

bluechip

CREATING COMPUTERS.



Matthias Geburzi
Produktmanager Software bei
bluechip Computer AG



Notwendige Umstellung der Zugriffsrechte (DAP -> GDAP)

Referenten: Matthias Geburzi, Gunter Köhler

mgeburzi@bluechip.de

03448/755-287

[linkedin.com/in/matthias-geburzi](https://www.linkedin.com/in/matthias-geburzi)

Ab sofort anmelden!

>> Q1 2023 <<

Workshops, Schulungen und
Messen bei bluechip

Windows Server 2022

- Februar + März
- Externer Referent: Ben Bachl-Tanaka

Azure Stack HCI

- Januar + März
- Externer Referent: Carsten Rachfahl (MVP)

Microsoft Licensing Professional (MLP)

- Februar
- Externer Referent: Karlheinz Mack

Was ist GDAP im Partner Center?

GDAP steht für **G**ranular **D**elegated **A**dmin **P**rivileges

GDAP ist eine Sicherheitsfunktion, die Partnern den **Zugriff** nach dem **Zero-Trust**-Cybersicherheitsprotokoll mit den **geringsten Rechten** ermöglicht. Damit können Partner **granularen und zeitgebundenen Zugriff** auf die Workloads ihrer Kunden in Produktions- und Sandbox-Umgebungen konfigurieren. **Dieser am wenigsten privilegierte Zugriff muss Partnern von ihren Kunden explizit gewährt werden.**

Der Zugriff der Partner kann pro Kunde partitioniert werden. Mit GDAP haben Partner **standardmäßig nicht mehr Zugriff auf alle Kundenmandanten** in Azure-Abonnements über Administrator-Agents. Stattdessen sind Partner, die Azure verwalten, Teil einer separaten **Sicherheitsgruppe**, die Mitglied der Admin-Agent-Gruppe ist. Diese Gruppe gewährt dem Besitzer **rollenbasierten Zugriffsteuerungszugriff** (RBAC) für alle Azure-Abonnements für diesen Kunden.

Was ist GDAP im Partner Center?

- Partner, die Azure verwalten, erhalten **nicht mehr die globale Administratorrolle** auf dem Mandanten ihres Kunden, sondern standardmäßig niedrigere Berechtigungen zum Lesen eines Kundenverzeichnisses.
- Partner können granulare delegierte Administratorrechte (GDAP) **anfordern**, um einen detaillierteren und zeitgebundeneren Zugriff auf die Workloads ihrer Kunden zu erhalten. Eine detailliertere Kontrolle geht besser auf die Sicherheitsbedenken der Kunden ein.
- Partner müssen von DAP zu GDAP wechseln und können schließlich DAP (Global Admin) auf dem Mandanten des Kunden entfernen.



DAP (Delegated Administration Privileges)

- globale Administratorrolle
- ohne zeitliche Begrenzung

GDAP (Granular Delegated Admin Privileges)

- nicht mehr automatisch die globale Administratorrolle
- mit zeitlicher Begrenzung

Termine beachten

Bestehende Mandanten		Neue Mandanten	
VOR dem 17.01.23	AB dem 17.01.23	VOR dem 02.01.23	AB dem 02.01.23
Partner hat nach wie vor über DAP Zugriff	Partner hat KEINEN Zugriff mehr via DAP	Mandanten werden standardmäßig mit DAP angelegt	Mandanten werden standardmäßig mit GDAP angelegt
Aktion			
Starten Sie VOR dem 17.01.23 mit dem Prozess für GDAP – wenn möglich sofort	Es muss zunächst eine GDAP Genehmigungsanfrage über das Partner Center an den globalen Admin des Endkunden geschickt werden	Starten Sie VOR dem 17.01.23 mit dem Prozess für GDAP – wenn möglich sofort	Nicht erforderlich

Welche Funktionen verliert ein Partner, wenn DAP entfernt wird?

- Beendet Berechtigungen zum Verwalten von Funktionen auf dem Kundenmandanten
- Beendet die Möglichkeit, Supportanfragen für den Kunden zu erstellen
- Ein Upgrade eines Abonnements ist nicht mehr möglich
- Der [Bereitstellungsstatus des Abonnements](#) kann nicht abgerufen werden
- Partner verlieren die Möglichkeit, Azure-Abonnements über Partner Center zu verwalten (können das Azure-Abonnement jedoch über [Microsoft Azure](#) verwalten)

Häufig gestellte Fragen

Ersetzt GDAP DAP?

- Ja. Während des Übergangszeitraums werden DAP und GDAP koexistieren, wobei GDAP-Berechtigungen Vorrang vor DAP-Berechtigungen für Microsoft 365-, Dynamics 365- und Azure-Workloads haben.

Benötige ich GDAP, um Bestellungen für neue und bestehende Kunden im Partner Center auszuführen?

- Nein. Sie benötigen GDAP nicht, um Bestellungen für neue und bestehende Kunden auszuführen. Sie können weiterhin denselben Prozess verwenden, um Kundenaufträge im bluechip Cloud Kundencenter auszuführen.

Kann ich eine GDAP-Beziehung zu einem Kunden dauerhaft machen?

- Nein. Permanente GDAP-Beziehungen zu Kunden sind aus Sicherheitsgründen nicht möglich. Die maximale Dauer einer GDAP-Beziehung beträgt **zwei Jahre**.
- Sie können die [GDAP-Beziehungsanalysen](#) verwenden, um das Ablaufdatum von GDAP-Beziehungen nachzuverfolgen und sich auf ihre Verlängerung vorzubereiten.

Sind die vorhandenen Abonnements des Kunden betroffen, wenn eine GDAP-Beziehung abläuft?

- Nein. Es gibt keine Änderung an den vorhandenen Abonnements eines Kunden, wenn eine GDAP-Beziehung abläuft.

Häufig gestellte Fragen

Wenn ich mehrere Kunden habe, benötige ich dann mehrere Sicherheitsgruppen für diese Kunden?

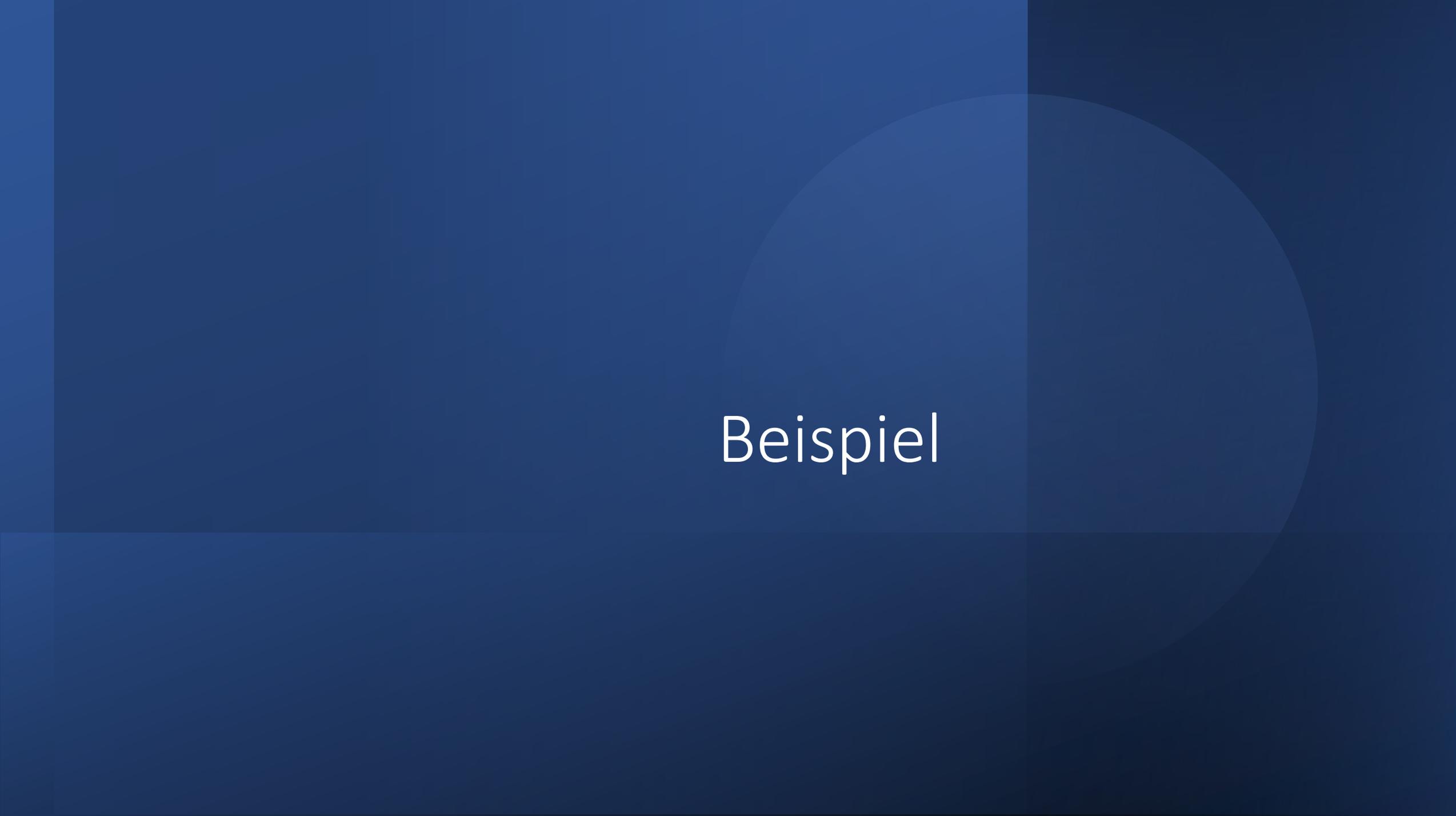
- Wenn Sie möchten, dass Ihre Partnerbenutzer alle Kunden verwalten können, können Sie alle Partnerbenutzer in einer Sicherheitsgruppe platzieren, und diese Gruppe kann alle Ihre Kunden verwalten.
- Wenn Sie möchten, dass verschiedene Partnerbenutzer verschiedene Kunden verwalten, weisen Sie diese Partnerbenutzer separaten Sicherheitsgruppen zur Kundenisolierung zu.

Wie funktioniert GDAP mit Microsoft 365 Lighthouse?

- Entweder granulare delegierte Administratorrechte (GDAP) plus eine indirekte Reseller-Beziehung oder eine delegierte Administratorrechte-Beziehung (DAP) sind erforderlich, um Kunden an Lighthouse zu binden.

Planung

- Wer ist in meiner Unternehmung betroffen?
- Welche **Rollen** und **Sicherheitsgruppen** werden benötigt (ggf. in Rücksprache mit den Kunden festlegen)?
- Sicherheitsgruppen und deren Mitglieder im M365 Admin Center anlegen
- GDAP Prozess starten



Beispiel

Checkliste

Partner

- Login im [MS Partner Center](#), wo Sie als CSP indirekt Reseller Ihre Kunden verwalten.
- Wählen Sie den Kunden aus und gehen Sie zum Punkt „Administratorbeziehungen“.
- Dort könnten Sie beim Endkunden eine neue Admin Beziehung anfordern.
- Wählen sie einen Namen und die entsprechenden Zugriffsrechte aus, die Sie anfordern möchten.
- Schicken Sie die Anforderung anschließend an den globalen Admin des Endkunden.
- Sie erhalten eine Mail, wenn der Endkunde die Anforderung bestätigt hat.
- Die ausgewählte Sicherheitsgruppe mit den damit verbundenen Admin-Rechten sollte nun zunächst als ausstehend, später als aktiv angezeigt werden.
- Es bestehen nun GDAP Rechte.
- Entfernen Sie ggf. bestehende DAP-Rechte.

Endkunde

- Kunde bestätigt Anfrage.

FAQ

- [GDAP-Rollenleitfaden](#)
- [Workloads, die von granularen delegierten Administratorrechten \(GDAP\) unterstützt werden](#)
- [Granulare Administratorberechtigungen zum Verwalten des Kundendienstes eines Kunden erhalten](#)
- [Kundengenehmigung der GDAP-Anfrage des Partners](#)
- [Erteilen granularer Berechtigungen für Sicherheitsgruppen](#)
- [Häufig gestellte Fragen zu GDAP](#)



Fragen