit dem Dienst zusammenarbeiten.

Anpassbare virtuelle Netzwerke mit privaten Domänen

Azure DNS unterstützt auch private DNS-Domänen. Mit diesem Feature können Sie in Ihren privaten virtuellen Netzwerken anstelle der von Azure bereitgestellten Namen Ihre eigenen benutzerdefinierten Domänennamen verwenden.

Ein Azure Privater DNS ist ein Dienst, mit dem du DNS-Namen (z. B. meineapp.meinedomain.com) innerhalb eines Azure Virtual Networks verwalten kannst, ohne dass sie öffentlich zugänglich sind. Er wird verwendet, um internen Ressourcen wie VMs, Datenbanken oder anderen Diensten innerhalb von Azure eindeutige DNS-Namen zuzuweisen, damit sie sich einfach und sicher miteinander verbinden können.

Beispiel:
Angenommen, du hast eine Webanwendung in Azure, die eine Datenbank verwendet. Du kannst der Datenbank den DNS-Namen meinedatenbank.privat zuweisen. Innerhalb deines Azure Virtual Networks können dann alle VMs diesen Namen auflösen und die Datenbank erreichen, ohne dass der Name über das öffentliche Internet sichtbar ist.

Aliaseinträge

Azure DNS unterstützt auch Aliasdatensatzgruppen. Sie können einen Aliaseintragssatz verwenden, um auf eine Azure-Ressource zu verweisen, beispielsweise eine öffentliche Azure-IP-Adresse, ein Azure Traffic Manager-Profil oder einen Azure CDN-Endpunkt (Azure Content Delivery Network). Wenn sich die IP-Adresse der zugrunde liegenden Ressource ändert, wird der Aliasdatensatz während der DNS-Auflösung nahtlos automatisch aktualisiert. Der Aliasdatensatz verweist auf die Dienstinstanz, und der Dienstinstanz ist eine IP-Adresse zugeordnet.

> **Wichtig**
>
> Es ist nicht möglich, Azure DNS zum Erwerben eines Domänennamens zu verwenden. Ein Domänenname kann für eine Jahresgebühr über App Service-Domänen oder über die Domänennamen-Registrierungsstelle eines Drittanbieters erworben werden. Nach dem Erwerb können Ihre Domänen dann in Azure DNS für die Verwaltung von Einträgen gehostet werden.
