Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.
Overview

Remote Connectivity Infrastructure
# Remote Connectivity Infrastructure – Table of Contents

- **Introduction**
- **General Architecture**
  - SAProuter
  - Connection Types
- **Main Connection Types in Operation**
- **Remote Connectivity in Operation**
- **IKEv2 migration project**
- **How-to Guide**
- **Summary**
Key Enabler of the Evolution of SAP Support

- Mission critical support and performance
- Total cost of operations
- Continuous Improvement
- Accelerated Innovation
- Cloud and On-Premise

SAP Digital Business Services

Remote Support Infrastructure

Time

Enabling the SAP Control Center Framework for Hybrid Solutions

Innovation Control Center
Build SAP like a factory
- Reduce implementation cost
- Reduce time to value
- Smoothen transition to operations
- Avoid unnecessary modifications
- Integration Validation

Operations Control Center
Run SAP like a factory
- Improve business continuity
- Higher degree of automation
- Better business performance
- Reduce total cost of operations

Mission Control Center
Enhanced Back Office
- Direct access to unmatched expertise from SAP
- Leveraging the entire SAP ecosystem
- Faster issue resolution
General Architecture

Remote Connectivity Infrastructure
Simplified Representation of the SAP Service and Support Architecture

SAP Service and Support Backbone

- SAP Clients
- SAP Proxy
- STFK Low Level Tools
- Remote Connectivity Framework (STFK)
- Launch
- Call Back

Network

- SAProuter
- VPN
- SNC
- Provider
- TCP/SAP NI
- Customer owned VPN

Application Server Farm

- Any Database Server
- SAP Web Application Server
- SAP HANA DB-Server
- WTS Server
- Citrix Server
- Telnet Server
- SSH Server
- SBOB Server
- B1 Server
- Any TCP based server

Customer Back-End
Usage per Primary Remote Service Connection Type

- **SAPSERV1** (Worldwide) VPN
- **SAPSERV2** (Worldwide) SNC
- **SAPSERV3** (EMEA): Service Provider
- **SAPSERV4** (Americas) Service Provider, VPN
- **SAPSERV5** (Japan) Service Provider
- **SAPSERV7** (Asia Pacific) Service Provider, VPN
- **SAPSERV8** (Americas) - planned SNC
- **SAPSERV9** (Asia) SNC
- **SAPSERV10** (China) Service Provider
Customer system data from the SAP Support Portal will be replicated into the SAP Service and Support Backbone.

Remote logon credentials can be easily maintained for each connection within the “Secure Area” in the SAP Support Portal.

SAP provides a detailed logging functionality the so-called “system logbook” in the SAP Support Portal where the customer can see an overview of all remote access related entries for each maintained system.
The SAProuter is a proprietary SAP software product which acts as an application level gateway.

- Operates in the actual logical communication channel between the participating systems.
- It is also used to monitor the communication between the customer server and the associated front-end computers.

Connections between SAProuters can be encrypted.

- It simplifies the configuration of the different connections.
- Multiple SAProuters can be used.
Simplified Representation of the SAP Remote Support Delivery Architecture

- SAP provides approx. 40 different connection types for customers
- Use exactly the type of connection that is required to ensure a secure connection and thereby meet your security requirements
- System connections can be easily maintained and operated in the SAP Support Portal

Customer Back-End
Application Server Farm
- Any Database Server
- SAP Web Application Server
- SAP HANA DB-Server
- WTS Server
- Citrix Server
- Telnet Server
- SSH Server
- SBOB Server
- B1 Server
- Any TCP based server
Remote Connection Types

SAP provides approx. 40 different Remote Connection Types to support our customers with the flexibility they need.
Main Connection Types in Operation

Remote Connectivity Infrastructure
Most Common Connection Types

We provide excellent support for our customers, with over 11 million remote connections in the last year. The ability to connect to almost all of our customers remotely worldwide at any time in a secure and controlled way is a major differentiator for SAP compared to its competitors.

- R/3 Support
  - SAP Note 812732
- HTTP Connect – URL access
  - SAP Note 592085
- Windows Terminal Server
  - SAP Note 605795
- SAP HANA Database
  - SAP Note 1592925
- WTS Connect with NLA
  - SAP Note 1912318
- SSH Connection
  - SAP Note 1275351

The TOP 4 remote connection types which covered more than 95% of all remote connections in 2019.
Remote Connectivity in Operation

Remote Connectivity Infrastructure
Prerequisites for a Remote Connection

In order to remotely connect to customer’s infrastructure, there are some prerequisites that need to be addressed. While availability of master data is part of the migration process, all other steps require actions by the customer.

Prerequisites for remote connection and support:
- Master data must be available (e.g. customer number, contract data, product versions, installation numbers)
- SAProuter must be installed, configured and registered with SAP ([SAP Note 28976](https://apo.sap.com/notes/28976))
- System data must be maintained and/or migrated
  – corresponding SAProuter(s), servers with host / IP address
- Remote connections must be configured
  – services must be activated / booked
  – configured with the right ports and opened
First Steps to Establish a Remote Support Connectivity to SAP (a)

1. Use existing or create a new S-User (see Appendix) for the SAP Support Portal (https://support.sap.com).

2. Select “Tools” → “Connectivity Tools” → “SAProuter” to navigate to the SAProuter installation package.
First Steps to Establish a Remote Support Connectivity to SAP (b)

3. Select the “Download Software” button on the right side of the screen.

4. Get SAProuter Tutorials and How-To-Guides
5. After selecting the “Download Software” button on the previous screen you will be forwarded to the download repository. There you have to select the operation system for which you would like to install to software.
IKEv2 migration

Remote Connectivity Infrastructure
IKEv2 migration – Overview C-Level

The German Federal Office for Information Security (BSI) has released a technical guideline regarding cryptographic mechanisms which consists of recommendations regarding key lengths and other parameters for the use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2).

Based on these recommendations, SAP plans to support our customers to make a timely transition within the next years to utilize IKEv2-based connectivity. Therefore, we already started in late 2018 migrating customers IPsec connections to IKEv2 due to the huge amount of migrations.

IKEv2 has many advantages, to name a few:

- provides better network attack resilience
- increases interoperability between different VPN products
- less overhead
- reduced SA delay
- faster rekey time
IKEv2 migration – Overview technical level

The German Federal Office for Information Security (BSI) has release a technical guideline regarding cryptographic mechanisms which consists of recommendations regarding key lengths and other parameters for the use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2).

Please refer to the BSI website for the IKEv2 technical guideline:
German: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index.htm.html
English: https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/tr02102_node.html

As the migration phase is planned to take at least three years time we would recommend to open an incident on component XX-SER-NET-NEW, to give us better resource planning capabilities and to optimize our support options for this project.

You can also get additional information as well as migration support via this component.
How-to Guide

Remote Connectivity Infrastructure
Communication Paths – CCOE View

**Customer**
Lines of Business

- Maintain system data and remote connections
- Raise incident message at SAP

**Customer**
Customer Center of Expertise / IT

- Initiate remote connection by opening connection / system
- Provide logon credentials in the Customer Remote Logon Depot

**SAP Support Portal**
http://support.sap.com

- Log system opening into system log book which is available to customer
- Log system access into logbook which is available to customer
- Access customer system via remote connection and provided credentials if offline analysis is not sufficient to solve the issue
- Analyze the problem and update the incident message

**SAP Support**
Support Experts

- Log system closing into logbook which is available to customer

Check and implement recommendations to correct the problem

- Close the connection / system
- Close the incident ticket at SAP

Remote Connections

Allow SAP support engineers remote access to your systems, so they can troubleshoot your issues faster.

Your S-user ID requires the Open Remote Connections authorization to manage these remote connections. Check your S-user ID’s existing authorizations, and contact your user administrator if you do not have this authorization.

There are three steps involved in opening a service connection via the SAP Support Portal:

1. Select the system to configure.
2. Set up the required service connection types (done once for each system).
3. Open the required service connection type and specify the time frame for allowing SAP access to the system.

In some circumstances a fourth step is required when the remote network connection is not permanent (see SAP Note 35010).

4. Start the Service Connector (by opening the executable stlkoez file) to open the existing network connection (if it is not already open).
5. If the system SAP is connecting to requires a login, ensure that the Customer Remote Logon Depot is updated with this information.
Maintain Remote Connections (b)

2. Remote Connections Overview:

System

- System Number: 312705611
- System Type: Development system
- Installation Product: SAP NetWeaver
- Installation Name: Internal
- Installation Number: 20270862
- Last Changed By: SAP
- Last Changed On: 13.01.2017
- Created By: SAP
- Created On: 13.01.2017
- Customer Name: SAP AG
- Customer Number: 33018
- Automated Update: Disabled
- System Status: Active

2 Connection Types

- OPENED: 0
- CLOSED: 2
- RESERVED: 0

Semi-Automatic Opening: Off

Manage URLs
Manage LOPs
Logbook
Choose Tools -> Connectivity Tools -> Remote Support. Select the tile “View Logbook”:

- To open / close of accepted service types
- To activate and configure service types

Remote Connections

Allow SAP support engineers remote access to your systems, so they can troubleshoot your issues faster.

Your S-user ID requires the Open Remote Connections authorization to manage these remote connections. Check your S-user ID’s existing authorizations, and contact your user administrator if you do not have this authorization.

There are three steps involved in opening a service connection via the SAP Support Portal:

1. Select the system to configure.
2. Set up the required service connection types (done once for each system).
3. Open the required service connection type and specify the time frame for allowing SAP access to the system.

In some circumstances a fourth step is required when the remote network connection is not permanent (see SAP Note 35010).

4. Start the Service Connector (by opening the executable sfk.oez file) to open the existing network connection (if it is not already open).
5. If the system SAP is connecting to requires a login, ensure that the Customer Remote Logon Depot is updated with this information.
The log can be exported to an excel sheet for further processing via the export button:

- SAP logbook enables the customer to view detailed information's about all remote connectivity activities, like location, access reason, related incident number, and restriction applied for each SID maintained.
- The customer can download the system logbook to create reporting's for example
- SAP support users accessing customer systems will be anonymized in the external logbook as “SAP Support” and “SAP Support 3rd Party”.
System Data Application via SAP Launchpad (a)

Log to SAP’s Support Portal with a registered S-User, then select “Access my launchpad”: 
2. Select “System Data”: 

![System Operations and Maintenance](image-url)
System Data Application in SAP Support Portal (c)

3. After selecting “System Data” you will be forwarded to the system ID overview page, where you can select already maintained systems or create new systems. In our example we select an already maintained system.
4. In this step we have to maintain product related data.
System Data Application in SAP Support Portal Servers (e)

5. In the this step we have to maintain server related data like hostname and IP address.
Learn more about SAP ONE Support Launchpad & Apps

Please visit: https://support.sap.com/en/my-support.html

SAP ONE Support Launchpad

Performing support tasks is simplified by user-centric applications that are accessed through one central entry point: the SAP ONE Support Launchpad. The launchpad provides access to task-driven support resources in an intuitive interface. By using customizable role profiles, it displays only the relevant applications and insights to ensure an efficient and user-friendly experience.

Learn more about generating new S-User IDs to allow your colleagues access to SAP support applications. Browsing our knowledge base for answers to known software issues, reporting incidents when you can’t find a solution, downloading and activating software, enabling SAP support to solve your issues more effectively by sharing the current technical information about your deployment and much more.

Enter the Launchpad
Summary

Remote Connectivity Infrastructure
How You Benefit from the Remote Connectivity Infrastructure

★ Use SAP Support Portal and the SAP Solution Manager application management solution to manage the operational tasks involved in maintaining your SAP software system

★ Use standardized processes for effective incident message processing and gain access to a range of self-help tools that facilitate problem resolution

★ Make use of remote services that contribute to maintaining the technical robustness of your software systems

★ Enable remote analysis of your installations, in order to speed up interaction with support

★ Avoid critical situations by proactively sending information on your system status to SAP

★ Enables you to keep your systems up-to-date