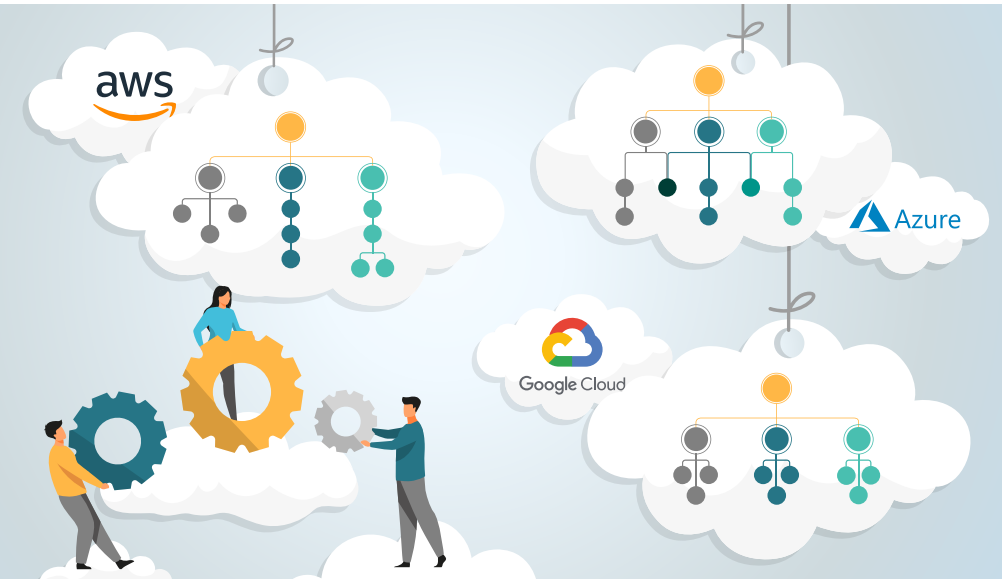


Organisationen in der Cloud

Teilen sich mehrere Beteiligte die Administration, gerät das Account- und Ressourcenmanagement für die Cloud zur organisatorischen Herausforderung. Zu deren Bewältigung bieten die großen Hyperscaler diverse Wege, Unternehmensstrukturen in ihren Plattformen abzubilden.

Von Christoph Puppe

Mit einzelnen Accounts fing es damals bei AWS an, aber heute sind kleine und große Firmen, Behörden und Konzerne in der Cloud. Und für diese braucht es andere Verwaltungsstrukturen als früher in der Legacy-Cloud. Die Verwaltung der Nutzer und daran angelehnt auch der Berechtigungen muss heute den Organisationsstrukturen der Kunden angemessen sein und diese möglichst exakt abbilden. Dieser Artikel sieht sich die Ansätze der drei Hyperscaler genauer an.

Am Anfang ist die Public Cloud

Bei Public Cloud denkt jeder zunächst an eine Webseite, über die man mit seiner Kreditkarte beliebige Mengen an Speicher, CPU und anderen Diensten mieten kann. Das funktioniert auch gut und verdrängt immer mehr die Legacy-IT, auch on Premises genannt. Wenn die Cloud-Nutzung aber nicht für das eigene Bastelprojekt oder die Firma mit nur einem Administrator sein soll, wird es schnell unübersichtlich.

Da jeder Mitarbeiter seinen eigenen Account beim Anbieter hat, ist es notwendig, diesen Accounts Berechtigungen für das eigene Projekt einzuräumen, möchte man gemeinsam an etwas arbeiten. Sobald Hunderte Administratoren für eine größere Firma Tausende Projekte und Hunderttausende Ressourcen verwalten müssen, ist dieses Modell komplett überfordert. Aber auch in KMU gefährdet das Chaos durch diese einzelnen Accounts die Sicherheit und behindert effektives Arbeiten.

Auch für die Firma ist es nicht zu überblicken, wer wo welche Accounts hat, was diese pro Monat kosten, welche Ressourcen eventuell gar nicht mehr benötigt werden und wo welche Sicherheitsmaßnahmen umgesetzt werden. Will etwa die Revision alle gemieteten Clouds auditieren, müssen alle Inhaber aller dieser Projekte den Accounts der Revisoren die Leseberechtigungen einräumen. Ständiges Monitoring, gemeinsame Ablage von Protokolldaten, Analyse der Kosten und so weiter sind zwar möglich, aber enden in einem wüsten Geflecht von Accounts und deren Berechtigungen. Selbst in den 90ern war es bei on Premises schon aufgeräumter. Hier zeigt sich, dass niemand aus der Geschichte lernt. Nur manche lernen, dass die meisten nicht lernen.

Nun versprechen die Hyperscaler, den Firmen einen Weg zu bieten, das Chaos zu bändigen und nach guter Verfügbarkeit auch gute Verwaltbarkeit zu ermöglichen.

Firmen wollen und müssen:

- alle Ressourcen im Blick haben, die Daten der Firma verarbeiten;
- alle Kosten sehen, die der Firma entstehen;
- Sicherheits-, Kosten- und Betriebsrichtlinien auf alle Ressourcen anwenden;
- Monitoring und Protokollierung über alle Ressourcen fahren;
- alle Ressourcen auditieren;
- alle berechtigten Accounts und deren Rollen und Gruppen einsehen, verändern und auditieren;
- alle neuen Anmietungen prüfen, bewerten und genehmigen.

Und das alles aus Abteilungen heraus, die mit den jeweiligen Projekten keine Verbindung haben. Das Personalwesen erstellt die Accounts, die Buchhaltung überwacht das Billing, die IT-Sicherheit führt Audits durch und gibt Veränderungen frei und die Administratoren verwalten die gesamte oder einen kleinen Teil der Cloud-Ressourcen. Das geht nur, wenn alle Ressourcen in einer gemeinsamen Verwaltung und Accounts von Mitarbeitern ein Teil dieser Verwaltung sind.

Azure

Microsoft hat den Anfang für diese Verwaltungsstrukturen, genannt Organisationen, gemacht, als sie mit Azure recht spät in den Markt eintraten. Ausgangs-

iX-TRACT

- Moderne Clouds müssen in der Ressourcenverwaltung die Organisationsstrukturen kleiner und großer Kunden abbilden können.
- Ein gemeinsames Account-Management für alle Cloud-Dienste eines Kunden ist von großem Vorteil für die Verwaltung und die Sicherheit.
- Alle drei großen Hyperscaler bieten Lösungen – mit teilweise sehr unterschiedlichen Ansätzen.

punkt waren die Erfahrungen aus dem Active Directory und der Verwaltung teilweise sehr großer Kunden. Somit ist bei allen Kunden, bei Microsoft Tenant (Mandant) genannt, immer ein Azure Active Directory (AAD) dabei. In den meisten Fällen ist dies eine Kopie des On-Premises AD und wird auch für die O365-Dienste genutzt. Wer möchte, kann aber auch ein eigenständiges AAD für die Azure-Umgebungen einsetzen.

Seit Kurzem hat Microsoft das AAD zusätzlich in die Entra-Produktfamilie eingegliedert, die die Verwaltung der Benutzer und technischen Accounts noch um ein CIEM (Cloud Infrastructure Entitlement Management) und eine Entra-ID für dezentrale Identitäten ergänzt. Hier der Hinweis, dass es nicht zu empfehlen ist, ein Single-Tier On-Premises AD für die Authentifizierung administrativer Benutzer einzusetzen. Nur Multi-Tier AD (beispielsweise mit Shadow oder Red Forrest) bietet eine halbwegs ausreichende Sicherheit. Administrative Benutzer als Cloud-Native ohne Synchronisation zum On-Premises AD mit MFA und am besten auch mit FIDO2 sind die Empfehlung.

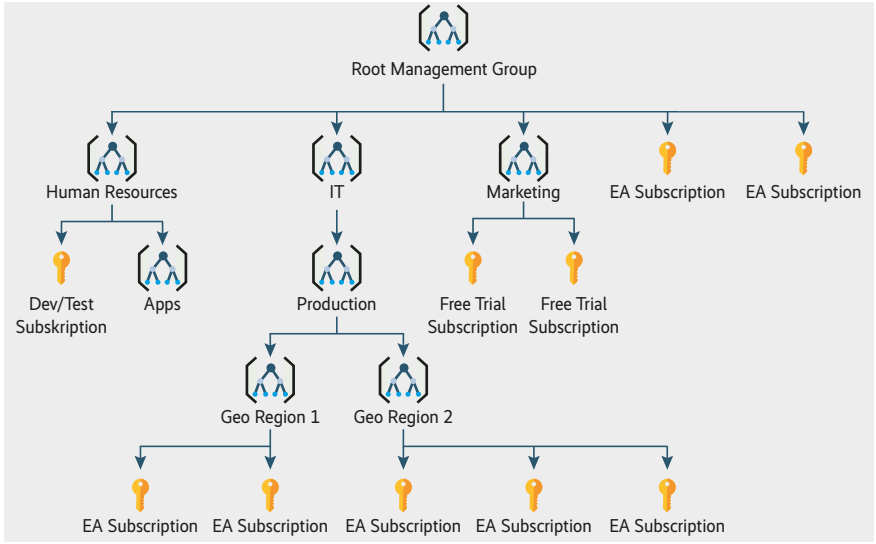
Auf dieser Basis lassen sich alle Berechtigungen in Azure und O365 vergeben. Es gibt Gruppen, Berechtigungen für Gruppen, Benutzer und technische Accounts und auch spezielle Accounts für Anwendungen und Dienste in Azure (Managed Identities). Das Regelwerk für Accounts und Berechtigungen im AAD und in Azure ist umfangreich und reicht von PAM (Priviledged Access Management) über Conditional Access (Zugang nach Regeln) bis zu den Standards wie MFA (Multi-Faktor-Authentifizierung). Auch ein dediziertes Modul zur Analyse der Anmeldevorgänge auf potenzielle Einbrüche ist enthalten. Wie alles heutzutage ist es ein Defender for Identity.

Wie Abbildung 1 zeigt, ist die Struktur einer Azure-Umgebung innerhalb eines Tenants als 1:n-Baum organisiert. Jede Ressource hat einen Parent und dieser kann viele Ressourcen enthalten. Das oberste Strukturelement ist dabei die Tenant Root Group. Diese Gruppe von Gruppen kann weitere Gruppen enthalten, hier als Management Groups (Verwaltungsgruppen) bezeichnet. Bis zu sechs Gruppenebenen sind möglich. So lassen sich Abteilungen, Fachbereiche, Niederlassungen und andere bereits in der Firma vorhandene Strukturen sehr einfach abbilden. Darunter kommen dann die Subscriptions. Diese bilden in einer Ebene die Verwaltungselemente für alle in Azure verfügbaren Arten von Ressourcen. Eine Subscription muss dabei immer Teil genau einer Management Group sein und kann selbst keine Subscriptions enthalten, sondern nur Ressourcen oder Resource Groups, die dann die Ressourcen enthalten. Eine Ressource befindet sich dabei immer in genau einer Subscription oder Resource Group.

Berechtigungen werden dabei auf jeder Ebene entweder direkt oder über Gruppen verwaltet. Azure kennt zudem eine Berechtigung, die nur die Vergabe von Berechtigungen ermöglicht. Eine Trennung von Berechtigungsmanagement und Administration ist damit sehr einfach möglich.

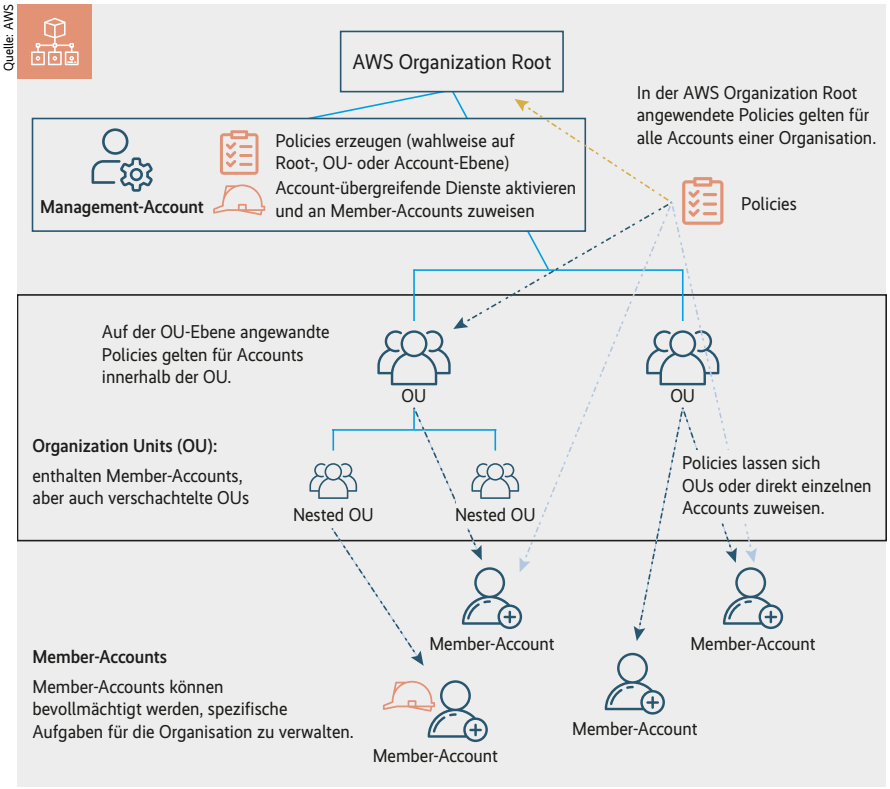
Richtlinien für die Ressourcen sind über die Management Groups oder auch

Quelle: Microsoft

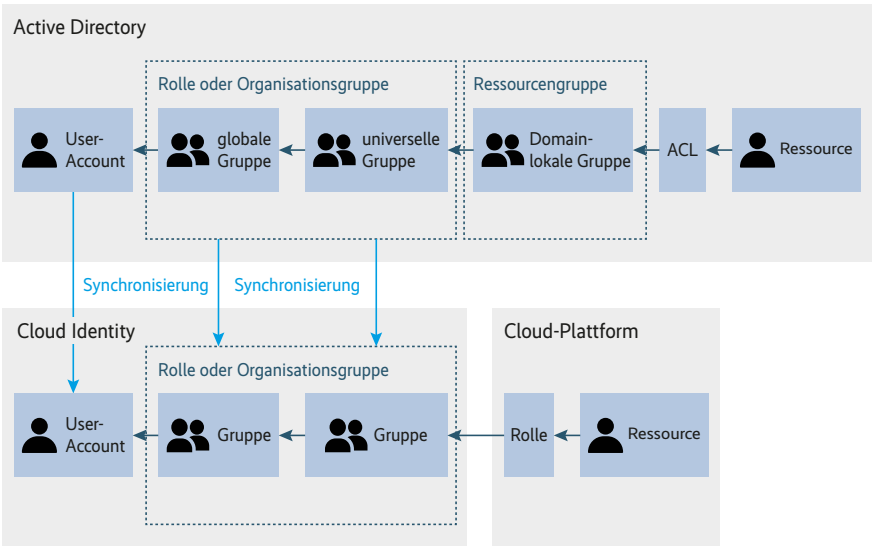


Mithilfe von Management Groups und Subscriptions (Abonnements) sowie Resource Groups lassen sich beliebig komplexe Organisationen in Azure nachbilden (Abb. 1).

Quelle: AWS



Organisationen in AWS sind eher eine Struktur für Multi-Account-Set-ups als eine eigenständige Ressource, die als Behälter für andere Ressourcen dient. Die Ressourcen kommen bei AWS über die Accounts in die Org (Abb. 2).



Quelle: Google

Bei GCP liegen die Accounts immer im Quellverzeichnis und werden nur in die Cloud Identity synchronisiert (Abb. 3).

Subscriptions oder einzelne Ressourcen zu vergeben. Wer bereits mit Group Policies (GPO) gearbeitet hat, wird sich hier schnell zurechtfinden. Es sind Regeln für alle Betriebsaspekte möglich, die bei Abweichungen entweder Berichte erstellen, sie automatisch korrigieren oder unerlaubte Einstellungen verhindern. Selbst Kubernetes und Multi-Cloud bei anderen Hyperscalern ist damit – ansatzweise – zu verwalten. Details dazu liefert der Artikel „Krähennest in der Wolke“ [1].

AWS

Auch AWS bietet seit 2017 Organisationen (Orgs) als Verwaltungselement an. Hier ist wie bei allen Hyperscalern ein erster Root-Account notwendig. Dieser richtet die Org ein und berechtigt die Benutzer, die dann die eigentliche Administration übernehmen. Der nächste Schritt besteht darin, die Policies für diese Org zu aktivieren. Warum diese nicht standardmäßig aktiv sind, ist nicht nachzuvollziehen, da fast jede Org so einfache Dinge wie Opt-out aus AI-Diensten, Backup, Service Control und Tag Policies benötigt. Nach dem Einrichten des Billing ist die Org einsatzbereit. Innerhalb der Org bilden Organizational Units (OU) die Untergruppen – wie Management Groups bei Azure und Folder bei GCP – die Abteilungen und anderen organisatorischen Einheiten des Kunden in der Cloud ab.

Beim Hinzufügen von Accounts für Benutzer und Administratoren unterscheidet sich AWS deutlich von GCP und Azure. AWS-Root-Accounts und reguläre AWS-Accounts sind der Org zugeordnet, es gibt also keinen Zwang zu einem eigenen Identity-Dienst und einer eigenen Domain. So lassen sich die Accounts schnell zusammenfassen sowie bereits vorhandene Strukturen, Ressourcen und Vertrauensstellungen mit in die neue Org überführen. Mit dem AWS Directory Service lässt sich auch das vorhandene On-Premises AD anbinden oder ein eigenes AD in der Cloud als Managed Service betreiben. Von diesem sind dann Vertrauensstellungen zur Org möglich. OU und Gruppen lassen sich für die Berechtigungsvergabe in der Org ebenfalls nutzen. Auch hier gilt die Empfehlung zur Entkopplung von AD für die Nutzer und Verwaltung der administrativen Benutzer.

Die Synchronisation ist bei AWS nicht so wichtig. Bei AWS gibt es kein O365 oder Google Workspace entsprechendes Angebot und daher benötigen die regulären Nutzer nur selten einen Zugang. Nur AWS-Root-Accounts und AWS-Accounts für Administratoren sind erforderlich.

Die Integration von Organisationen in AWS-Dienste ist bislang nicht vollständig abgeschlossen, da die Organisationen ein Multi-Account-Set-up vereinfachen sollen. Die Org ist daher auch nicht der Inhaber der Ressourcen wie bei anderen Hyperscalern. Eine Liste der Dienste, die mit allen Ressourcen aller Accounts in einer Org arbeiten können (Trusted Access) oder die in der Org technische Benutzer für die Administration anlegen können (Delegated Administrator), findet sich im User Guide (siehe ix.de/za45). Die wichtigsten Dienste zur Verwaltung sind dabei enthalten, viele andere fehlen allerdings. Hier zeigt sich deutlich, dass AWS die Organisationen erst nachträglich eingebaut hat. Dieser Punkt wie auch das Fehlen einer Übersicht über alle Ressourcen in allen Regionen und die Schwierigkeiten, Monitoring und Protokollierung über alle Regionen einzurichten, zeigen das Alter von AWS. Es war der Erste und ist Marktführer, aber Technical Debt und Legacy sind auch in der Cloud ein Thema. Es wäre vielleicht übertrieben, AWS als Legacy-Cloud zu bezeichnen, aber wer öfter mit allen Hyperscalern und auch den kleineren Anbietern wie IONOS, Hetzner, OVH und Telekom zu tun hat, merkt, dass auch ein Cloud-Dienst mit den Fehlern der Anfangsjahre zu kämpfen hat.

Auch bei den Policies und der Rechtevergabe über RBAC zeigt sich der nachträgliche Einbau und die teilweise fehlende Integration. Es lassen sich die Berechtigungen und Regelwerke an die Org, die OU und alle Ressourcen anhängen. Diese vererben sich dann auf die untergeordneten Einheiten. Die Service Control Policies sind allerdings in der Granularität und Flexibilität im Vergleich zu den anderen recht überschaubar. Wie auch Google verteilt AWS diese und andere Policies nicht nur als direkte Zuordnung, sondern auch per Tag an Org, OU und Ressourcen. Die Tagverwaltung ist dabei eine eigene Berechtigung, die nur sehr wenige Administratoren oder Tools haben dürfen.

Insgesamt machen damit die Verwaltung von Rechten und der Organisationen wie auch die Richtlinien den Eindruck, eine der Ursachen für die vergleichsweise hohe Zahl von Datenabflüssen und auch Fremdkontrolle über Cloud-Dienste der Kunden zu sein. Aber wie beschrieben ist der nachträgliche Einbau in eine solche Umgebung auch durch die Pflicht zur Abwärtskompatibilität mit den Legacy-Verfahren geprägt.

Google Cloud

Auch Googles Cloud-Plattform kennt Organisationen. Allerdings waren sie bis 2016 nicht an eine Cloud Identity geknüpft und nur ein Strukturelement etwa für die Abrechnung. Wer mehr braucht, muss zuerst einen hier Cloud Identity genannten Verzeichnisdienst erstellen und diesen mit einer Domain verbinden, die er kontrolliert. Das könnte cloud.firma.tld sein. Das Set-up ist relativ umständlich, aber sobald es fertig ist, wird eine Organisation als eigene Ressource erstellt. Die Cloud Identity hat dann entweder Accounts in der Form user@cloud.firma.tld oder sie wird gegen ein On-Premises AD authentisiert. Dann ist noch ein Billing-Account zu erstellen und es kann losgehen. Vorsicht: Wer das DNS dieser Domain kontrolliert, kann auch die Organi-

sation in GCP übernehmen. Auch hier gilt die Empfehlung, das AD für die Nutzer von dem für die Verwaltung der administrativen Benutzer zu entkoppeln.

Als Nächstes führt ein Agent durch den Aufbau der Organisation. Dabei wird von Abrechnung über Gruppen und Rollen, Netzwerk und Monitoring bis zur Sicherheit alles bedacht. Für jeden Schritt gibt es Best-Practice-Vorschläge, aus denen sich der Nutzer sich das Passende aussucht. Bereits ab der Einrichtung der Admin-Gruppen lässt sich die Arbeit auf die jeweiligen Experten aufteilen.

Etwas unverständlich sind die Nutzungsgrenzen für neue Accounts. Diese scheinen sehr klein gewählt. Eine Nutzung der neuen Umgebung ist erst nach dem Aufheben dieser Quotas möglich. Der Aufbau ist hier wie bei Azure an einen zentralen Inhaber des Mandanten geknüpft, der die Cloud Identity und damit die Organisation erstellt. Darunter befinden sich Folder, die den Management Groups in Azure entsprechen und 1:n verschachtelt sein können. Eine Ebene tiefer hängen die Projects, die die eigentlichen Ressourcen wie Netze, Dienste, Server und so weiter enthalten.

Berechtigungen lassen sich auch bei Google Cloud auf jeder Ebene vergeben. Allerdings gelten Richtlinien meist für die gesamte Organisation und sind nicht so feingranular wie bei Azure [1].

Fazit

Azure hat mit seinem Aufbau und der sehr konsequenten Umsetzung den Goldstandard für die Verwaltung im Kontext einer Organisation geschaffen, an dem sich die anderen Anbieter messen lassen müssen, aber dessen Eleganz sie derzeit nicht erreichen. Das begründet sich in der Geschichte. AWS und Google haben jeweils vor einigen Jahren angefangen, den Bedürfnissen der Großkunden Rechnung zu tragen. Beide haben jeweils Organisationen eingeführt und diese so gut es geht in die vorhandenen Strukturen zur Verwaltung von Ressourcen, Berechtigungen und Accounts eingebaut. Man merkt aber sehr deutlich, dass dies nachträglich geschah. Hätte Azure nicht gefühlt jeden Monat eine schwerwiegende Verwundbarkeit in der Verwaltungsschicht, wäre es aus Sicht der Sicherheitsorganisation klar in Führung. So wie es jetzt ist, kann man sich zwar an den komfortablen Verwaltungsfunktionen erfreuen und dies macht die tägliche Arbeit auch sehr viel einfacher, aber das Risiko einer erneuten schweren Verwundbarkeit wie OmiGod trübt das Bild. (avr@ix.de)

Quellen

[1] Christoph Puppe; Krähennest in der Wolke; Cloud Security Operations Center im Vergleich, iX 7/2021, S. 88

[2] Hintergrundinfos zu den Ansätzen der einzelnen Hyperscaler: ix.de/za45

CHRISTOPH PUPPE

ist Managing IT Security Architect und Auditteamleiter für ISO 27001 nach Grundschutz bei SVA System Vertrieb Alexander GmbH, Mitautor des Grundschutz-Kompendiums und ehemaliger Penetrationstester.