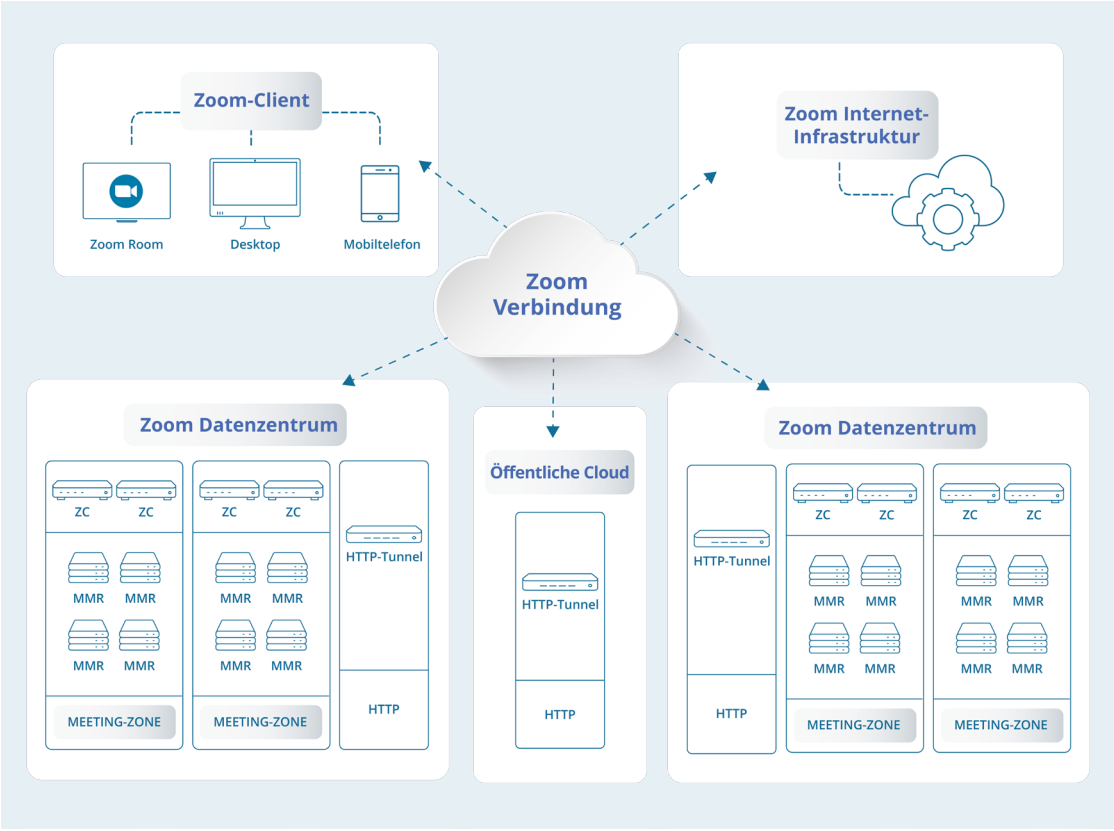
Überblick

Zoom ist führend in der modernen Unternehmensvideokommunikation mit einer einfachen und zuverlässigen Cloud-Plattform für Video- und Audiokonferenzen, Zusammenarbeit, Chat und Webinare auf Mobilgeräten, Desktop-Computern, Telefonen und Raumsystemen. Einer der Gründe für die Einfachheit und Zuverlässigkeit der Cloud-Plattform ist der Verbindungvorgang von Zoom. Mit dem Verbindungsvorgang von Zoom wird sichergestellt, dass bei jedem Zugriff auf die Plattform ein optimierter Pfad auf die geografisch zugeschnittene und stets verfügbare Zoom-Infrastruktur vorliegt. In diesem Whitepaper werden dieser Vorgang und die dahinterliegende Technologie vorgestellt.

Hauptkonzepte und -komponenten

Vor der Durchführung dieses Prozesses ist es wichtig zu verstehen, welche Schlüsselkomponenten mit dem Verbindungsfluss zusammenhängen und welche Funktion sie in der Zoom-Architektur einnehmen.



Zoom-Client

Der Zoom-Client ist die primäre Methode einer Person für den Zugriff auf die Zoom-Cloud. Obwohl er für unterschiedliche Betriebssysteme (macOS, Windows, Linux, Android, iOS, Chrome OS) und für eine Vielzahl an kontextbezogenen Anwendungen (Mobilgeräte, Desktop-PC, Zoom Rooms) verfügbar ist, bleibt sein Interaktionsmuster mit der Zoom-Cloud für alle Konfigurationen gleich.

Zoom Internet-Infrastruktur

Bei der Internet-Infrastruktur handelt es sich um eine Web-Anwendung mit hoher Verfügbarkeit, mit

der nicht nur die täglich genutzte zoom.us-Webseite hostet, sondern mit der auch über die weitläufigen API-Ressourcen Anfragen von Anwendungen bedient werden können, die von den externen Entwicklern und den unterschiedlichen Komponenten der Zoom-Infrastruktur gestellt werden.

Zoom-Meeting-Zone

Bei einer Zoom Meeting-Zone handelt es sich um einen logischen Zusammenschluss von Servern, die normalerweise physisch zusammengelegt werden, und auf denen Zoom-Sitzungen gehostet werden können. Eine Zoom Meeting-Zone und die zugehörigen Server können sich innerhalb eines der globalen Datenzentren von Zoom oder innerhalb eines Netzwerkes einer Organisation befinden, wenn die On-Premise-Lösung von Zoom eingesetzt wird. Die primären Komponenten der Meeting Zone sind Multimedia-Router und Zone Controller.

Zoom Zone-Controller

Ein Zoom Zone-Controller ist für die Verwaltung und Abstimmung aller Aktivitäten verantwortlich, die in einer bestimmten Zoom Meeting-Zone stattfinden. Diese Systeme, die eine Konfiguration mit einer hohen Verfügbarkeit besitzen, zeichnen die Last auf allen Servern in der Zone auf und verwalten Anfragen für neue Verbindungen in die Zone.

Zoom Multimedia Router (MMR)

Ein Zoom Multimedia Router ist für die Ausrichtung von Zoom-Meetings und Webinaren verantwortlich. Wie der Name schon sagt stellen diese Server sicher, dass der gesamte Umfang von Stimmen, Videos und Inhalten richtig zwischen allen Teilnehmern einer bestimmten Sitzung verteilt wird.

Zoom HTTP Tunnel (HT)

Der Service Zoom HTTP Tunnel ist ein integraler Bestandteil der Belastbarkeitsstrategie des Zoom-Netzwerkes. Diese Server, die sich in unterschiedlichen öffentlichen Clouds und Zoom-Datenzentren befinden, stellen einen Verbindungspunkt für Clients dar, die sich nicht über andere Netzwerkkanäle mit der Zoom-Plattform verbinden können. Sobald ein Tunnel zwischen dem Zoom Client und dem Zoom HTTP Tunnel aufgebaut wurde, kann der Client über die unterschiedlichen Datenzentren auf die Zoom-Meeting-Zone zugreifen.

Verbindungsablauf

Der Prozess einer Verbindung mit der Zoom-Sitzung ist in vier Phasen unterteilt, die im Folgenden beschrieben werden.

Suchen des Meetings

Nach dem Erhalt einer Anfrage über die Teilnahme an einer Sitzung kontaktiert der Zoom-Client zuerst die Zoom-Internet-Infrastruktur, um die entsprechenden Metadaten zu erhalten, die für den Zugriff auf ein Meeting oder Webinar nötig sind. Diese Kommunikation findet über eine HTTPS-Verbindung mit dem Port 443 statt, und der Zoom-Client nutzt diese Gelegenheit, um mehr Informationen über seine aktuelle Netzwerkumgebung zu erhalten (darunter Angaben wie die Verwendung eines Proxy-Servers). Am anderen Ende der Verbindung bereitet die Zoom-Internet-Infrastruktur ein Paket mit für diesen Client optimierten Daten vor. Mithilfe von Geo-IP und anderen Zoom-Service-Technologien wird eine Liste der optimal verfügbaren Zoom-Meeting-Zones und zugehörigen Zoom Zone-Controllern zusammen mit Meeting-Daten an den Client zurückgeschickt, damit der Client mit der nächsten Phase des Verbindungsvorgangs fortfahren kann.

Auswahl der Meeting-Zone

Der Verbindungsprozess geht dann mit einer Auflistung der Zoom Meeting-Zones, die der Zoom Client für die Sitzung verwenden könnte, in die nächste Phase des Arbeitsablaufs über. Um sicherzustellen, dass die beste Verbindung verwendet wird, versucht der Zoom-Client, eine Verbindung mit jedem der Zoom Zone-Controller innerhalb der Zoom-Meeting-Zones aufzubauen, die im vorherigen Schritt bereit gestellt wurden, und führt dann einen Netzwerk-Leistungstest durch. Durch einen Vergleich dieser Ergebnisse ist der Client in der Lage, zu bestätigen, dass ein Verbindungspfad zu jeder Zoom-Meeting-Zone vorliegt, und er kann diejenige mit der besten Leistung auszuwählen. Das innovative Protokoll von Zoom verwendet HTTPS. Diese Verbindung wird über SSL (Port 443) aufgebaut.

MMR-Auswahl

Der Client fragt dann nach Auswahl der idealen Zoom-Meeting-Zone aus der vorherigen Phase vom Zoom Zone Controller Angaben über den besten Zoom Multimedia Router (MMR) an. Nach der Identifikation kommuniziert der Zoom Client direkt mit dem MMR, um einen Steuerungskanal für die Sitzung aufzubauen. Diese Verbindung verwendet ein Protokoll, das von Zoom entwickelt wurde, welches über SSL mit Port 443 kommuniziert.

Medien-Routing

Der Zoom-Client führt nach einer Verbindung mit dem für die Sitzung optimalen Zoom Multimedia Router eine Priorisierung durch, in der er eine Verbindung für jede Medienart durchführt, die ausgetauscht wird, z. B. Video, Audio und Inhalt. Jede dieser Medienverbindungen versucht, das eigene Protokoll von Zoom zu verwenden und über UDP eine Verbindung mit Port 8801 aufzubauen. Wenn diese Verbindung nicht aufgebaut werden kann, wird Zoom versuchen über Port 8801 eine Verbindung mit TCP aufzubauen (gefolgt von SSL auf Port 443). Indem unterschiedliche Verbindungen für jede Medienart verwendet werden, können weitere Netzwerkoptimierungstechnologien (DSCP-Marking) verwendet werden, womit sichergestellt wird, dass im Netzwerk das wichtigste Medium gefördert wird.

Sonderfälle

Obwohl der oben beschriebene Vorgang viele Benutzerfälle abdeckt, gibt es einige Sonderfälle, die umgesetzt wurden, um sicherzustellen, dass eine zuverlässige Sitzung sogar in komplexen Netzwerken vorliegt.

Proxyserver

Während der Phase der Meeting-Suche im Verbindungsaufbau kann der Zoom Client bestimmen, ob ein Proxyserver im Netzwerk-Verbindungspfad verwendet wird. Wenn während des Verbindungsvorgangs in der Meeting Zone- und der MMR-Auswahl ein Proxyserver erkannt wurde, wird dieser sofort vom Zoom-Client verwendet, und es wird versucht, die entsprechenden Verbindungen mit dem Zoom Zone Controller und Zoom Multimedia-Router (mit Hilfe von SSL) aufzubauen.

HTTP-Tunnel

Wenn es nach 5,5 Sekunden keine Antwort von einem Zone Controller gibt, wird der Zoom-Client versuchen, eine Verbindung mit HTTP-Tunnel aufzubauen. Um mehrere Pfade für eine erfolgreiche Verbindung sicherzustellen, befinden sich diese Server sowohl in öffentlichen Clouds als auch hin Zoom-Datenzentren. Diese Verbindung wird über SSL (Port 443) aufgebaut. Der Zoom-Client wird mehrere HTTP-Tunnel anpingen, und der erste, der sich meldet, wird verwendet.

Web-Client

Wenn der Zoom-Client nicht in der Lage ist, sich mit einer der beschriebenen Methoden zu verbinden, wird er den Benutzer anweisen, sich mit dem Zoom Web-Client in seinem Browser mit dem Meeting zu verbinden, ohne bestimmte Plugins oder Software herunterzuladen. Der Zoom Web-Client versucht, über SSL (Port 443) eine Verbindung aufzubauen.

Schlussfolgerung

Immer mehr kleine und große Unternehmen verlassen sich täglich auf Zoom-Services. Zoom stellt mehrere Verbindungspfade bereit, die unterschiedliche Protokolle in geographisch weit verbreiteten Infrastrukturen einsetzen, um eine sichere Verbindung für alle Benutzer zu gewährleisten.