AVAYA Deutschland GmbH

Implementation Service Description (ISD) - IP Office Web Collaboration

ISD Bezeichnung: IPO_Web Collab_V01_DE_E
Ausgabe: Februar 2015

1.0 Grundlagen der Implementierung

Dieses ISD ist eine Anlage zum Vertrag zwischen Avaya GmbH & Co. KG (nachfolgend „Avaya“) und dem Kunden. Zusätzlich finden die „Bedingungen für Implementierungsleistungen“ in der jeweils aktuellen Fassung Anwendung.

2.0 Produktspezifische Leistungen

2.1 Folgende produktspezifische Leistungen sind enthalten:

Die Einrichtung der Applikation Web Collaboration beinhaltet die folgenden Leistungen:

- Austausch der benötigten, technischen Daten im Rahmen eines telefonischen Workshops, vorgelagert zur Implementierung.
- Inbetriebnahme des von Avaya mitgelieferten, vorinstallierten Servers mit der Applikation Web Collaboration. Die Applikation wird durch starten der Serverdienste bzw. verschiedener Instanzen aktiviert.
- Server einrichten nach Kundendaten (IP-Adressen etc.)
- Konfiguration des Web Collaboration Servers nach Kundenvorgabe.
- Implementierung der kundeneigenen Server Zertifikate auf dem Server.
- Lizenz-Server überprüfen und ggf. anpassen.
- Funktionstest

2.2 Zusätzliche Leistungen

Zusätzliche Leistungen, die

- über die Standardimplementierung hinausgehen, oder
- optionale Leistungen gemäß Ziffer 4.0 darstellen, oder
- durch die nicht zeitgerechte oder nicht vollständige Bereitstellung der unter Ziffer 3.0 genannten Mitwirkungs- und Beistellungsleistungen verursacht werden,

werden von Avaya jeweils nach tatsächlichem Aufwand zu den dann jeweils gültigen Listenpreisen berechnet.

3.0 Mitwirkungspflichten und Beistellungen des Kunden

Die Informationen die während des remote Workshops ausgetauscht, bzw. angefordert werden, müssen zum Zeitpunkt der Implementierung vorliegen.

- Stellen von Zertifikaten pro FQDN (Fully Qualified Domain Name; vollständiger Netzwerk Domänen Name) der „Network Elements“ des Web Collaboration (Self-signed möglich)
- Für Web Collaboration wenn vom Internet erreichbar: Stellen von 2 Server Zertifikaten. Empfohlen werden zwei Zertifikate von einer „Trusted Signing Authority“, Zertifikatsformat PEM,PKCS#12. Nur damit sind alle Funktionen möglich. Die Alternative mit Einschränkungen ist ein „Self Signed Certificate“. Dieses muss dann auf allen Clients installiert werden.

3.1 Netzwerk Voraussetzung

- Fest zugewiesene IP-Adressen.
- FQDN Bezeichnung für die Serverdienste und pro laufende Instanz je einen FQDN nach Vorgabe.
- Stellen von 2 öffentlichen FQDNs für den Aufruf der Web Collaboration vom Internet aus (in Verbindung mit dem Bereitstellen der dazugehörigen Zertifikate)
- DNS und NTP Server erreichbar

3.2 Power Management Voraussetzungen

Ein Power Management, das von einigen Herstellern angeboten wird, darf auf dem betreffenden Server/PC nicht aktiviert werden. Ein Power Management kann den Prozessor und die Festplatte in einen Stromsparmodus schalten. Alle Power Management Funktionen müssen abgeschaltet sein.

3.3 Lizenz Voraussetzungen

- System Lizenz „Preferred Edition“ oder „Server Edition“
- Je Benutzer (Konferenzraum) die Lizenz „Tele Worker“ (nicht verfügbar bei „Server Edition“), „Office Worker“ oder „Power User“.
- Je Benutzer (Konferenzraum) zusätzlich die Lizenz „Web Collaboration“

3.4 Hardware Voraussetzungen

3.4.1 Kommunikationssystem

- IP Office mit mindestens Release 9.1
- Aktives one X-Portal für IP Office.

3.4.2 Schnittstellen

Nicht zutreffend

3.4.3 Server/PC

Der von Avaya mitgelieferte Server entspricht den Vorgaben.

3.5 Software Voraussetzungen

3.5.1 Server

Der von Avaya mitgelieferte Server entspricht den Vorgaben.

3.5.2 Client

- Installierte Software für One X-Portal User oder IP Office Outlook Plug-in oder Avaya Communicator for Windows oder Avaya Communicator for iPad
- Windows 7 oder 8.1 mit Internet Explorer 10 oder höher oder Mozilla Firefox 32 oder höher
  oder Chrome 37.0 oder höher
- MAC OS X 10.7 bis 10.09 mit Safari 5 bis 7 (nicht IPad)
- Für einen Web Collaboration Agent; Adobe Flash 10.2.0 oder höher
- Für Web Collaboration: Java 6 update 18 (1.6.0_18) oder höher.
- Server Zertifikat installiert im Browser

3.6 Produktspezifische Sicherheitsmaßnahmen

Der Kunde sorgt für ausreichenden Virenschutz durch Installation eines geeigneten Virenscanners. Das regelmäßige Update der Virensignaturen (Voraussetzung ist ggf. ein zugehöriger Vertrag mit einem Drittlieferanten) obliegt dem Kunden.
Für die Nutzung von WEB Collaboration, mit externen Benutzern, muss der zugehörige Server über das Internet von außen erreichbar sein. Dafür muss ein Reverse Proxy durch den Kunden konfiguriert werden.
Der Server darf nicht direkt an einen Internetanschluss angeschlossen werden, sondern muss hinter einer Firewall in das Kunden-LAN, einer sogenenten DMZ, implementiert werden.

4.0 Optionale Leistungen

Nachfolgende Leistungen sind nur dann Bestandteil dieser Implementation Service Description (ISD), wenn diese vom Kunden jeweils gesondert schriftlich beauftragt wurden.

4.1 DLI IPO Web Collab. Kunden-Server (#.230.007.746)

4.1.1 Produktspezifische Leistungen

Implementierung einer IP Office Web Collaboration Lösung auf einem kundeneigenen Server. Dies kann auch ein virtueller Server basierend auf VM-WARE sein.

Server Überprüfung:

- Austausch der benötigten, technischen Daten im Rahmen eines telefonischen Workshops, vorgelagert zur Implementierung.
- Hardwareanforderungen laut Avaya Produktvorgabe prüfen.
- Bei Verwendungs einer virtuellen Serverumgebung wird die initiale Implementierung nur zusammen mit dem Kundenadministrator ausgeführt. Dazu gehören plattformnahe Einstellungen wie z. B. Zuweisung von Prozessorkernen, Speicherplatz, IP-Adressen, etc.
- Bei Verwendung einer virtuellen Umgebung: Übergabe der OVA-Files an Kunden und gemeinsames Einschalten der virtuellen Instanz
- Ausführen der Setuproutinen von Web Collaboration inklusive aktueller Updates. Dabei wird das Betriebssystem Linux mit installiert.
- Konfiguration von Web Collaboration und IP Office.
- Implementierung der kundeneigenen Server Zertifikate auf dem Server.
- Lizenz-Server überprüfen und ggf. anpassen.
- Funktionstest

4.1.2 Voraussetzungen

- Vor Beginn der Arbeiten an kundeneigenen Servern/PCs, hat der Kunde eine Datensicherung vorzunehmen. Dies muss Avaya schriftlich bestätigt werden.
- Die Informationen, die während des remote Workshops ausgetauscht bzw. angefordert werden, müssen zum Zeitpunkt der Implementierung vorliegen.
- Stellen von Zertifikaten pro FQDN der „Network Elements“ des Web Collaboration (Self-signed möglich)
- Für Web Collaboration wenn vom Internet erreichbar: Stellen von 2 Server Zertifikaten. Empfohlen werden zwei Zertifikate von einer „Trusted Signing Authority“, Zertifikatsformat PEM,PKCS#12. Nur damit sind alle Funktionen möglich. Die Alternative mit Einschränkungen ist ein „Self Signed Certificate“ Dieses muss dann auf allen Clients installiert werden.
- System Lizenz „Preferred Edition“ oder „Server Edition“
- Je Benutzer (Konferenzraum) die Lizenz „Tele Worker“ (nicht verfügbar bei „Server Edition“), „Office Worker“ oder „Power User“.
- Je Benutzer (Konferenzraum) zusätzlich die Lizenz „Web Collaboration“

Netzwerk Voraussetzung

- Fest zugewiesene IP-Adressen.
- FQDN Bezeichnung für die Serverdienste und pro laufende Instanz je einen FQDN nach Vorgabe.
- Stellen von 2 öffentlichen FQDNs für den Aufruf der Web Collaboration vom Internet aus (in Verbindung mit dem Bereitstellen der dazugehörigen Zertifikate)
- DNS und NTP Server erreichbar

Power Management Voraussetzungen

- Ein Power Management, das von einigen Herstellern angeboten wird, darf auf dem betreffenden Server/PC nicht aktiviert werden. Ein Power Management kann den Prozessor und die Festplatte in einen Stromsparmodus schalten. Alle Power Management Funktionen müssen abgeschaltet sein.

Kommunikationssystem

- IP Office mit mindestens Release 9.1
- Aktives one X-Portal für IP Office.

Server/PC

- Avaya Web Collaboration wird ausschließlich mit von Avaya positiv getesteten Applikationen auf einem Server implementiert. Nur dann ist der Servicesupport von Avaya gewährleistet.
- Server muss betriebsfertig, aber ohne Betriebssystem installiert und für die Verbindung mit dem lokalen Netzwerk des Kunden vorbereitet sein.
- Es ist ein PC erforderlich, der auf einer Server Hardware basiert (24/365 Betrieb).
- Mindestvoraussetzung für den Server:
- HP ProLiant DL360p G8
- Intel 2x8 Core a 2,3GHz E5-2630
- 32 GB RAM
- 2x300 GB freien Festplatten Speicher (RAID1)
- DVD-Laufwerk
- Monitor, Maus und Tastatur für die Dauer der Implementierung

Abweichend in einer virtuellen Serverumgebung:

- Die initiale Implementierung der virtuellen Umgebung erfolgt nur zusammen mit dem Kundenadministrator.
- Die Anforderungen an die virtuelle Hardware wird während des Designs gemäß der Kundenkonfiguration von Avaya dem Kunden mitgeteilt. Der Kunde muss diese auf der virtuellen Server Umgebung entsprechend reservieren.
- Als virtuelle Umgebung wird nur die Plattform VM-Ware ESXi 5.1 Hypervisor mit vCenter sowie vSphere unterstützt.

Client

- Installierte Software für One X-Portal User oder IP Office Outlook Plug-in oder Avaya Communicator for Windows oder Avaya Communicator for iPad
- Windows 7 oder 8.1 mit Internet Explorer 10 oder höher oder Mozilla Firefox 32 oder höher
  oder Chrome 37.0 oder höher
- MAC OS X 10.7 bis 10.09 mit Safari 5 bis 7 (nicht IPad)
- Für einen Web Collaboration Agent; Adobe Flash 10.2.0 oder höher
- Für Web Collaboration: Java 6 update 18 (1.6.0_18) oder höher.
- Server Zertifikate installiert im Browser

Produktspezifische Sicherheitsmaßnahmen

- Der Kunde sorgt für ausreichenden Virenschutz durch Installation eines geeigneten Virenscanners. Das regelmäßige Update der Virensignaturen (Voraussetzung ist ggf. ein zugehöriger Vertrag mit einem Drittlieferanten) obliegt dem Kunden.
- Für die Nutzung von WEB Collaboration, mit externen Benutzern, muss der zugehörige Server über das Internet von außen erreichbar sein. Dafür muss ein Reverse Proxy durch den Kunden konfiguriert werden.
- Der Server darf nicht direkt an einen Internetanschluss angeschlossen werden, sondern muss hinter einer Firewall in das Kunden-LAN, einer sogenenten DMZ, implementiert werden.