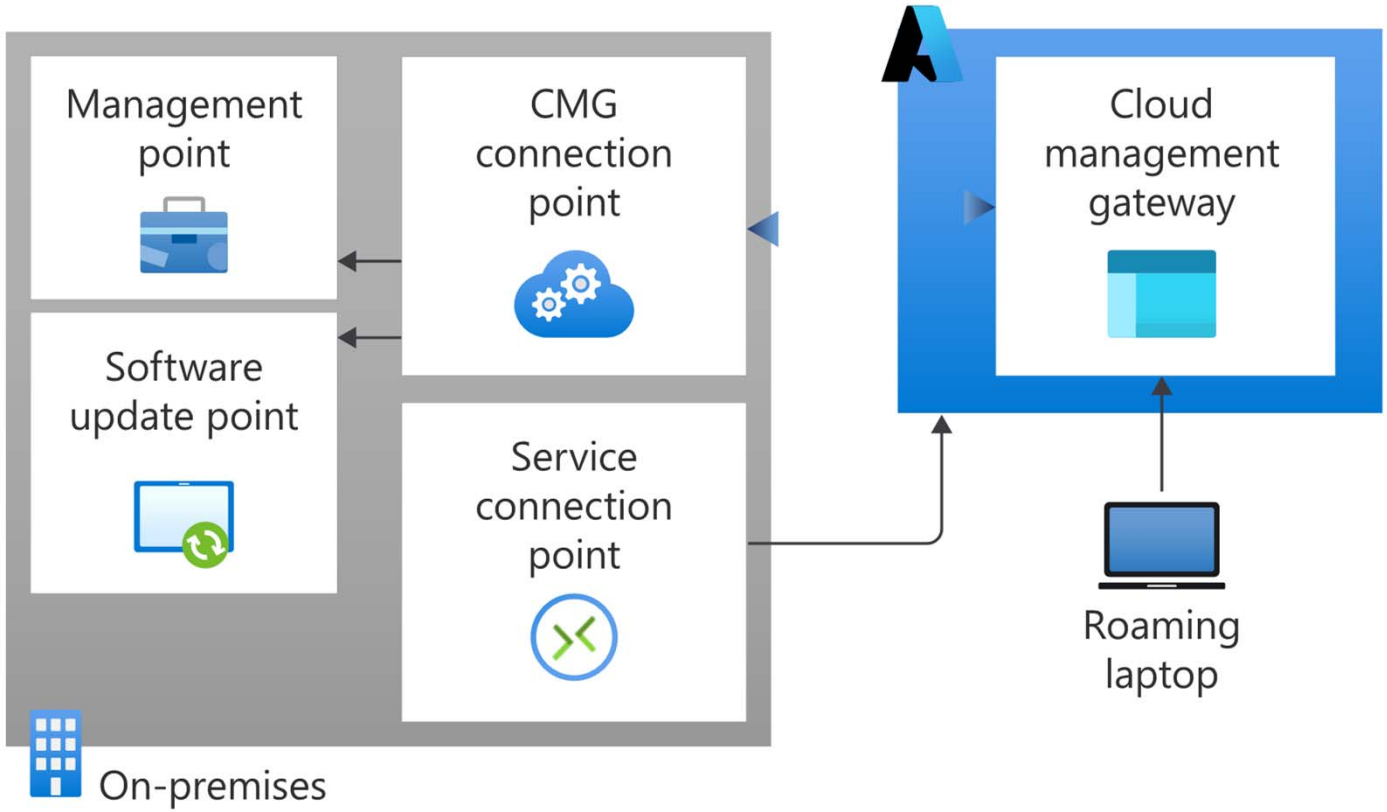
Microsoft Endpoint Manager: Leitfaden zu (Microsoft Endpoint Configuration Manager) MECM und Microsoft Intune - Teil 4

Cloud Management Gateway mit Microsoft Endpoint Configuration Manager (MECM)

Cloud Management Gateway



Quelle: https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/overview

Cloud Management Gateway - Checklist

- Komponenten und Anforderungen
  - Beachten der Systemanforderungen und notwendigen Anforderungen
- Entwurf der Hierarchie
  - Planen wo das CMG in Ihrer Umgebung platziert werden soll.
- Client-Authentifizierung
  - Festlegen welche Authentifizierungsmethode für Clients aus potenziell nicht vertrauenswürdigen Netzwerken verwendet werden soll.

Cloud Management Gateway - Checklist

- Unterstützte Konfigurationen
  - Verstehen welche Configuration Manager-Funktionen auf internetbasierten Clients unterstützt werden, die sich mit dem CMG verbinden.
- Leistung und Skalierung
  - Entscheiden wie viele Instancen (VM Scale Set) Sie benötigen, um die Anzahl Ihrer Clients optimal zu unterstützen.
- Kosten
  - Verstehen der Kosten für die Azure-basierten Komponenten.

Cloud Management Gateway - Komponenten

- Der **CMG-Cloud-Service** in Azure authentifiziert und leitet Configuration Manager-Client-Anfragen über das Internet an den CMG-Verbindungspunkt vor Ort weiter.
- Die **CMG Connection Point** Site System-Rolle ermöglicht Verbindung vom lokalen Netzwerk zum CMG-Dienst in Azure. Der CP veröffentlicht auch Einstellungen für den CMG, einschliesslich Verbindungsinformationen und Sicherheitseinstellungen. Der CMG-Connection Point leitet Client-Anforderungen vom CMG an lokale Rollen gemäss URL-Zuordnungen weiter. Zum Beispiel an den Management Pont und den Software Update Point.

Cloud Management Gateway - Komponenten

- Die Site System Role **Service Connection Point** Site führt die Komponente Cloud Service Manager aus, die alle CMG-Bereitstellungsaufgaben übernimmt. Ausserdem überwacht und meldet sie den Zustand des Dienstes und protokolliert Informationen aus Azure Active Directory (Azure AD).
- Der Management Point und Software Update Point bedienen Client-Anfragen wie üblich.
- Das CMG verwendet einen zertifikatbasierten HTTPS-Webdienst, um die Netzwerkkommunikation mit Clients zu sichern.

Cloud Management Gateway - Design

- Unabhängig davon, ob Sie eine Central Administration Site (CAS), eine eigenständige primary Site oder ein kleines Testlabor haben, planen Sie das Cloud Management Gateway (CMG) für diese Umgebung.
- Erstellen Sie die CMG an der obersten Site Ihrer Hierarchie. Wenn dies ein CAS ist, erstellen Sie CMG-Connection Points an untergeordneten primary Sites.
- Sie können mehrere CMG-Dienste in Azure erstellen und mehrere CMG-Connection Points erstellen. Mehrere CMG-Connection Points sorgen für einen Lastausgleich des Client-Datenverkehrs von der CMG zu den lokalen Rollen.

Cloud Management Gateway - Design

- Beispiel 1: Standalone Primary Site
  - Contoso verfügt über eine Standalone Primary Site in einem lokalen Rechenzentrum an seinem Hauptsitz in New York City.
    - Sie erstellen eine CMG in der Azure-Region East US, um die Netzwerklatenz zu verringern.
    - Es werden zwei CMG-Verbindungspunkte eingerichtet, die beide mit dem einzelnen CMG-Dienst verbunden sind.
  - Wenn sich Clients im Internet bewegen, kommunizieren sie mit der CMG in der Azure-Region East US. Die CMG leitet diese Kommunikation über die beiden CMG-Verbindungspunkte weiter.

Cloud Management Gateway - Design

- Beispiel 2: Hierarchy
  - Fourth Coffee hat ein CAS in einem lokalen Rechenzentrum am Hauptsitz in Seattle. Eine primary Site befindet sich im selben Rechenzentrum und die andere primary Site befindet sich in der europäischen Hauptniederlassung in Paris.
    - Auf dem CAS wird ein CMG-Service in der Azure-Region West US eingerichtet. Sie skalieren die Anzahl der VMs entsprechend der erwarteten Last der Roaming-Clients in der gesamten Hierarchie.
    - Am primären Standort in Seattle wird ein CMG-Connection Point eingerichtet, der mit der einzelnen CMG verbunden ist.
    - Am primären Standort in Paris wird ein CMG-Connection Point eingerichtet, der mit dem einzigen CMG verbunden ist.
  - Wenn sich die Clients im Internet bewegen, kommunizieren sie mit der CMG in der Azure-Region West US. Die CMG leitet diese Kommunikation an den CMG-Connection Point an der zugewiesenen primary Site des Clients weiter.

Tip: Sie müssen nicht mehr als ein CMG für die Zwecke der Geolokalisierung bereitstellen. Der Configuration Manager-Client ist von der geringen Latenz, die beim Cloud-Service auftreten kann, weitgehend unbeeinflusst, selbst wenn er geografisch weit entfernt ist.

Cloud Management Gateway - Client-Authentifizierung

- Clients, die eine Verbindung zu einem Cloud-Management-Gateway (CMG) herstellen, befinden sich potenziell im nicht vertrauenswürdigen öffentlichen Internet. Aufgrund der Herkunft des Clients bestehen höhere Anforderungen an die Authentifizierung. Es gibt drei Optionen für die Identität und Authentifizierung bei einem CMG:
    - Azure AD
    - PKI certificates
    - Configuration Manager site-issued tokens

Cloud Management Gateway - Client-Authentifizierung

	Azure AD	PKI certificate	Site token
ConfigMgr version	All supported	All supported	All supported
Windows client version	Windows 10 or later	All supported	All supported
Scenario support	User and device	Device-only	Device-only
Management point	E-HTTP or HTTPS	E-HTTP or HTTPS	E-HTTP or HTTPS

- Azure AD
  - Wenn Ihre internetbasierten Geräte unter Windows 10 oder höher laufen, sollten Sie die moderne Azure AD-Authentifizierung mit der CMG verwenden. Diese Authentifizierungsmethode ist die einzige, die benutzerzentrierte Szenarien ermöglicht. Zum Beispiel die Bereitstellung von Apps für eine Benutzersammlung.

Quelle: https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/plan-client-authentication

Cloud Management Gateway - Client-Authentifizierung

	Azure AD	PKI certificate	Site token
ConfigMgr version	All supported	All supported	All supported
Windows client version	Windows 10 or later	All supported	All supported
Scenario support	User and device	Device-only	Device-only
Management point	E-HTTP or HTTPS	E-HTTP or HTTPS	E-HTTP or HTTPS

- PKI Certificate
  - Wenn Sie über eine Public-Key-Infrastruktur (PKI) verfügen, die Client-Authentifizierungszertifikate für Geräte ausstellen kann, sollten Sie diese Authentifizierungsmethode für internetbasierte Geräte mit Ihrem CMG in Betracht ziehen. Sie unterstützt keine benutzerzentrierten Szenarien, dafür aber Geräte, auf denen jede unterstützte Version von Windows läuft.

Quelle: https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/plan-client-authentication

Cloud Management Gateway - Client-Authentifizierung

	Azure AD	PKI certificate	Site token
ConfigMgr version	All supported	All supported	All supported
Windows client version	Windows 10 or later	All supported	All supported
Scenario support	User and device	Device-only	Device-only
Management point	E-HTTP or HTTPS	E-HTTP or HTTPS	E-HTTP or HTTPS

- Site token
  - Wenn Sie Geräte nicht mit Azure AD verbinden oder PKI-Client-Authentifizierungszertifikate verwenden können, verwenden Sie die Token-basierte Authentifizierung von Configuration Manager. Vom Standort ausgestellte Client-Authentifizierungstoken funktionieren mit allen unterstützten Client-Betriebssystemversionen, unterstützen aber nur Geräteszenarien.

Quelle: https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/plan-client-authentication

Cloud Management Gateway - Konfigurationen

- Die unterstützten Konfigurationen sind perfekt auf der folgenden Website beschrieben:
- https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/supported-configurations

Cloud Management Gateway - Leistung/Skalierung

- Leistung und Skalierung des CMG:
  - Sie können mehrere Instanzen des Cloud Management Gateways (CMG) an primären Standorten oder am zentralen Verwaltungsstandort (CAS) installieren.
  - Ein CMG unterstützt bis zu 16 Instanzen virtueller Maschinen (VM) im Azure-Cloud-Service.
  - Die gleichzeitigen Client-Verbindungen pro CMG-VM-Instanz hängen vom Bereitstellungsmodell und der VM-Größe ab:
    - Cloud-Dienst (klassisch): 6.000
    - Virtual Machine Scale Set: (Version 2010 und 2103 für Cloud Service Provider (CSP)-Abonnements): 2,000
    - Virtual Machine Scale Set: (Version 2107 oder höher)
      - Labor (B2s): 10 (Die VM der Größe Lab (B2s) ist nur für Labortests und kleine Proof-of-Concept-Umgebungen gedacht.
      - Standard (A2_v2): 6.000
      - Groß (A4_v2): 10.000

Cloud Management Gateway - Leistung/Skalierung

- Leistung und Skalierung des CMG Connection Point:
  - Sie können mehrere Instanzen des CMG-Connection Points an primären Standorten installieren.
  - Ein CMG-Connection Point kann einen CMG mit bis zu vier VM-Instanzen unterstützen. Wenn der CMG mehr als vier VM-Instanzen hat, fügen Sie einen zweiten CMG-Connection Point für den Lastausgleich hinzu. Ein CMG mit 16 VM-Instanzen sollte mit vier CMG-Connection Points verbunden werden.

Cloud Management Gateway – Leistung verbessern

- Die folgenden Empfehlungen können Ihnen helfen, die CMG-Leistung zu verbessern:
    - Die Verbindung zwischen dem Configuration Manager-Client und dem CMG ist nicht regionsabhängig. Die Client-Kommunikation ist weitgehend unabhängig von Latenzzeiten und geografischen Abständen. Es ist in der Regel nicht erforderlich, mehrere CMG für die Zwecke der geografischen Nähe einzusetzen. Stellen Sie das CMG am obersten Standort in Ihrer Hierarchie bereit. Um die Skalierung zu erhöhen, fügen Sie VM-Instanzen hinzu.
    - Um eine hohe Verfügbarkeit des Services zu gewährleisten, erstellen Sie eine CMG mit mindestens zwei VM-Instanzen und zwei CMG-Connection Points pro Standort.
    - Skalieren Sie die CMG, um mehr Clients zu unterstützen, indem Sie weitere VM-Instanzen hinzufügen. Der Azure Load Balancer steuert die Client-Verbindungen zum Service.
    - Erstellen Sie weitere CMG-Connection Points, um die Last auf sie zu verteilen. Der CMG verteilt den Datenverkehr nach dem Round-Robin-Prinzip auf seine CMG-Connection Points.

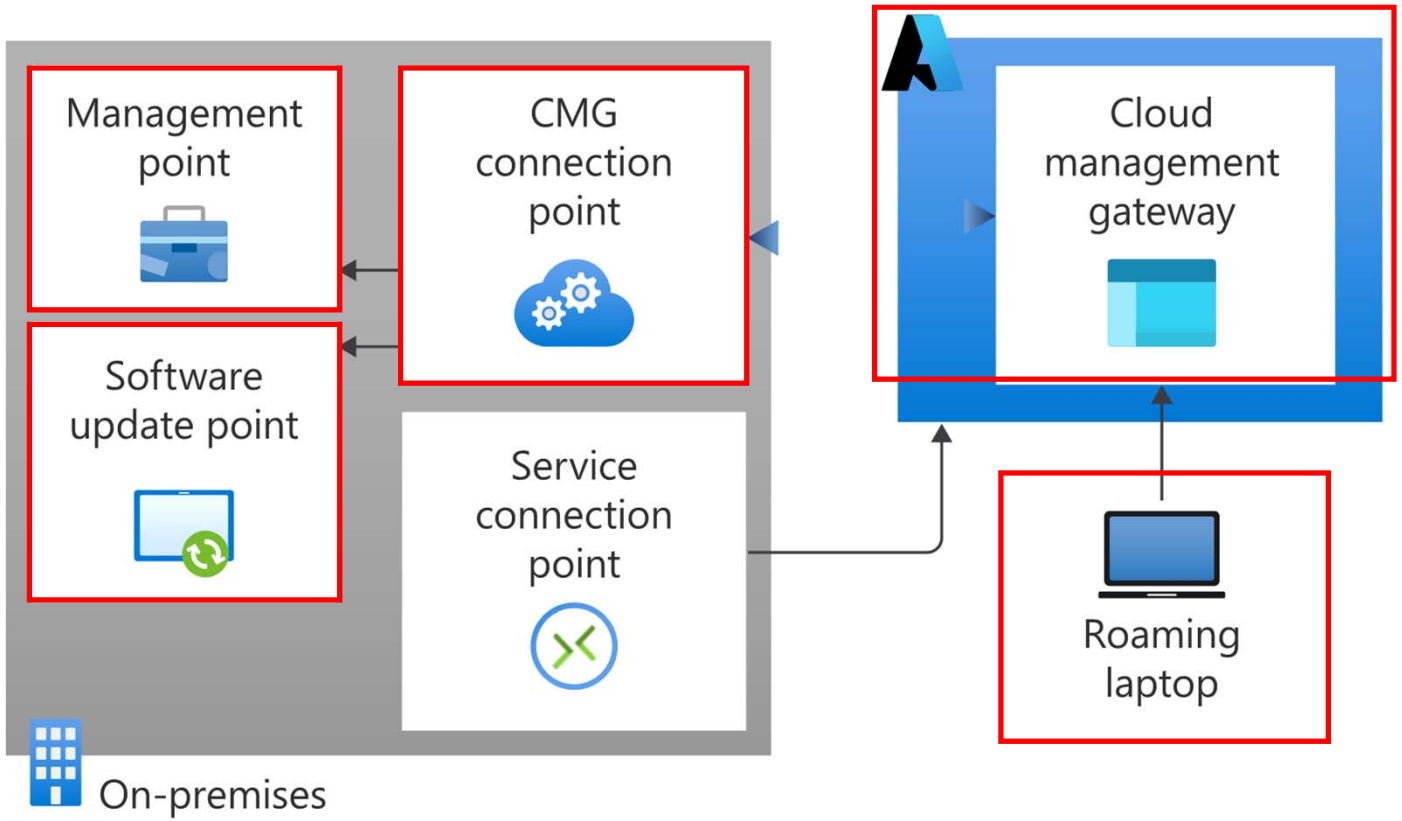
Cloud Management Gateway – Kosten

- Der Cloud Management Gateway (CMG) in Configuration Manager verwendet mehrere Komponenten in Microsoft Azure. Für diese Komponenten fallen Gebühren für das Azure-Abonnementkonto an. Einige Kosten sind fest, andere variieren je nach Nutzung.
- CMG nutzt Azure Platform as a Service (PaaS), das virtuelle Maschinen (VMs) verwendet. Für diese VMs fallen Rechenkosten an. Der spezifische Typ, der bei der Kostenschätzung zu verwenden ist, hängt davon ab, welche Bereitstellungsmethode Sie verwenden.
- Die Gebühren basieren auf den Daten, die aus Azure herausfliessen, was auch als Egress oder Download bezeichnet wird.
- Der CMG-Datenfluss aus Azure umfasst Richtlinien für den Client, Cleintbenachrichtigungen und Clientantworten, die der CMG an den Standort weiterleitet. Zu diesen Antworten gehören Bestandsberichte, Statusmeldungen und der Konformitätsstatus.
- Auch wenn keine Clients mit einem CMG kommunizieren, verursacht eine gewisse Hintergrundkommunikation Netzwerkverkehr zwischen dem CMG und dem lokalen Standort.
- Die ausgehende Datenübertragung (GB) wird in der Configuration Manager-Konsole angezeigt.

Cloud Management Gateway – Kosten

- Internetbasierte Clients erhalten Microsoft-Software-Update-Inhalte von Windows Update kostenlos. Verteilen Sie keine Update-Pakete mit Microsoft-Update-Inhalten an eine inhaltsaktivierte CMG.
- Eine Fehlkonfiguration der CMG-Option zur Überprüfung des Widerrufs von Client-Zertifikaten kann zu mehr Datenverkehr von Clients an die CMG führen. Dieser weitere Datenverkehr kann die Azure-Egress-Daten erhöhen, was Ihre Azure-Kosten erhöhen kann.
- Detaillierte Infos finden Sie hier:
- https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/cost

Cloud Management Gateway - Übersicht



Quelle: https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/overview