UNIFY Harmonize your enterprise

Remote Service Platform RSP Grundlagen des Betriebes

Document Release : V1.1
Release Date : 2016-01-28

Table of Contents

1. Remote Service Platform RSP

Die Remote Service Platform RSP von Unify stellt Remote Zugänge zu Unify Produkten auf Kundenseite für Partner und Unify selbst bereit.
Die RSP selbst besteht intern aus dem bewährten SIRA (Secured Infrastructure for Remote Access) und SSDP (Smart Service Delivery Platform).

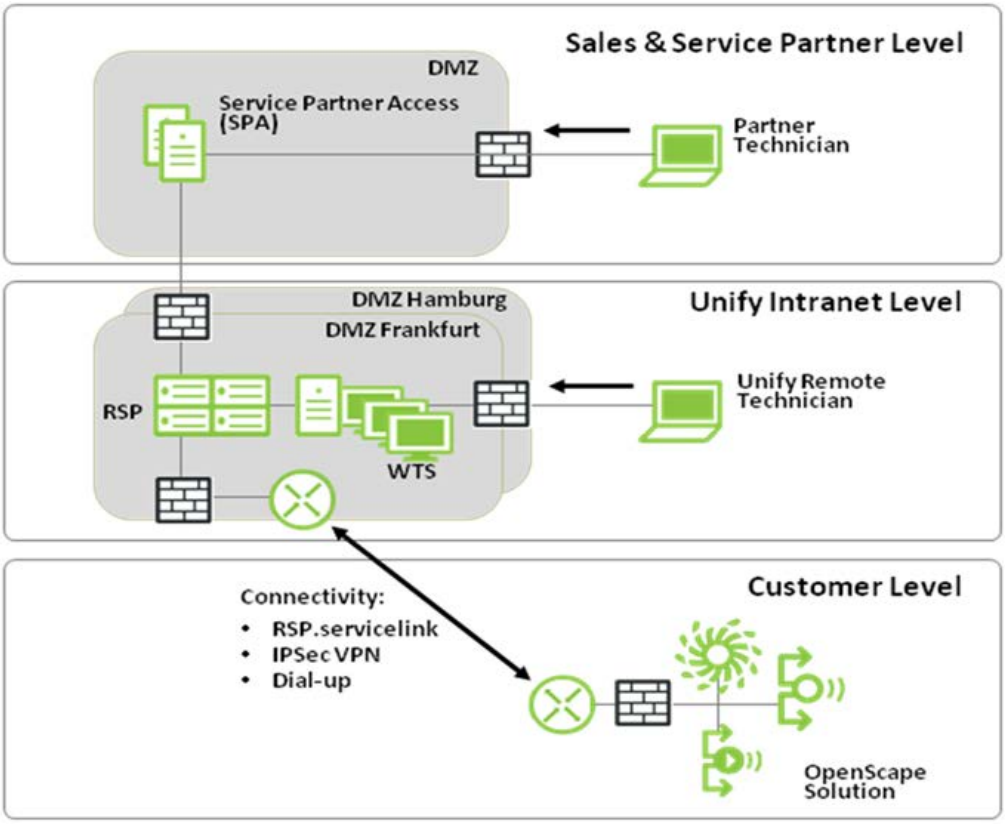
Der SIRA Teil der RSP wurde um die neue Verbindungsart RSP.servicelink erweitert, die als direkter Nachfolger von SSDP deutliche Verbesserungen bietet. Es gibt zur Zeit sowohl die in der OpenScape Business (OSBiz) integrierte Version und auch den RSP Buffalo Router zur Anbindung aller Geräte eines Kundenstandortes.

Die RSP stellt heute eine über viele Jahre gewachsene und stetig verbesserte Infrastruktur dar, an der aktuell über 220.000 Geräte remote angeschaltet sind und mehr als die doppelte Anzahl möglich ist. Die Art der Anschaltung dieser Geräte hat sich mit den Jahren entwickelt.

So sind heute folgende Verbindungsarten in RSP vorhanden:

1. Breitbandiger Zugang mit **IPSec-VPN**.
2. Breitbandiger Zugang mit **RSP.servicelink** (Neu).
3. ISDN Zugang, (nur mehr für bestehende Verbindungen).
4. Modem Zugang, (nur mehr für bestehende Verbindungen).
5. Breitbandiger Zugang mit SSDP (bereits in Ausphasung).

Jede Remote Connection zu Unify Geräten von Unify Remote Service läuft über RSP.



Im Betrieb werden folgende Themen betrachtet:

- **Infrastruktur**
  Hardware, Software, Kapazität, Schwellwerte, Auswahl, Bestellung, Inbetriebnahme, Monitoring, Wartung, Security,.. In diesem Dokument wird der Ist Stand beschrieben. Die Planung der Infrastruktur wird getrennt durch Unify IT beschrieben.
- **Support**
  Tätigkeiten der verschiedenen Support-Level, Erreichbarkeit, Qualität, Ticket Tool,... In diesem Dokument ist der Ist Stand beschrieben soweit vereinbart. Die Planung des künftigen Supports wird getrennt durch Unify IT beschrieben.
- **Operations**
  Verfügbarkeit des Systems, Verwaltung der Partner- und Kundengruppen und Anwender, Backup/Restore, Ersatzteilverwaltung,...
  In diesem Dokument ist der Ist Stand beschrieben soweit konkret vereinbart. Die Planung des künftigen Betriebes wird getrennt durch Unify IT beschrieben.
- **SLA/OLA**
  (Vereinbarungen mit den Stakeholdern, Monitoring, Berichte,...)
  Heute ist der Betrieb intern durch eine „Best Effort" Vereinbarung geregelt. Eine SLA/OLA Regelung mit definierten Zeiten ist in Vorbereitung

1.1. Verfügbarkeit

Unify trifft die notwendigen Vorkehrungen um eine hohe Verfügbarkeit der RSP sicherstellen.

Die gesamte Infrastruktur der RSP (Server, Anbindungen,Datenbanken, ...) ist heute (mit Ausnahme von SSDP) gedoppelt vorhanden und als georedundante **Standort-Dopplung** auf die identisch ausgerüsteten Standorte Frankfurt und Hamburg verteilt.
Zusätzlich dazu sind innerhalb der einzelnen Standorte (mit Ausnahme von SSDP) alle relevanten **Server gedoppelt** und auf diesen weiters Hard-Disk Dopplung (RAID) verwendet. Auch Datenbanken, Zugänge und Tools sind in redundanter Form vorhanden.

An beiden Standorten sorgt ein USV (Unterbrechungsfreie Stromversorgung) dafür, dass bei kurzen Stromausfällen die RSP Infrastruktur nicht ausfällt.
Die Serverräume sind mit Brand- und Feuermeldern ausgestattet, die 24 Stunden von einer Betreiberfirma überwacht werden.

Staging
Es gibt mehrere Systeme der RSP, die für Entwicklung und Test oder Staging oder den Live-Betrieb eingesetzt werden. Neue Hard- und Software durchläuft einen Staging Prozess, in dem vor der Übernahme in das Live-System die Unbedenklichkeit geprüft wird.

Backup/Restore:
Backups werden toolgestützt täglich durchgeführt um bei Bedarf Systeme in kürzester Zeit wieder herstellen zu können.
Sonderfall SSDP:
Der SSDP Teil befindet sich bereits in **Ausphasung**. Unify hat sich entschlossen SSDP auszuphasen und ALLE neuen Produkte über die SIRA Platform mit der neuen Anbindungsart RSP.servicelink anzuschalten. Ein Großteil der heute mit SSDP angeschalteten Produkte wird auf RSP.servicelink migriert werden.

Die Entscheidung zur Ausphasung von SSDP hat zur Folge, dass **SSDP der einzige Teil der RSP ist, der nicht Teil des Redundanzkonzeptes ist.**
SSDP wird so wie die anderen Teile der RSP in der Performance überwacht und die Erreichung von Schwellwerten führt auch hier zu Einflüssen in der Kapazitätsplanung.

1.2. Security

Security allgemein:
Die RSP Infrastruktur besteht aus dem abgesicherten RSP Netzwerk. Dieses ist gegen das UNIFY Network sowie in Richtung Außenwelt jeweils durch Firewall-Systeme abgesichert.

Alle Verbindungen zu Kundensystemen werden über den im RSP Netzwerk befindlichen Windows Terminal Server WTS aufgebaut.

VPN-Tunnel über Internet, Wähl- oder Standleitungen zum Kunden erfolgen über Access Router oder Gateways (z.B. für X.75, MSV1 / CSR1). Eigener RSP IP-Adressraum, der erst auf den Access-Routern auf die Kundenadresse umgewandelt wird.

Die Benutzerverwaltung erfolgt in einem weltweit verteilten RSP Active Directory mit Berechtigungen für jeden Benutzer mit Trust zwischen den Domänen.

Zugangssicherheit räumlich:
An beiden RSP Standorten sind die Zugänge zu den Gebäuden und den Server-Räumen gesichert und überwacht. Zugang ist nur für qualifiziertes und registriertes Personal möglich.

Zugangssicherheit Online:
Der Zugriff auf die RSP über WTS wird durch die UNIFY CN-seitige Firewall beschränkt auf RDP-Zugriff für die Workstations der UNIFY Mitarbeiter mit Fernwartungsaufgaben und Mitarbeiter, die den Remote Access Service (RAS) ins UNIFY Corporate Network nutzen.
Der WTS Zugriff erfolgt verschlüsselt (RC4 Algorithmus) mittels Microsoft RDP 6.0 Protokoll.

Der Remote Access Service (RAS) ist ein Sicherheits-Zugang vom öffentlichen Netz ins UNIFY Corporate Network, welcher IP-Sec Verschlüsselung benutzt.

Der Online Zugang zur RSP erfordert mehrmalige Authentifizierung.
Eine erste Authentifizierung ist nötig, um in das Unify Intranet zu kommen. Dort ist eine weitere Authentifizierung nötig, um sich an der RSP einloggen zu können.

Der Zugang für Partner zur eigenen Gruppe innerhalb der RSP erfolgt über Login am Partner Portal and RSP Login.

Remote Service Techniker können sich weltweit bei entsprechender Autorisierung an der RSP anmelden, um eine Vertretung, Produktspezialisierung, 2nd-, 3rd-Level oder Vendor-Support sicherzustellen.

Trennung von Partnern, Kunden und Unify:
Sales und Service Partner können in vollem Umfang die Vorteile der Remote Service Platform nutzen. Benutzer und Geräte sind von anderen Partnern und Unify durch Verwendung von Closed User Groups völlig getrennt.
Jeder Partner erhält Administrationrechte für seine Gruppe und zur sicheren Eskalation eine eigene Eskalationsgruppe, die auch bei Eskalationen die Sichtbarkeit gezielt einschränkt.

Virus Schutz:
An beiden RSP Standorten laufen Virenschutzprogramme, die bereits vor der Einspielung jeder Software auf dem Staging System ablaufen.

Sichere Verbindung von der RSP zum Kundengerät:
In der RSP Datenbank können zu jedem Kundengerät zwei Verbindungsarten konfiguriert werden, wobei eine davon als bevorzugte Verbindung markierbar ist.

- **RSP.servicelink:** Gesicherte Internetverbindung auf Basis von OpenVPN und SSL-VPN Protokoll verwendet AES 256 bit CBC Verschlüsselung. Serverzertifikat und individuelle Client Zertifikate.
- **IPSec-VPN:** Gesicherte Internetverbindung braucht gegenseitige manuelle Administration sowohl auf Kunden- als auch auf Unify Seite. Die jeweilige andere Seite ist manuell eingetragen. Sicherung durch IPSec-VPN und 256bit AES/DES.
- **ISDN:** Wählverbindung von der RSP zum Kundengerät, Sicherung durch Call back und CHAP (projektspezifisch Verschlüsselung bis 3DES/168 Bit möglich).

- **Modem:** Wählverbindung von der RSP zum Kundengerät (nicht mehr für Neugeräte)
- **SSDP:** Gesicherte Internetverbindung auf Basis von SSL-VPN. AES 128 bit CBC Verschlüsselung SHA-1. Server-Zertifikat.

Der Vollständigkeit halber sind hier alle Verbindungsarten aufgelistet, obwohl heute fast nur noch RSP.servicelink (für LAN taugliche Produkte ohne Monitoring Bedarf) und IPSec-VPN (Grosse Bestandskunden mit Monitoring Bedarf) zum Einsatz kommen.

Verbindungen zwischen Kundensystemen sind über die RSP explizit verhindert.

Weitere Details dazu sind im Remote Service Platform V2 White Paper zu finden.

Logging von Zugriffen:
Jeder Zugriff auf ein Kundengerät (wer verbindet sich wann wohin) wird zentral mitgeloggt, gespeichert und periodisch an einem anderen Ort archiviert. Im Bedarfsfall können diese Zugangsinformationen dem Kunden oder Partner innerhalb eines Jahres zur Verfügung gestellt werden. Die Unify User sind nicht mit Namen, sondern nur mit Unify eindeutigen Benutzerkennungen ersichtlich. Namen werden nicht nach extern gegeben.

Logging der Zugriffe auf Kunden- oder Partnerseite ist mit Mitteln der RSP nicht möglich. Soweit bei uns bereits Erfahrung dazu existiert, kann aber Beratung zu Logging Produkten von anderen Herstellern erfolgen, die ein lokales Protokoll auf Kundenseite erzeugen können.

Logging von Inhalten:
Alle Passwort Anfragen und Änderungen werden protokolliert.

Alle ausgeführten Kommandos, wenn eine Kommando Schnittstelle benutzt wird, werden am WTS geloggt.

Projektspezifisch existiert die Möglichkeit bei Sessions mit graphischen User Interface (RDP/Web) ein Video Logging aufzunehmen.

1.3. Kapazitäts-Management

1.3.1. Dimensionierung

Das RSP Operations Team berücksichtigt bereits jetzt viele Parameter, die dazu beitragen, die Systemleistung der RSP hoch zu halten.

Es werden auf allen WTS Servern Schwellwerte beobachtet, die frühzeitig dazu führen, dass ein zusätzlicher WTS bestellt und in Betrieb genommen wird. Dies ist wichtig für die Anzahl der Anwender, welche die RSP aktiv nutzen. WTS sind für 100 gleichzeitige Sessions ausgelegt. Es sind weltweit verteilt ausreichend WTSen vorhanden und bei Bedarf kommen weitere dazu. (Ausfallsicher durch n+1 WTS)

In ähnlicher Weise wird die zentrale Datenbank überwacht.

Messungen der Performance der WAN Anbindung führten zu einer deutlichen Erhöhung der WAN Bandbreite, wodurch wir bereits heute für den Betrieb mit einer deutlich erhöhten Anzahl von Benutzern gerüstet sind.

Ein RSP.servicelink Server ist für 8000 gleichzeitige Verbindungen ausgelegt. (Ausfallsicher n+1 Server). Hier erfolgt eine periodische Kapazitätsplanung, welche sich aus der Anzahl der angeschalteten Geräte über einen bestimmten Zeitraum und Planungsdaten vom Produkthaus, Service und Partner zusammensetzt.

Die RSP ist ausgelegt, eine deutlich höhere Anzahl von Geräten mit den Verbindungsarten ISDN, RSP.servicelink oder IPSec-VPN Verbindungen zu verkraften.

Nachdem SSDP ausgephast wird und nun für alle Unify Produkte die Möglichkeit besteht, die Remote Verbindung über RSP.servicelink zu realisieren, erfolgt für SSDP keine neue Kapzitätsanpassung. Durch die Migration von SSDP auf RSP.servicelink werden für SSDP Ressourcen frei, welche den Betrieb und Performance in der Ausphasung stabil hält.

1.3.2. Monitoring des Systemverhaltens

Aktuell wurde zusätzlich zu den oben beschriebenen Überwachungen der Systemparameter ein neues automatisierten Monitoring (Scapa) eingeführt, das im Bereich von SSDP heute bereits erste Ergebnisse zeigt.

Heute werden die Loginwartezeit und die Oberflächenperformance von SSDP automatisch überwacht und wöchentlich reportet

Dieses automatisierte Monitoring ist ein wichtiger Aspekt bei der aktuellen Planung der RSP und soll auf alle Bereiche der RSP ausgeweitet werden. Ein RSP weites automatisiertes Monitoring, ähnlich wie bei SSDP, ist in Planung und Aufbau.

Die Ergebnisse dieses Monitorings von Last- und Performance Werten haben direkten Einfluss auf das Kapazitätsmanagement und ist eine deutliche Hilfe bei der rechtzeitigen Reaktion auf Erreichung von Schwellwerten.

Das rechtzeitige Erkennen, Analysieren, Bestellen und Inbetriebnehmen von Systemerweiterungen sind wichtige Schritte zur Sicherung der Verfügbarkeit der RSP.

1.3.3. Redundante Standorte

Die RSP Infrastruktur ist heute auf die Standorte Frankfurt und Hamburg in redundanter Form verteilt. Im Normalbetrieb werden die beiden Standorte technisch auf dem gleichen Stand gehalten, was Hardware, Software und die Datenbanken betrifft.

Die Standort Dopplung hat deutliche Vorteile, da im Hintergrund auf dem inaktiven System Veränderungen vorgenommen werden können ohne Auswirkung auf Anwender.
Upgrades oder andere Wartungsaktivitäten werden nach erfolgreichen Tests auf dem Staging System zuerst auf dem inaktiven Standort vorgenommen. Danach erfolgt manuell eine **Umschaltung der Standorte**, wobei versucht wird, die Umschaltung auf einen Zeitpunkt zu legen, an dem möglichst wenige User angeloggt sind. Anwender, die zum Zeitpunkt der Umschaltung aktiv gearbeitet haben, werden getrennt und können nach neuem Login sofort weiter arbeiten. Sie merken gar nicht, dass sie nun auf dem anderen System angeloggt sind. Danach kann das zweite System im Hintergrund hochgerüstet werden.

Ähnliches gilt auch für Störungen, die über eine Harddisk Redundanz und eine Server Redundanz hinausgehen. In diesem Fall wird heute eine manuelle Umschaltung des aktiven Systems auf das Standby System durchgeführt. Je nachdem, in welcher Phase und zu welcher Uhrzeit die Störung erkannt wurde, ist entweder ein nahtloser Übergang möglich oder eine Unterbrechung vorhanden.

Heute kann diese Umschaltung nur manuell während der deutschen Arbeitszeiten durchgeführt werden. Ein automatisches Umschalten ist bereits in Planung.

Die Internet Anbindung der Standorte (WAN) basiert auf zwei Anbietern, bei denen wir Platinum Contract (oder vergleichbares) haben. Dies gilt für alle Breitbandverbindungen inklusive SSDP.

Geplante Wartungstätigkeiten:
Wartungstätigkeiten führen innerhalb der RSP zu keinen Ausfällen, da die Standort-umschaltung Wartung im Hintergrund ermöglicht.
SSDP bietet die Möglichkeit der Standortumschaltung nicht. Bis zur endgültigen Abschaltung von SSDP besteht das Risiko, dass bei einer Wartung Anwender betroffen sind.

1.4. Change Management

Änderungen in der RSP stehen unter der Vorgabe, dass der Betrieb für die Anwender keine oder nur geringe Auswirkungen hat. Die entsprechende Planung und Umsetzung von Erweiterungen oder Änderungen sind Aufgabe der für die RSP zuständigen IT Abteilung und möglichst ausserhalb der Bürozeiten durchzuführen. Erweiterungen des Systems durch weitere Server sind im Normalfall auch durch die Möglichkeit der Standortumschaltung ohne Auswirkung auf Anwender möglich.

Es besteht das Risiko, dass während der Hochrüstung des inaktiven RSP Systems im aktiven System ein Problem auftritt. Die Erfahrung hat gezeigt, dass durch die Harddisk Redundanzen und Server Redundanzen noch nie eine Standort-Umschaltung notwendig wurde.

SSDP bietet die Möglichkeit der Standortumschaltung nicht. Bis zur endgültigen Abschaltung von SSDP besteht das Risiko, dass bei einer Änderung Anwender betroffen sind.

Notwendigen Änderungen in der RSP, für SIRA als auch SSDP, werden frühzeitig an die Anwender kommuniziert.

1.5. Service Support

Unify intern übernimmt der Global Service Desk die Level 1 Support Aktivitäten.
Im Partner Business übernimmt der Sales- und Service Partner in der Regel diese Level 1 Support Rolle und eskaliert im Bedarfsfall zu Unify.
Aus Partnersicht übernimmt der **Partner Desk** den Level 2 Support.
Das verwendete Ticket Tool für den Partner ist GSI.flow.

Für eine Weiterverarbeitung auf höherem Level wird das Ticket vom Partner Desk in ITSM umgesetzt. Die höheren Support Level sind durch Unify abgedeckt.

Weitere Details zur Supportkette entnehmen sie bitte der RSP Servicerichtlinie.

1.6. Gegenüberstellung von RSP Systemparametern für IPSec, ISDN, Modem, RSP.servicelink und SSDP:

	IPSec	ISDN	Modem	RSP.servicelink	(SSDP)
Breitband	X	-	-	X	X
Zugang über WTS	X	X	X	X	X
Harddisk-dopplung	X	X	X	X	X
Server-dopplung	X	X	X	X	Tlw.
Standort-dopplung	X	X	X	X	-
Lastverteilung über Loadbalancer	X	X	X	X	X
DB - Mirroring	X	X	X	X	Tlw.
DB - Backup	X	X	X	X	X
Zugriffs-Logging	X	X	X	X	X
Logfile - Mirroring	X	X	X	X	X
VMWare Vcenter	X	X	X	X	-
VMWare redundant	X	X	X	X	-
Netapp NAS Speicher	X	X	X	X	X

Über Unify

Unify ist ein global führendes Unternehmen für Kommunikationssoftware und -services, das für Geschäftskunden von 5 bis über 500.000 Mitarbeitern integrierte Kommunikations- und Kollaborationslösungen weltweit bereitstellt. Unsere Lösungen vereinen unterschiedliche Sprach-, Video- und Datennetzwerke, vernetzte Geräte und Applikationen auf einer einzigen, einfach bedienbaren Plattform, die Teams einen umfassenden und effizienten Austausch ermöglicht – zu jeder Zeit, überall. Damit verändert sich die Art und Weise, wie Unternehmen kommunizieren und zusammenarbeiten, nachhaltig – die Teamleistung wird erhöht, das Geschäft belebt, die Zufriedenheit der Mitarbeiter gesteigert und die Business-Performance verbessert. Unify hat eine lange Tradition aus verlässlichen Produkten und Innovationen gepaart mit offenen Standards und Sicherheit. Unsere Kommunikationslösungen OpenScape und Circuit ermöglichen die nahtlose und effiziente Zusammenarbeit auf jedem Gerät. Unser globales Team aus UCC Experten und Service-Fachleuten setzt gemeinsam Standards für ein einzigartiges Kommunikations- und Kollaborationserlebnis, das Teams zu besseren Ergebnissen verhilft.

Unify.com/de

UNIFY Harmonize your enterprise

unify.com