StarLeaf Cobal Gobal Network Whitepaper



Inhalt

1. Übersicht	3
Globale Verbindungen, Quality of Service und Zuverlässigkeit Ausgezeichnete Qualität	
2.2 Sicherheit und Zuverlässigkeit	
3. Endpunkte und Clients	4
3.1 Fähigkeiten der Endpunkte	4
3.2 Zusätzliche Leistungsmerkmale der StarLeaf Endpunkte	5
4. Management	5
4.1 Vorbereitung	5
4.2 Installation	5
4.3 Management der Besprechungsräume	6
4.4 Nutzer Management	6
5. Überwachung und Berichte	7
5.1 Detaillierte Verbindungsdaten	7
5.2 Anrufinformation	7
5.3 Nutzungsstatistik der Organisation	7
6. Sicherheit und Firewall Übergang	8
6.1 Überblick	8
6.3 Firewall Übergang	8
6.4 Bekannte Points of Presence	8



1. Übersicht

StarLeaf besitzt und betreibt ein globales Kommunikationsnetzwerk, die StarLeaf Cloud mit acht Pointsof-Presence (PoP) verteilt über Nord-Amerika, Europa, Asien und Australien.

Die Infrastruktur, auf der dieses Kommunikationsnetz basiert, wurde komplett von StarLeaf entwickelt und bietet eine leistungsfähige und zuverlässige Plattform für Videokonferenzen als Service für globale Unternehmen.

Wichtiges Unterscheidungsmerkmal der StarLeaf Lösung ist das kundeneigene Infrastruktur weder vorausgesetzt, noch benötigt wird. Diese einzigartige Unabhängigkeit ermöglicht es StarLeaf, sehr schnell auf Anforderungen zu reagieren und kontinuierlich die Bedürfnisse der Anwender zufrieden zustellen.

Die zugrundeliegenden Technologien und fortschrittliche Techniken bieten dem Nutzer folgende Vorteile:

- Die Möglichkeit jeden überall anzurufen, unabhängig von der Art des jeweiligen Kommunikationsendpunktes, sei es Microsoft Skype for Business/Lync, Cisco, Polycom, Lifesize oder jedes andere Standard basierte Gerät
- Sehr hohe Audio- und Videoqualität durch außergewöhnlichen Quality of Service
- Verschlüsselung zur Gewährleistung der Privatsphäre aller Gespräche
- Zuverlässiger Firewallübergang, ohne die Notwendigkeit zusätzliche Ports freigeben zu müssen
- Einfache zentrale Verwaltung, Steuerung, Überwachung und Auswertungen
- Ein Web Portal zur Verwaltung von Nutzern und Endpunkten
- Möglichkeit, nicht nur StarLeaf Endpunkte zu registrieren und zu verwalten, sondern auch alle bereits vorhandenen, standardbasierten H.323/SIP Endpunkte

2. Globale Verbindungen, Quality of Service und Zuverlässigkeit

Die Points-of-Presence (PoP) sind strategisch um den Globus verteilt und sichern so eine unvergleichliche Kommunikation mit effizienter Anrufvermittlung und kurzen Verzögerungszeiten weltweit.

Abb. 1: StarLeaf Points of Presence





2.1 Ausgezeichnete Qualität

Durch die Nutzung fortschrittlicher Techniken kann StarLeaf den bestmöglichen Quality of Service liefern. Dazu zählen die Nutzung von modernen flexiblen Codecs wie H.264 SVC und AAC-LD aber auch dynamisches Bandbreitenmanagement, Nutzung von Direkt Media und Fehlerkorrekturmechanismen. Dies ist nicht nur über hoch-verfügbare MPLS basierte Unternehmensnetzwerke möglich, sondern gerade auch über weniger zuverlässige Netzwerke, wie das Internet.

2.2 Sicherheit und Zuverlässigkeit

Die StarLeaf Could ist völlig redundant aufgebaut und wird an jedem PoP dupliziert. In dem unwahrscheinlichen Fall des Ausfalles eines Rechenzentrums, werden alle Verbindungen automatischen an einen alternativen PoP umgeleitet.

3. Endpunkte und Clients

StarLeaf unterstützt die Anmeldung von allen H.323 und SIP basierten Endpunkten, wodurch diese Teil der Cloud Infrastruktur werden und ein gesicherter Firewallübergang möglich wird. Diese alten Systeme können dadurch an den Clouddiensten teilnehmen und diese nutzen.

3.1 Fähigkeiten der Endpunkte

Die StarLeaf Cloud bieten allen Client-Systemen, ob H.323, SIP oder StarLeaf Software bzw. Hardware Videoendpunkten die folgenden Möglichkeiten:

- Zuweisung einer Rufnummer
- Integrierter Wählplan
- Anwahl aller Cloudsysteme mittels Rufnummer oder Email Adresse
- Anwahl externer H.323 und SIP-Geräte über Emailadresse (URI) oder IP-Adresse
- Erreichbar für alle externen H.323 und SIP Geräte über Email Adresse (URI)
- Fähigkeit über Microsoft Lync an zu rufen oder angerufen zu werden
- Herunterladen von Verbindungsberichten für die Fehlerdiagnose oder die Diagnose der Verbindungsqualität



3.2 Zusätzliche Leistungsmerkmale der StarLeaf Endpunkte

Zusätzlich bieten die StarLeaf Hardware und Software Endpunkte folgende Möglichkeiten:

- Im Portal zentral verwaltetes Adressbuch mit allen Teilnehmern und Raumsystemen
- Dynamisches Verbinden zur StarLeaf Cloud mit verschiedenen Techniken (einschließlich der Nutzung von TCP, um auch in schlecht konfigurierten Umgebungen effizient arbeiten zu können)
- Möglichkeit die verfügbaren Ports im Rahmen eines effizienten Firewall Management einzugrenzen
- Breitband Audio mit AAC-LD für geringe Verzögerung
 - » Fortschrittliche Techniken für die Behandlung von unterschiedlichen Netzwerksituationen:
 - » Dynamische Bitrate
 - » Skalierbare Videokodierung
- Vorwärtsfehlerkorrektur bei Packet-Loss Fehlern
- Fähigkeit, ein Zweier-Gespräch über den "create conference-Schalter in eine adhoc Besprechung mit mehreren Teilnehmern zu erweitern

4. Management

Das Herzstück der StarLeaf Cloud ist ein Management-Portal, welches Ihrem Unternehmen die komplette Kontrolle der bestehenden Videosysteme ermöglicht. Von dieser Schaltzentrale aus können Video-Endpunkte, Räume und Nutzer versorgt und verwaltet werden. Dadurch ist ein immer aktuelles Verzeichnismanagement gewährleistet. Es bietet auch die Kontrolle über die Weitergabe und Nutzung der StarLeaf Breeze Software Clients. Diese kann von allen Nutzern und temporären Gästen genutzt werden. Es besteht auch die Möglichkeit, neben StarLeaf Systemen andere Videoendpunkte zu registrieren und zu verwalten.

4.1 Vorbereitung

Das StarLeaf-Portal bietet Administratoren alles, was zur Vorkonfiguration von Systemen für Nutzer oder Besprechungsräumen notwendig ist.

4.2 Installation

Alle vorbereiteten Systeme sind automatisch für eine Plug-and-Play Installation vorkonfiguriert. Dazu erzeugt das Portal einen QuickConnectTM Code der direkt über den Touchscreen der StarLeaf Hardware eingegeben wird. Ist der Code eingegeben, verbindet sich das System automatisch mit der Cloud und wird von dort authentifiziert. Alle notwendigen Informationen, wie auch das Telefonverzeichnis werden automatisch geladen. Dieser Vorgang dauert nur einige Minuten, dann ist das vorkonfigurierte System fertig installiert und betriebsbereit.



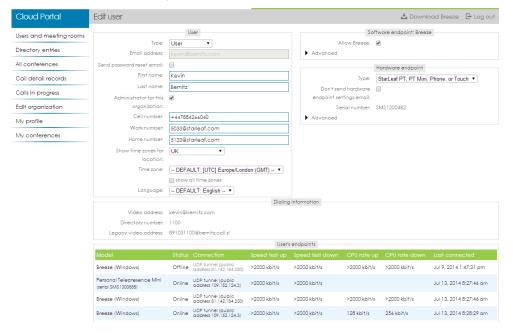
4.3 Management der Raumsysteme

Wenn Endpunkte einmal vorbereitet sind, können sie über das Portal verwaltet und alle Einstellungen vorgenommen werden.

4.4 Nutzer Management

Administratoren können über das Portal Anwender mit Konten und Client Systemen versorgen und dann die detaillierten Angaben über die Anwender aktualisieren.

Abb. 2: Benutzerverwaltung in dem Cloud Portal



In dem obigen Beispiel kann der Administrator Informationen über Software Clientsysteme und Hardware Endpunkte einsehen und bekommt Informationen zu Verbindungsgeschwindigkeit und dem Verbindungstyp.

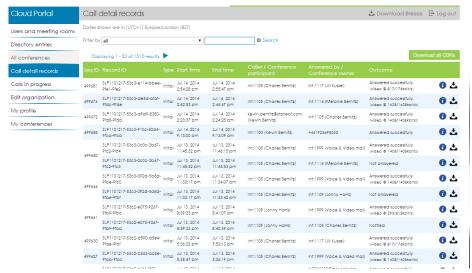


5. Überwachung und Berichte

5.1 Detaillierte Verbindungsdaten

Zur Unterstützung des Enduser Support kann der Administrator in der "Call-Detail-Records" Ansicht Informationen zu einem Gespräch suchen und danach Filtern (z. B. nach dem Namen des Anrufenden).

Abb. 3: Überwachung von Anrufen in dem Cloud Portal



5.2 Anrufinformation

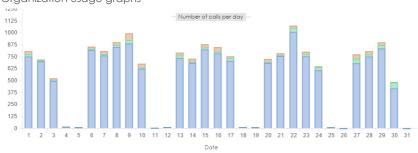
Die 'Call Information'-Ansicht zeigt eine Zusammenfassung von dem Anruf, wie z. B. verwendete Codecs , Zustand der Netzwerkverbindung (Bit-Rate, Paketverlustrate, max / min / average, jitter etc.) bidirektional für jeden Kanal separat. Dies ist hilfreich bei der Diagnose von Problemen mit der Anrufqualität.

5.3 Nutzungsstatistiken

Der Administrator kann monatliche Nutzungsberichte (für die letzten 3 Monate) der Organisation abrufen. Diese enthalten:

- Anzahl der Videokonferenzen pro Tag (Punkt-zu-Punkt, QuickMeet und geplante Konferenzen)
- Videokonferenzdauer in Minuten pro Tag (Punkt-zu-Punkt, QuickMeet und geplante Konferenzen)
- Die aktivsten Teilnehmer
- Die aktivsten Raumsysteme







6. Sicherheit und Firewall Übergang

6.1 Überblick

Sicherheit ist von höchster Wichtigkeit und Sicherheitsaspekten wurde in allen Ebenen der StarLeaf Architektur berücksichtigt, damit die Privatsphäre bei allen Gesprächen gewährleistet ist.

Die StarLeaf Serie von Endpunkten und Clientsystemen beinhalten signierte Zertifikate, wie dies auch bei den StarLeaf Servern an den Points-of-Presence der Fall ist. Diese Zertifikate werden für die gegenseitige Authentifizierung der Endpunkte und der Server verwendet, um eventuelle "man-in-themiddle"-Attacken zu unterbinden.

Weiterhin ermöglicht der StarLeaf Service einen problemlosen Firewallübergang, sodass die Endpunkte innerhalb gesicherter Umgebungen verbleiben können. Dabei werden Verschlüsselungen wie z. B. AES unterstützt.

6.2 Authentifizierung und Verschlüsselung

Authentifizierung erfordert ein unterzeichnetes Zertifikat, welches bei allen StarLeaf Endpunkten (Hardware- und Software-Endpunkte) implementiert ist. Alle StarLeaf Server in den PoPs besitzen ebenfalls Zertifikate, welche von den StarLeaf Endpunkten zur Authentifizierung angefordert werden.

Jeder, von einem StarLeaf Endpunkt getätigter Anruf ist authentifiziert und verschlüsselt. Ein Anruf an einen beliebigen Endpunkt ist auch verschlüsselt, sofern dieser Endpunkt die Verschlüsselung unterstützt. Sofern Endpunkte anderer Hersteller in Verbindung mit StarLeaf Endpunkten verwendet werden, kommen die Industriestandards AES, H.325 und TLS zum Einsatz.

6.3 Firewallübergang

Alle, bei der StarLeaf Cloud registrierten Endpunkte können über eine Firewall hinweg Gespräche aufbauen oder an Besprechungen teilnehmen. Das ermöglicht einfache und direkte Business-to-Business Gespräche ohne das Sicherheitsniveau zu senken.

Das wird durch StarLeaf's eingebaute Firewall / NAT-Technologie möglich. Dabei wird nur ein einziger Port für die Verbindung zum StarLeaf Netzwerk benötigt.

Der Firewall-Durchgang für StarLeaf Endpunkte nutzt nur einen einzigen TCP und maximal einen UDP-Port. Für StarLeaf müssen an der Firewall nicht eine Vielzahl von Ports geöffnet werden, was eine Schwächung der Sicherheit bedeuten würde.

Wenn Geräte Dritter zum Einsatz kommen, so werden Industriestandards wie z. B.: H.460 und ICE verwendet.

6.4 Bekannte Points-of-Presence

Einigen Unternehmen haben sehr strenge Firewall Regeln, die entsprechend konfiguriert sind, um Datenverkehr nach außen zu zulassen. Da das StarLeaf Netzwerk in der Hand von StarLeaf ist, bedarf es nur der Öffnung für eine einzige IP Adresse oder einer DNS-Adresse. Somit bleibt die Sicherheit vollständig erhalten.