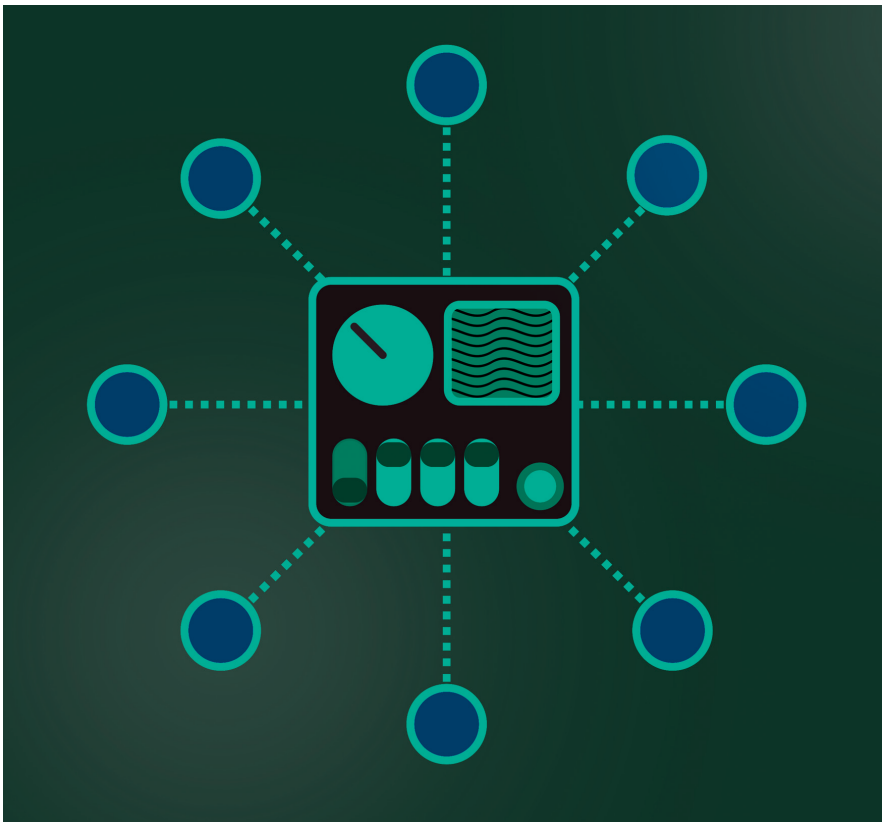
MULTICLOUD-VERWALTUNG

Verbindung nach draußen

Microsofts Dienst Azure Arc öffnet die Microsoft-Cloud für externe Anbieter.

Der Einsatz von Cloud-Diensten in einem Unternehmen setzt sich inzwischen immer mehr durch. Parallel dazu werden Cloud-Strategien immer populärer und gewinnen an Bedeutung. Unternehmen sehen konkret vielfältige Gründe, um sich eine Multicloud-Strategie zurechtzulegen. Allerdings steigt mit jedem weiteren Cloud-Anbieter, bei dem Dienste gebucht sind, die Komplexität im Management, in der Administration und im Aufwand für die Unternehmen.

Microsoft begegnet diesen Punkten, indem es die eigene Cloud für Produkte weiterer Cloud-Anbieter öffnet. Um diesen Ansatz zentral anbieten zu können, hat Microsoft den Dienst Azure Arc entwickelt. Dieser Service ist mittlerweile zu einem wichtigen Baustein geworden, um IT-Dienste unabhängig vom Standort oder dem gewählten IT-Backend über die Azure-Steuerungsebene (Control Plane) zu verwalten.



Azure Arc als zentrale Schnittstelle der Hybrid-Cloud

Microsoft hat die Vorabversion von Azure Arc im November 2019 auf der Microsoft-Konferenz Ignite vorgestellt, der Dienst ist noch relativ jung. Trotzdem hat er seitdem beachtlich an Bedeutung gewonnen und begründet mittlerweile eine eigene Produktfamilie, die sich vollständig auf Hybridlösungen konzentriert [1].

Der Grundstein für Azure Arc wurde aber bereits deutlich früher gelegt, mit Einführung des Azure Resource Manager (ARM) API. Dieses API hielt mit dem Ibiza-Portal (das aktuell bekannte Weblayout) Einzug. Es ist die zentrale Schnittstelle zwischen externen Anfragen, beispielsweise via Webportal, PowerShell und allen weiteren Zugriffswegen, und den internen Ressourcenanbietern, welche die Anforderungen entgegennehmen (Bild 1).

Mit Azure Arc besteht die Möglichkeit, diese zentrale Steuerung von Microsoft Azure auf alle Dienste außerhalb von Azure zu erweitern. Zu diesen Diensten zählen aktuell unter anderem:

- physische und virtuelle Server,
- Containerdienste (Kubernetes),
- Datenservices (zum Beispiel SQL Server).

Das Einbinden von Windows- und Linux-Servern geschieht dabei über die Installation eines Agenten. Die Installation kann sowohl manuell als auch automatisiert erfolgen. Die automatisierte Installation wird dabei empfohlen, da sich hierbei die notwendigen Parameter mit übergeben lassen. Das Werkzeug hierfür ist ein PowerShell-Skript in Verbindung mit einem MSI-Paket, das den Agenten enthält.

Das Skript wird schon vorkonfiguriert bereitgestellt. Dazu sind im Azure-Portal die notwendigen Informationen einzugeben, das Skript wird dann zur Installation bereitgestellt. Es enthält zum einen Angaben zum Download des aktuellen Agenten und der Installation; zum anderen übergibt es bei der Installation die notwendigen Parameter zum Tenant, zum Abonnement und zur Ressourcengruppe, um eine nahtlose Integration der gewählten VM ins Azure-Portal zu gewährleisten.

Sichere Kommunikation

Sobald die Installation abgeschlossen ist, registriert sich der Agent im vorgegebenen Tenant und der Arc-Verwaltungsinstanz. So wird bei der Installation die Auswahl zwischen *Public*, *Proxy* und *Private* angeboten.

Wie der Name vermuten lässt, erfolgt die Verbindung zwischen Agent und Azure-Arc-Instanz über vordefinierte öffentliche Endpunkte über Port 443. Die eingerichteten Endpunkte ermöglichen es, ausgehenden Datenverkehr über die Firewall auf die entsprechenden Endpunkte zu begrenzen.

Die Verbindung kann auch über einen Proxy laufen, wobei dies aktuell kaum eine Option ist, da derzeit nur HTTP-basierte, unauthentifizierte Proxys unterstützt werden.

Die dritte Option für private Endpunkte ermöglicht es, den kompletten Datenverkehr zwischen den Servern und Azure Arc ausschließlich über private Netzwerke zu erlauben [2]. Bei dieser Option müssen alle die für Arc vorgesehenen Server über das interne Netzwerk Azure Arc erreichen können. Dabei geht es dabei nur um die Kommunikation zwischen Server und Azure Arc – weitere Dienste, wie zum Beispiel Azure Monitor, werden über die bestehende Konnektivität genutzt.

Diese Optionen werden gleichermaßen für weitere unterstützte Szenarien, wie Kubernetes und Datenplattform, bereitgestellt.

Ein Agent, viele weitere Dienste

Da Azure Arc ständig weiterentwickelt wird, kommen quasi monatlich neue Funktionen für den Azure-Arc-Agenten dazu [3]. Daher ist es sinnvoll, die automatischen Updates für den Agenten zu aktivieren und darauf zu achten, dass dieser regelmäßig aktualisiert wird.

Die Verbindung des Servers über den Agenten mit dem ARM-API ermöglicht es, alle vorhandenen Azure-Dienste einzubinden, von denen bereits ein Großteil für die Integration bereit ist. Dies eröffnet spannende Möglichkeiten, wie zum Beispiel die Integration aller Azure-Arc-VMs in die Sicherheitsanwendung Microsoft Defender for Cloud und die enthaltene Threat-Intelligence-Lösung. In Verbindung mit der Installation des Log-Analytics-Agenten (Azure Monitor) wird der Server wie eine native Azure-VM behandelt und alle vorhandenen Sicherheitsempfehlungen und Anomalien werden durch Microsoft Defender for Cloud erkannt.

Zusätzlich ermöglicht die Arc-Integration die Aufnahme in Microsoft Sentinel des Cloud-SIEM-Systems von Microsoft. Dadurch werden die Windows-Server-Ereignisse in Echtzeit an Sentinel übermittelt und ausgewertet. Vorhandene Workbooks und vorkonfigurierte Abfragen lassen sich verwenden, um den Server-Status auszuwerten und bei Bedarf Maßnahmen zum Schutz der Infrastruktur zu ergreifen. Sentinel legt alle Daten im Log Analytics Workspace ab, in dem sich diese via KQL – der Abfragesprache der Log Analytics – ermitteln und auswerten lassen.

Eine weitere interessante Möglichkeit ist die Azure Policy in einer Gastkonfiguration. Azure Policy ist der zentrale Dienst innerhalb von Azure, um Compliance- und Sicherheitsanforderungen innerhalb des Tenant sicherzustellen und durchzusetzen. Da Azure Policy ein Teil des ARM-API ist, lässt sich dieser Dienst nutzen, um Richtlinien auf Servern durchzusetzen.

Solche Richtlinien gibt es für Linux- und Windows-Server. Damit ist das Durchsetzen von Serverrichtlinien auf Windows-Servern ohne Domänenzugehörigkeit möglich, und das kann die Serververwaltung in hybriden Cloud-Szenarien erheblich vereinfachen. Die Basis dieses Features ist Desired State Configuration (DSC) in der Version 3 auf PowerShell 7 und wird häufig in regulierten Umgebungen eingesetzt, um die Compliance-Anforderungen auf VMs (ohne Domänenzugehörigkeit) umzusetzen. Diese Funktionalität wird durch den Gast-Konfigurationsagenten bereitgestellt, der als Teil des Azure-Arc-Agenten mitgeliefert wird.

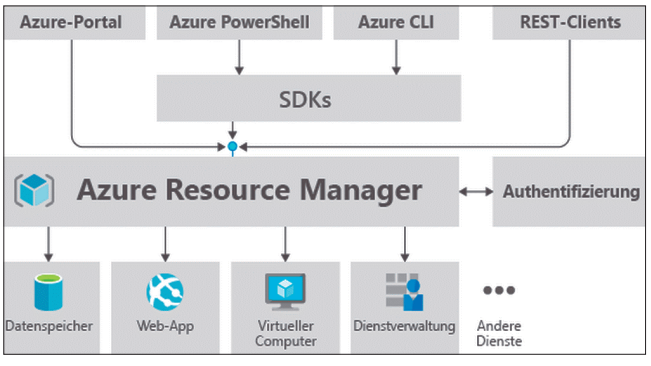
VMs automatisch verwalten

Wie erwähnt erweitert Azure Arc das ARM-API auf Ressourcen außerhalb von Azure. Dies bietet auch die Möglichkeit, vorhandene und neue Azure-Dienste auf Ressourcen außerhalb von Azure anzuwenden.

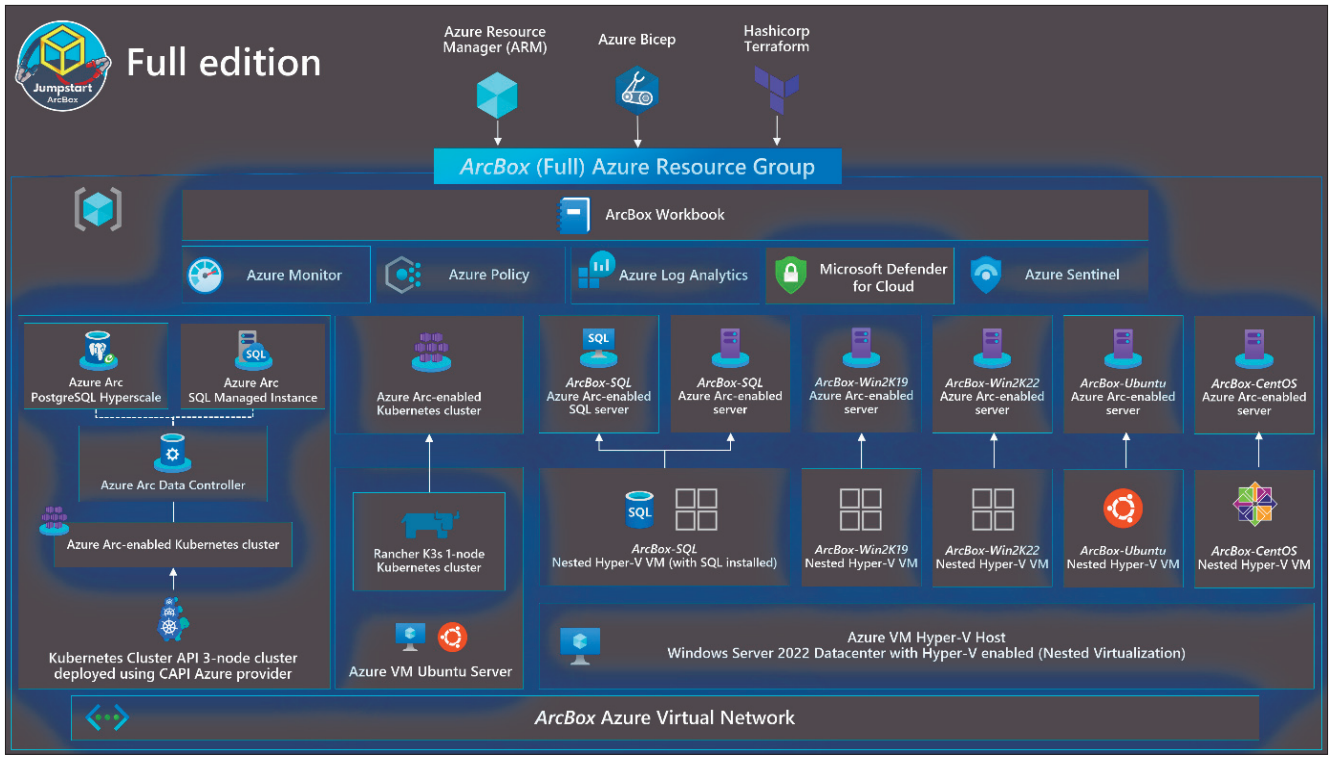
Ein spannendes Beispiel ist Azure Automanage, ein Dienst zum automatisierten Verwalten von VMs, der sich derzeit noch in der Phase einer öffentlichen Preview befindet. Azure Automanage ist ein Schritt, um Best Practices für Azure-VMs automatisiert durch die Verzahnung verschiedener Azure-Dienste über einen zentralen Dienst auf VMs umzusetzen. Dazu gehören unter anderem die Installation eines Monitor-Systems, die Integration in eine Update- und Antivirenverwaltung, eine Backup-Anwendung und vieles mehr. Mit Azure Arc besteht die Möglichkeit, Azure Automanage auf alle VMs anzuwenden, die über Azure Arc erreichbar sind und den Automanage-Dienst für alle VMs unabhängig von Azure verfügbar zu machen.

Container ohne Cloud betreiben

Für Entwickler bieten neben Serverless Computing nach wie vor Container optimale Möglichkeiten, um Applikationen auf Basis einer Mikroarchitektur zu entwickeln. Da Container sich schnell über DevOps-Pipelines in Betrieb nehmen lassen, bestehen optimale Möglichkeiten, Container in verschiedenen Cloud-Umgebungen einzurichten. Azure Arc ist hier ebenfalls ein hilfreicher Dienst, da die Containerverwaltung und -absicherung zentral über das Azure-ARM-API möglich ist, unabhängig davon, in welcher Umgebung die Container betrieben werden. Azure Arc unterstützt dabei jeden Kubernetes-Cluster, sofern dieser eine CNCF-Zertifizierung besitzt. ▶



Das Azure Resource Manager API ist die zentrale Schnittstelle (Bild 1)



Mit der ArcBox gibt es eine Blaupause, um eine Azure-Arc-fähige Lösung in einer dedizierten Subscription zu erstellen (Bild 2)

Jumpstart als Blueprint zum erfolgreichen Einsatz

Azure Arc ist quasi ein Schweizer Taschenmesser für die Hybrid-Cloud und es gibt etliche unterstützte Dienste und Integrationsmöglichkeiten, um Dienste in die Azure-Datenebene aufzunehmen. Um diesen vielen Möglichkeiten Rechnung zu tragen, hat Microsoft das Projekt Azure Arc Jumpstart ins Leben gerufen, das sich allen Möglichkeiten der Einrichtung und Konfiguration rund um Azure Arc widmet [4].

Etwas ungewöhnlich ist, dass es sich nicht in die bestehende Dokumentation der Microsoft Docs einreiht, sondern parallel unter einer eigenen Webadresse mit eigenem Layout erreichbar ist.

In diesem Jumpstart sind etliche Blueprints enthalten. Spannend an diesem Projekt ist die sogenannte ArcBox, eine komplette Blaupause, um eine Azure-Arc-fähige Lösung in einer dedizierten Subscription zu erstellen. Jumpstart bietet verschiedene „Geschmäcker" an, die nur bestimmte Azure-Arc-Dienste oder den kompletten Stack enthalten.

Fazit

Microsoft Azure Arc ist für Hybrid- und Multicloud-Projekte ein interessanter Ansatz, um das Azure-ARM-API unabhängig vom gewählten Cloud-Anbieter oder der vorhandenen Infrastruktur zu erweitern. Die Kompatibilität mit Windows- und Linux-Systemen deckt damit die üblichen Unternehmenssysteme ab und ermöglicht einen breiten Einsatz dieses Dienstes [5].

Die Integration in weitere Themen, wie Containertechnologien und Datenplattformen, und die ständige Weiterentwicklung ermöglichen es, für die komplette Infrastruktur eine Control Plane zu nutzen. Dadurch lässt sich die Komplexität deutlich reduzieren und über die Umgebung hinweg ein einheitliches Featureset integrieren.

Die Integration weiterer Dienste, wie zum Beispiel Azure Automanage, zeigt, welches Potenzial die Azure-Plattform in Verbindung mit Azure Arc bietet und dass auch in Zukunft sicher mit weiteren, spannenden Neuerungen zu rechnen ist. ■

[1] Julia White, Azure services now run anywhere with new hybrid capabilities: Announcing Azure Arc, www.dotnetpro.de/SL2209AzureArc1
[2] Use Azure Private Link to securely connect servers to Azure Arc, www.dotnetpro.de/SL2209AzureArc2
[3] Neuerungen im Agent für Azure Arc-fähige Server, www.dotnetpro.de/SL2209AzureArc3
[4] Azure Arc Jumpstart, www.dotnetpro.de/SL2209AzureArc4
[5] Azure Automanage for Machines Best Practices - Azure Arc-enabled servers, www.dotnetpro.de/SL2209AzureArc5

Gregor Reimling
arbeitet bei adesso SE als Managing Consultant und Cloud Solutions Architect für Azure. Er betreibt einen eigenen Azure-Blog, den Podcast „Cloud Inspires". Seit 2018 ist er mit dem MVP Award für Microsoft Azure ausgezeichnet und ist Microsoft Certified Trainer.

dnpCode A2209AzureArc