PUBLIC
2020-04-28

Checklist for Support Backbone Update

For SAP Solution Manager 7.2 SPS 5

THE BEST RUN SAP

Content

1 Introduction. 4

2 Step-by-Step Checklist. 5

2.1 Request a Technical Communication User. 6

2.2 Check the Required Kernel Version. 8

2.3 Check and Install CommonCryptoLib. 9

2.4 Check and Adjust the TLS/SSL Protocol Version. 10

2.5 Configure and Activate HTTPS/SSL. 11

2.6 Check the Application Server. 14

2.7 Install SSL Certificates. 15

2.8 Execute Task List `SAP_SUPPORT_HUB_CONFIG`. 16

Check the `SAP-SUPPORT_PORTAL` Connection. 18

2.9 Execute Task List `SAP_BASIS_CONFIG_OSS_COMM`. 19

Check the `SAP-SUPPORT_PARCELBOX` Connection. 20

Check the `SAP-SUPPORT_NOTE_DOWNLOAD` Connection. 21

2.10 Prepare Note Assistant. 22

2.11 Adjust Your User Logon Information. 23

2.12 Finalize Support Hub Connectivity. 25

2.13 Check Jobs Using the New Connections. 26

2.14 Apply Final Corrections. 29

3 Functions and Scenarios Impacted by the Support Backbone Update. 31

Change History

Document Date	Change
2020-04-28	Updated the recommendation regarding `SAPOSS` in Adjust Your User Logon Information [page 23].
2020-02-27	Check Jobs Using the New Connections [page 26] erroneously stated that the job `REFRESH_ADMIN_DATA_FROM_SUPPORT` had been deactivated. This has been corrected to `SEND_SYSTEM_RELATIONSHIP_TO_SUPP`.
2020-02-18	Added information about the discontinuation of jobs `SM:UPLOAD SYSTEM DATA` and `REFRESH_ADMIN_DATA_FROM_SUPPORT`. See Check Jobs Using the New Connections [page 26].
2020-01-27	Updated links to SAP Notes

1 Introduction

The support backbone is the infrastructure that we use to provide you with technical support. Your systems connect to the support backbone to exchange information, such as support incident data, maintenance planner data, and SAP EarlyWatch Alert data.

Due to the increasing demand placed on the support backbone, we have updated the infrastructure so that we can continue to provide you with the support you require. As part of this process, the way in which systems connect to SAP has been redesigned to include the following changes:

- The HTTPS protocol is now used instead of RFC.
- A technical communication user handles the data transfer instead of generic users.
- There is no generic inbound interface.
- Applications send data asynchronously unless the data is sent manually.

To help you transition smoothly to the updated support backbone, the legacy infrastructure will remain in place until January 8, 2020.

This document provides step-by-step tasks to help you retain connectivity to the support backbone after this date.

> ⚠ Caution
>
> This checklist is **not** intended for value-added resellers (VAR) or partners running another multi-customer scenario.

Before you start to work through this checklist, please familiarize yourself with the following information:

- SAP Support Backbone Update: How the SAP Support Backbone Update Affects SAP Solution Manager and Focused Run (including a list of affected SAP Solution Manager scenarios)

2 Step-by-Step Checklist

Before You Begin

We recommend that you work through the configuration steps with a user that has extended basic authorizations, as well as authorizations for SAP Solution Manager Configuration.

For the latest updates to SAP Solution Manager authorizations, see SAP Note 2250709.

> ⚠ Caution
>
> Information about the changes you need to make to connect to the updated support backbone is provided in this checklist, documentation in SAP Solution Manager Configuration (transaction `SOLMAN_SETUP`), and task list documentation in transaction `STC01`. If, despite our best efforts, you find discrepancies between these sources, please treat them with the following order of priority:
>
> 1. This checklist
> 2. Task list documentation
> 3. Documentation in SAP Solution Manager Configuration

If You Need Help

Throughout this document, we provide some hints that you can use to resolve any problems that you may encounter. However, if your system does not run as expected after you have migrated to the updated support backbone, please refer to the central point of call for troubleshooting at Support Hub Connectivity: Guided Answers.

If you have configured all of the settings described in this document but you continue to experience connectivity issues, please open a message on component **SV-SMG-INS-CFG** and prefix your message title with "Backbone Update:" to simplify processing.

If you have a question about the technical infrastructure of the new communication channels, please open an incident on component **XX-SER-NET-HTL**. If you require more background about the relationship between the support backbone and SAP Solution Manager, see Connectivity to SAP's Support Backbone.

Procedure

Use the following overview to work through the steps required to retain communication with the updated support backbone.

1. Request a Technical Communication User [page 6]
   Where: SAP ONE Support Launchpad | **Useful SAP Notes:** 2174416, 2740667, 2805811, 2911301
2. Check the Required Kernel Version [page 8]
   Where: SAP Solution Manager system
3. Check and Install CommonCryptoLib [page 9]
   Where: transaction `STRUST` | **Useful SAP Notes:** 2390726
4. Check and Adjust the TLS/SSL Protocol Version [page 10]
   Where: transaction `RZ11` | **Useful SAP Notes:** 510007
5. Configure and Activate HTTPS/SSL [page 11]
   Where: transaction `SMICM` | **Useful SAP Notes:** 510007
6. Check the Application Server [page 14]
   Where: system OS
7. Install SSL Certificates [page 15]
   Where: transaction `STRUST` | **Useful SAP Notes:** 2631190
8. Execute Task List SAP_SUPPORT_HUB_CONFIG [page 16]
   Where: transactions `STC01`, `SM59` | **Useful SAP Notes:** 2500061, 2454045
9. Execute Task List SAP_BASIS_CONFIG_OSS_COMM [page 19]
   Where: transactions `STC01`, `SM59` | **Mandatory SAP Notes:** 2827658
10. Prepare Note Assistant [page 22]
    Where: transactions `SA38`, `SNOTE` | **Mandatory SAP Notes:** 2576306 | **Important SAP Notes:** 2537133, 2721941, 2836302
11. Adjust Your User Logon Information [page 23]
    Where: transaction `AISUSER` | **Useful SAP Notes:** 2000132, 2174416
12. Finalize Support Hub Connectivity [page 25]
    Where: transaction `SOLMAN_SETUP` | **Useful SAP Notes:** 2525999, 2880549
13. Check Jobs Using the New Connections [page 26]
    Where: transaction `SM37` | **Useful SAP Notes:** 2250709, 2525987
14. Apply Final Corrections [page 29]
    After you have completed the upgrade tasks, there are handful of SAP Notes that you must implement and some related activities to work through.

2.1 Request a Technical Communication User

Where: SAP ONE Support Launchpad | **Useful SAP Notes:** 2174416, 2740667, 2805811, 2911301

Technical communication users allow machine-to-machine communication and data exchange. Only super administrators and user administrators have access to the *Technical Users* app, where they can create, activate, and delete technical communication users.

> **i** Note
>
> Depending on your current release, you may already have at least one technical communication user (although you can request more if required). Technical communication users were introduced with SAP Solution Manager 7.2. They are also occasionally referred to as “technical S-users”, “support hub users”, or “users for support hub communication”.

Make sure that you request your technical communication users in good time. It can take up to 24 hours to receive them.

The number of technical communication users that you require depends on your company policy. It is possible to use one technical communication user for all systems. However, this may lead to connectivity issues if the user gets locked.

> → Recommendation
>
> We recommend that you request one technical communication user per installation / system track (for example, DEV-QAS-PRD). The highest level of flexibility and security can be reached by using one technical communication user per system.

Procedure

1. Request your technical communication user as described in SAP Note 2174416 and create client certificates for it as described in 2805811 (initial creation) and 2911301 (automated renewal).
2. Replace generic users with the technical communication user(s) as instructed in SAP Note Request your technical communication user as defined in SAP Note 2740667.
3. Make sure that you activate your technical communication user as described in SAP Note 2174416.

For a list of frequently asked questions about technical communication users, see the *User Handling* section at Update of SAP's Support Backbone: Frequently Asked Questions (FAQ).

Check

You can check whether your technical communication user has been activated successfully at https://launchpad.support.sap.com/#/techuser.

Your Notes

Parent topic: Step-by-Step Checklist [page 5]

Next: Check the Required Kernel Version [page 8]

Related Information

SAP Note 2174416
Creation and activation of users in the Technical Users application - SAP ONE Support Launchpad

SAP Note 2740667
RFC connection SAPOSS to SAP Service & Support backbone will change (latest) in January 2020

SAP Note 2805811
How to enable client certificate authentication for technical communication users

SAP Note 2911301
SAP Support Portal connection - Renew client certificate of technical S-user

2.2 Check the Required Kernel Version

Where: SAP Solution Manager system

To retain communication with the support backbone, you must make sure that your SAP Solution Manager system is running on the correct kernel version and Support Package level.

Valid kernel versions and Support Package levels are:

- Kernel release 742, Support Package level 401 and above
- Kernel release 745, Support Package level 400 and above
- Kernel release > 745

Procedure

1. In your SAP Solution Manager system, choose *System* > *Status...* .
2. Click (Other kernel info.) or press SHIFT + F5.

Your kernel release and Support Package level are shown in the *Kernel Information* area. If they are below the required levels, patch to the level specified above.

Your Notes

Parent topic: Step-by-Step Checklist [page 5]

Previous: Request a Technical Communication User [page 6]

Next: Check and Install CommonCryptoLib [page 9]

2.3 Check and Install CommonCryptoLib

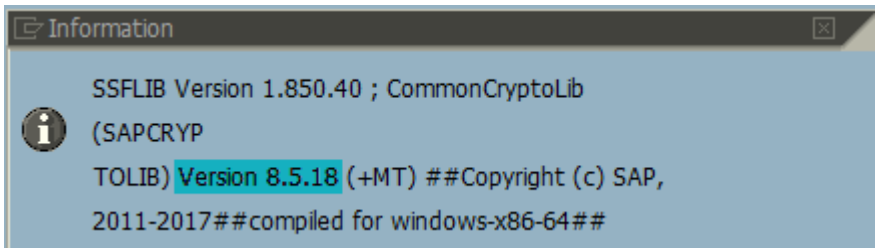
Where: transaction `STRUST` | **Useful SAP Notes:** 2390726

You require at least version 8.4.48 of the CommonCryptoLib library to retain your connection to the support backbone.

> → Recommendation
>
> We recommend that you always upgrade to the latest version of CommonCryptoLib.

Procedure

1. In your SAP Solution Manager system, call transaction **`STRUST`** and choose *Environment* > *Display SSF Version* from the menu.
2. Check the installed version of CommonCryptoLib.



3. If you have to update your version of CommonCryptoLib, go to the Software Downloads area of SAP Support Portal and search for **`CommonCryptoLib`** in the *Support Packages and Patches* area.

For more information, see the *Prerequisites* section of Support Hub Connectivity Configuration in SAP Solution Manager 7.2 SP05 or Higher.

Your Notes

Parent topic: Step-by-Step Checklist [page 5]

Previous: Check the Required Kernel Version [page 8]

Next: Check and Adjust the TLS/SSL Protocol Version [page 10]

Related Information

SAP Note 2390726
Fixes in CommonCryptoLib 8.5.7

2.4 Check and Adjust the TLS/SSL Protocol Version

Where: transaction `RZ11` | **Useful SAP Notes:** 510007

The connection to the support backbone requires SSL protocol version TLS1.1 or higher for outbound HTTP connections. TLS versions 1.0, 1.1, and 1.2 are enabled by the `ssl/client_ciphersuites` parameter value.

To communicate properly with the support backbone, make sure that SSL profile parameter `ssl/client_ciphersuites` for outgoing HTTP connections is set correctly. We recommend a value of `150:PFS:HIGH::EC_P256:EC_HIGH` provided that you have implemented the correction instructions and manual activities in SAP Note 2781565. For detailed, expert information, see SAP Note 510007. You can also use the value `918:PFS:HIGH::EC_P256:EC_HIGH` for SAP Solution Manager (in which case, SAP Note 2781565 is not required). However, this will not work with TLS protocol versions above 1.2.

Also make sure that you are using the most recent version of CommonCryptoLib (8.4.31 or higher).

Check

1. Call transaction **`RZ11`** and enter **`ssl/client_ciphersuites`**.
2. Check that the value of parameter `ssl/client_ciphersuites` is set to `150:PFS:HIGH::EC_P256:EC_HIGH` (unless you have an exceptional use case, in which case refer to the values in SAP Note 510007).

Your Notes

_____
_____
_____
_____
_____
_____
_____
_____

Parent topic: Step-by-Step Checklist [page 5]

Previous: Check and Install CommonCryptoLib [page 9]

Next: Configure and Activate HTTPS/SSL [page 11]

Related Information

SAP Note 510007
Setting up SSL on Application Server ABAP

2.5 Configure and Activate HTTPS/SSL

Where: transaction `SMICM` | **Useful SAP Notes:** 510007

Check that the communication between your Web browser and your SAP Solution Manager system is handled using the HTTPS protocol.

> → Recommendation
>
> Allow yourself plenty of time to complete this step. It may take a few hours.
>
> The connection to the updated support backbone concerns only ABAP systems, although we recommend that you use HTTPS in your Java systems as well.

Most functions in SAP Solution Manager use either BSP or Web Dynpro technologies, which are both based on the HTTP or HTTPS protocols. The infrastructure required to handle HTTP and HTTPS requests using work processes in the SAP system is provided by the Internet Communication Framework (ICF). The ICF also handles Internet communication between systems that use the standard protocols HTTP, HTTPS, and SMTP.

To secure communication with a Web browser, you do not require any additional SAP program libraries. The only condition is that your system platform is able to access the Internet, meaning that you have the greatest amount of flexibility when responding to various communication requirements.

→ Recommendation

For security reasons, always use the secure HTTPS protocol for communication between Web browsers and your SAP systems.

Procedure

1. Check whether HTTPS communication is used in your SAP Solution Manager system in one of the following ways:
   - Check the URL that you use to access SAP Solution Manager applications. If it starts with `https://`, the HTTPS protocol is used in your system.
   - Call transaction **SMICM** and choose *Goto* > *Services* from the menu. Check whether the HTTPS protocol is listed under *Active Services*.

   i Note

   If both HTTP and HTTPS are used in your system, consider using HTTPS only.

   If you want to configure the support backbone connection in a sandbox/test environment, HTTPS is not mandatory and this step can be skipped.
2. If an HTTPS connection is not used, see the *SAP NetWeaver Security Guide* on SAP Help Portal and pay particular attention to the following topics:

   Transport Layer Security
   Configuring SAP NetWeaver AS for ABAP to Support SSL
   Configuring Transport Layer Security on SAP NetWeaver AS for Java
3. After you have configured the HTTPS connection, enter it in *SAP Solution Manager Configuration* (transaction `SOLMAN_SETUP`) in the *System Preparation* scenario. Navigate to the *Check Prerequisites* step and maintain the activity *Check Secure Web Browser Comm. (HTTPS)*.

Using HTTPS in SAP Solution Manager ABAP and Java Only

In your SAP Solution Manager ABAP system, you can use transaction `RZ11` to set the value of parameter `login/ticket_only_by_https` to 1 to make sure that only the HTTPS protocol is used. SAP Solution Manager then also uses HTTPS whenever a “jump-in” URL to the SAP Solution Manager Java system is generated.

However, setting this parameter to 1 may cause inconsistencies when applications submit calls via HTTP (for example, from the SAP Fiori launchpad). To avoid these inconsistencies, open *SAP Solution Manager Configuration* (transaction **SOLMAN_SETUP**) and under **Infrastructure Preparation**, navigate to *Set Up Connectivity* > *Define HTTP Connectivity*. From there, you can specify that only HTTPS is to be used.

Using SAP Web Dispatcher

For information about the protocols used for SAP Web Dispatcher, see SAP Web Dispatcher and SSL.

Table `HTTPURLLOC`

Table `HTTPURLLOC` is automatically updated with the external access URLs that are specified in the *Define HTTP Connectivity* step of the *Infrastructure Preparation* scenario. If you have a special landscape layout and

you want to manually maintain table `HTTPURLLOC`, remember to change the status of the *Update HTTPURLLOC Table* activity to *Manually Performed* (you can find this activity in the *Enable Connectivity* step of the *Infrastructure Preparation* scenario).

For more information, see Configuration Table HTTPURLLOC.

Troubleshooting

For troubleshooting information, see the guided answer Check the SMICM Log.

Your Notes

Parent topic: Step-by-Step Checklist [page 5]

Previous: Check and Adjust the TLS/SSL Protocol Version [page 10]

Next: Check the Application Server [page 14]

Related Information

SAP Note 510007
Setting up SSL on Application Server ABAP

2.6 Check the Application Server

Where: system OS

Make sure that the SAP Solution Manager application server can reach a server outside your network (that is to say, check your network access at OS level). In particular, the following servers must be reachable:

- `apps.support.sap.com`
- `documents.support.sap.com`
- `notesdownloads.sap.com`
- `servicepoint.sap.com`

External access can be managed in any of the following ways:

- The application server has direct access to the Internet via HTTPS
- The application server has indirect access to the Internet via HTTPS and a Web proxy.
- The application server has indirect access to external networks via HTTPS and the SAP proxy “SAProuter”.

For more information, see the guided answer Check All Prerequisites.

Your Notes

Parent topic: Step-by-Step Checklist [page 5]

Previous: Configure and Activate HTTPS/SSL [page 11]

Next task: Install SSL Certificates [page 15]

2.7 Install SSL Certificates

Where: transaction `STRUST` | **Useful SAP Notes:** 2631190

Context

The following certificates are required for the support backbone:

- VeriSign Class 3 Public Primary Certification Authority - G5
- DigiCert Global Root CA
- DigiCert Global Root G2
- DigiCert High Assurance EV Root CA

Procedure

1. Call transaction **`STRUST`** and check that *SSL client SSL Client (Standard)* and *SSL client SSL Client (Anonymous)* are correct.
2. Check that the status is green and that all of the above certificates are present for both the anonymous and standard PSEs. If this is the case, no futher action is required. Otherwise, proceed with step 3 [page 15].
3. Download the required certificates from SAP Note 2631190.
4. In transaction `STRUST`, choose *Certificate* > *Import* to add the certificates to *SSL client SSL Client (Standard)* and *SSL client SSL Client (Anonymous)*.

Task overview: Step-by-Step Checklist [page 5]

Previous: Check the Application Server [page 14]

Next: Execute Task List SAP_SUPPORT_HUB_CONFIG [page 16]

Related Information

SAP Note 2631190
Download location of SSL certificates required for Support Hub Connectivity configuration

2.8 Execute Task List SAP_SUPPORT_HUB_CONFIG

Where: transactions STC01, SM59 | **Useful SAP Notes:** 2500061, 2454045

Task list SAP_SUPPORT_HUB_CONFIG contains a number of tasks, some of which you may have already set up. In this case, you can use the task list to check your setup.

The task list also creates connection SAP-SUPPORT_PORTAL, which is required for the updated support backbone. Other required connections are created by task list SAP_BASIS_CONFIG_OSS_COMM.

All of the relevant information is provided in the task list itself.

> **i** Note
>
> The user and password defined in this task list must be correct. User RFC_OSS is no longer supported for any of the new connections. Make sure that you have the correct users and that they are correctly assigned.
>
> Use your technical communication user **only** for communication with the support backbone. Do not use it for any other connections. If you try to log in to a system such as SAP ONE Support Launchpad using the technical communication user, you risk locking it.
>
> If you change the password, wait for 30 minutes so that the new password can be propagated to all of the relevant SAP systems. During this time, avoid testing the channels, starting jobs, and uploading data (for example, via LMDB). The technical communication user will be locked after five failed logon attempts.
>
> If your technical communication user does become locked ("SAP service point ping error: 401 Unauthorized"), please see SAP Note 2392726 for instructions on how to unlock it.

Procedure

1. Call transaction **STC01**.
2. Enter the name of the task list.
3. Run all of the activities described here.
4. Call transaction **STC02** to check that the task list ran successfully.

For more information, see How to Configure the Step "Support Hub Connectivity" in SAP Solution Manager 7.2 as of SP05.

Troubleshooting

For information about changing the technical communication user, password, SAProuter string, or proxy settings for the support backbone, see this guided answer.

General troubleshooting information is available at Configuration: Support Hub Connectivity. For specific errors, refer to the table below.

Issue	Check
The step “Check connectivity and credentials to SAP Support Portal” fails with the error message `HTTP ERROR 401 : Unauthorized (SP05)` or `SAP service point ping error : 401 Unauthorized (SP06)`.	See the guided answer at Check the Possible Root Causes.
The step “Check connectivity and credentials to SAP Support Portal” fails with the error message `SAP portal connection error 404 : Proxy Connection Refused`.	See the guided answer at Check if Relevant HTTP Proxy or SAProuter Is Reachable from SAP Solution Manager 7.2.
The step “Check connectivity and credentials to SAP Support Portal” fails with the error message `SAP portal connection error 500 : SSL Peer Certificate Untrusted`.	See the guided answer at Check the Certificate SSL Client (Anonymous) in Transaction STRUST.
RFC destination and connection type are incorrect in the documentation.	See the guided answer at Documentation Errors in Help Text of the Task List in Transaction STC01 in SAP Solution Manager 7.2 SP05.
All applications that use a synchronous communication channel return an error message even though configuration was successful.	See the guided answer at Delete the Value in Field Path Prefix in HTTP Destination SAP-SUPPORT_PORTAL and Save the Entry.

Your Notes

Parent topic: Step-by-Step Checklist [page 5]

Previous task: Install SSL Certificates [page 15]

Next: Execute Task List SAP_BASIS_CONFIG_OSS_COMM [page 19]

Related Information

SAP Note 2500061

Support Hub Connectivity: Configuration Steps in SAP Solution Manager 7.2 as of SP05

SAP Note 2454045
Support Hub Connectivity configuration in Solution Manager 7.2 SP05 or higher - Guided Answer

2.8.1 Check the SAP-SUPPORT_PORTAL Connection

After you have executed task list SAP_SUPPORT_HUB_CONFIG, connection SAP-SUPPORT_PORTAL (*HTTP Connection to ABAP System* [type H]) should be fully operational. You can verify this in transaction SM59.

Procedure

1. Call transaction SM59 and open the connection SAP-SUPPORT_PORTAL.
2. Enter the path prefix **/sap/bc/bsp/svt/sapping** and run the connection check.
3. If the check is successful, delete the prefix from the connection and reenter the credentials for the technical communication user.

Troubleshooting

Issue	Check
You test destination SAP-SUPPORT_PORTAL or ping the Web service for the asynchronous channel in SOAMANAGER and you get the error `407 Proxy Authentication Required`.	See the guided answer at Check the Proxy Settings and Password.
Although the support hub channels were configured successfully, the connection test for destination SAP-SUPPORT_PORTAL finished with HTTPIO_PLG_CANCELED.	See the guided answer at Activate the HTTPS Service.
Access to target host `servicepoint.sap.com` fails with the error `SAP service point ping error : 404 Connection Refused`.	See the guided answer at Ensure That SAProuter String Was Entered and Is Correct.
When you enter the password for the proxy user, it is automatically converted into uppercase or shown in plain text.	See SAP Note 2525999.
When destination SAP-SUPPORT_PARCELBOX is created via the task list, the proxy parameters are incorrect and the connection test fails during the task list run, no matter which parameter you specify.	See SAP Note 2722769.
The task *Check connectivity and credentials to SAP Support Portal* returns the error `SAP Support Documents channel ping failed`.	See SAP Note 2735772.

Issue	Check
Access to target hosts `servicepoint.sap.com` or `apps.support.sap.com` fails with the error `NIECONN_REFUSED(-10)`.	See the guided answer at Ensure That SAProuter String Was Entered in STC01.

Your Notes

2.9 Execute Task List `SAP_BASIS_CONFIG_OSS_COMM`

Where: transactions `STC01`, `SM59` | **Mandatory SAP Notes:** 2827658

Task list `SAP_BASIS_CONFIG_OSS_COMM` contains a number of tasks, some of which you may have already set up. In this case, you can use the task list to check your setup.

The task list also creates connections `SAP-SUPPORT_PARCELBOX` and `SAP-SUPPORT_NOTE_DOWNLOAD`, which are required for the updated support backbone. Other required connections are created by task list `SAP_SUPPORT_HUB_CONFIG`.

> **i** Note
>
> Make sure that you have implemented SAP Note 2827658 to include this task list in your system.

Make sure that you run the activity *Create/Test HTTPS Connections for SAP Services (SM59)*.

Procedure

1. Call transaction **`STC01`**.
2. Enter the name of the task list.
3. Run all of the activities described here.
4. Call transaction **`STC02`** to check that the task list ran successfully.

Troubleshooting

For information about changing the technical communication user, password, SAProuter string, or proxy settings for the support backbone, see this guided answer.

Your Notes

_____
_____
_____
_____
_____
_____
_____
_____

Parent topic: Step-by-Step Checklist [page 5]

Previous: Execute Task List SAP_SUPPORT_HUB_CONFIG [page 16]

Next: Prepare Note Assistant [page 22]

Related Information

SAP Note 2827658
Automated Configuration of new Support Backbone Communication - Update 02

SAP Note 2815061
HTTP Response 404 for Digitally Signed SAP Notes' RFCs

SAP Note 2820957
Destinations SAP-SUPPORT_PARCELBOX and SAP-SUPPORT_NOTE_DOWNLOAD giving error 401 Unauthorized

2.9.1 Check the `SAP-SUPPORT_PARCELBOX` Connection

After you have executed task list `SAP_BASIS_CONFIG_OSS_COM`, connection `SAP-SUPPORT_PARCELBOX` (*HTTP Connection to External Serv.* [type G]) should be fully operational. You can verify this in transaction `SM59`.

Procedure

1. Call transaction SM59 and open the connection SAP-SUPPORT_PARCELBOX.
2. Check that the path prefix **/parcel/** is entered and run the connection checks.

Your Notes

2.9.2 Check the SAP-SUPPORT_NOTE_DOWNLOAD Connection

After you have executed task list SAP_BASIS_CONFIG_OSS_COM, connection SAP-SUPPORT_NOTE_DOWNLOAD (*HTTP Connection to External Serv.* [type G]) should be fully operational. You can verify this in transaction SM59.

Procedure

1. Call transaction SM59 and open the connection SAP-SUPPORT_NOTE_DOWNLOAD.
2. Enter the path prefix **/note/0040000000874972019** and run the connection check.
3. If the check is successful, delete the prefix from the connection and reenter the credentials for the technical communication user.

Your Notes

2.10 Prepare Note Assistant

Where: transactions `SA38`, `SNOTE` | **Mandatory SAP Notes:** 2576306 | **Important SAP Notes:** 2537133, 2721941, 2836302

> **i** Note
>
> This section applies only to systems to which you want to download SAP Notes (such as development or quality assurance environments). If you are transporting SAP Notes to your SAP Solution Manager system, this section is not relevant.

With the updated support backbone, downloading SAP Notes no longer uses RFC connection `SAPOSS`. Instead, the SAP NetWeaver Download Service is used. This service supports the automated download of TCIs (transport-based correction instructions), including any prerequisite SAP Notes to the SAP Note you want to download.

Procedure

To implement the SAP NetWeaver download service, proceed as follows:

1. Configure Note Assistant to use the SAP NetWeaver download service as described in SAP Note 2537133.
2. In your SAP Solution Manager system, execute report `RCWB_UNSIGNED_NOTE_CONFIG` and select the option *Do not download unsigned SAP Note*.

Check

Check that Note Assistant connects to the updated support backbone via the download service by running the report *Defining Procedure for Downloading SAP Note* (`RCWB_SNOTE_DWNLD_PROC_CONFIG`). Check that the option *Download Service Application* is selected. If either of the other options is selected, return to the procedure and check your configuration.

> **i** Note
>
> Changing the setting of the radio button in report `RCWB_SNOTE_DWNLD_PROC_CONFIG` is not sufficient. You must go back to the procedure and set up Note Assistant correctly.

> **→** Tip
>
> Regardless of which procedure you use to download SAP Notes, you can check the log of the downloaded SAP Note to see whether it is digitally signed. The log also includes the procedure that was used for the download.

Your Notes

Parent topic: Step-by-Step Checklist [page 5]

Previous: Execute Task List SAP_BASIS_CONFIG_OSS_COMM [page 19]

Next: Adjust Your User Logon Information [page 23]

Related Information

SAP Note 2537133
FAQ - Digitally Signed SAP Notes

SAP Note 2576306
Transport-Based Correction Instruction (TCI) for Download of Digitally Signed SAP Notes

SAP Note 2721941
Download of digitally signed note - changes to configuration report and other minor changes

SAP Note 2836302
Automated guided steps for enabling Note Assistant for TCI and Digitally Signed SAP Notes

2.11 Adjust Your User Logon Information

Where: transaction `AISUSER` | **Useful SAP Notes:** 2000132, 2174416

An S-user is a user in the support backbone with actual authorizations and must be assigned to SAP Solution Manager system users in table `AISUSER`, specifically to the users `SOLMAN_BTC`, `SOLMAN_ADMIN`, and `SAPSUPPORT`. This will allow the assigned system users to perform specific activities with the support backbone (such as sending an incident to SAP).

> **i** Note
>
> Table `AISUSER` contains your S-user, not your technical communication user. The technical communication user is intended only to establish the connection to the support backbone, and does not have any authorizations itself.

Procedure

1. Call transaction **AISUSER** and check that the correct contact person (S-user number) is correctly assigned to the users `SOLMAN_BTC`, `SOLMAN_ADMIN`, and `SAPSUPPORT`.
2. If the contact person is incorrect, enter the correct S-user.

> → Recommendation
>
> Most of the RFC destinations that were previously used to connect to the support backbone are now superfluous. After you have updated the destinations, we recommend that you disable or remove all of the RFCs that are no longer required. For example, you can disable or remove `SAP-OSS`, `SAP-OSS-LIST-001`, `SAPNET_RTCC`, `SDCC_OSS` and even `SAPOSS`. (`SAPOSS` is being been kept alive through July 2020 as an emergency fallback RFC destination; its continued use is, however, no longer recommended because of its imminent expiry.)
>
> The status column indicates whether the destinations are active. Inactive destinations are shown with a red traffic light; removed destinations are not shown at all.

Your Notes

Parent topic: Step-by-Step Checklist [page 5]

Previous: Prepare Note Assistant [page 22]

Next: Finalize Support Hub Connectivity [page 25]

Related Information

SAP Note 2000132
Configuring RFC connections to the SAPNet R/3 front end (OSS) correctly

SAP Note 2174416
Creation and activation of users in the Technical Users application - SAP ONE Support Launchpad

Secure Configuration Security Guide

2.12 Finalize Support Hub Connectivity

Where: transaction `SOLMAN_SETUP` | **Useful SAP Notes:** 2525999, 2880549

"Finalize Support Hub Connectivity" is an automatic activity in SAP Solution Manager Configuration. It creates logical ports and checks whether the communication channels (both synchronous and asynchronous) are operational. Specifically, it creates logical port `LP_SISE_SUPPORTHUB` for the following consumer proxies:

- `CO_SISEHUB_MI_O_AS_PUT_EXTERNA`
- `CO_SISEHUB_MI_O_S_SHB_GET_EX`
- `CO_SISEHUB_MI_O_S_SHB_LIST`
- `CO_SISEHUB_MI_O_S_SHB_REMOVE`

Procedure

1. Open SAP Solution Manager Configuration (transaction **`SOLMAN_SETUP`**) and navigate to step 3.2 (*Support Hub Connectivity*) in the *System Preparation* scenario.
2. Execute the automatic activity *Finalize Support Hub Connectivity*.

Check

1. Open SOA Management (transaction **`SOAMANAGER`**) and click *Web Service Configuration*.
2. Change the selection filter for the object name from *is* to *contains* and search for object names that contain **`*HUB*`**.
   The search returns the consumer proxies mentioned above.
3. Click each of the consumer proxies in turn to open their details and ping logical port `LP_SISE_SUPPORTHUB` by clicking  (*Ping Web Services*).

For more information, see How to Check the Asynchronous Channel.

Troubleshooting

For troubleshooting information, see Error Messages in Task "Check Connectivity and Credentials to SAP Support Portal".

Your Notes

Parent topic: Step-by-Step Checklist [page 5]

Previous: Adjust Your User Logon Information [page 23]

Next: Check Jobs Using the New Connections [page 26]

Related Information

SAP Note 2525999
Proxy password converted to uppser case and shown in plain text in task list SAP_SUPPORT_HUB_CONFIG

SAP Note 2522789
How to check error ' Web service ping failed for logical port LP_SISE_SUPPORTHUB ' in Solution Manager 7.2 as of SP05

SAP Note 2880549
RFC Connectivity is displayed with red light

2.13 Check Jobs Using the New Connections

Where: transaction `SM37` | **Useful SAP Notes:** 2250709, 2525987

User `SOLMAN_BTC` runs a number of jobs that connect to the support backbone. These are:

Job Name	Job Frequency	Relevant for Systems...
`REFRESH_ADMIN_DATA_FROM_SUPPORT`	Daily	Production only
`SEND_SYSTEM_RELATIONSHIP_TO_SUPP`	Daily	All
`SERVICE_CONNECTION_LISTENER`	Every minute	Production only
`SM:AGS_SISE_SUPHUB_OUTBOX_PROCES`	Hourly	All
`SM:EXEC SERVICES`	Daily	All
`SM:GET_PPMS_DATA_FROM_OSS`	Daily	Production only

Job Name	Job Frequency	Relevant for Systems...
SM:GET CSN COMPONENTS	Weekly	Production only
SM:LMDB GENERIC UPLOAD	Hourly	Production only
SM:LONG FILE EXT DOWNLOAD	Weekly	Production only
SM:RCD_CHECK_UPDATES	Weekly	All
SM:REFRESH MESSAGE STATUS	Hourly	Production only
SM:SELFDIAGNOSIS	Daily	All
SM:SELFDIAGNOSIS_SEND_TO_SAP	Monthly	All
SM:SERVICE_CONNECTION_MIGRAT_SP7	Run once only	All
SM:SERVICE CONTENT UPDATE	Daily	All
SM:SYNC SAP SESSIONS	Daily	All
SM:SYNC SERVICE REQUESTS	Hourly	Production only
SM:SYSTEM RECOMMENDATIONS	Weekly	All
SM:TOP ISSUE TRANSFER	Daily	Production only
SM:UPDATE RULES	Daily	All
SM:UPLOAD SYSTEM DATA	Daily	All

> **i Note**
>
> The background job SM:UPLOAD SYSTEM DATA has been deactivated as of January 27, 2020. For more information, see SAP Note 2863831. Tasks that were handled by this job are now handled by job SM:LMDB GENERIC UPLOAD.
>
> Background job SM:REFRESH_RFCDEST (not listed above) is now completely obsolete (see SAP Note 894279) and can be deleted (using transaction SM37).

Procedure

1. Even though you are using a lower Support Package Stack, update role SAP_SM_BATCH as specified in SAP Note 2250709.

Check

1. Call transaction **SM37** and make sure that there are no errors or references to old destinations in the logs for the jobs mentioned above.
   Note that some jobs use legacy destinations (such as SAPOSS) as a fallback if communication with SAP fails using a new destination. The overall status of a job can therefore be misleading, and so we recommend that you check the job logs and not just the overall status of a job in SM37.

2. If a job runs infrequently and a scheduled run hasn't taken place since you migrated your system to the updated support backbone, wait for the first scheduled run to take place and then check your system.

Troubleshooting

Issue	Check
General issues regarding the job log.	See the guided answer at Check the Job Log.
When you check the response from SAP, the job fails with the message `Internal Server Error SRT_CORE 122` or `Timeout error (ICM_HTTP_TIMEOUT).`	See SAP Note 2525987.
Logical port `LP_SISE_SUPPORTHUB` isn't available for proxy class `CO_SISEHUB_MI_O_S_SHB_LIST`	See SAP Note 2665368.

Your Notes

Parent topic: Step-by-Step Checklist [page 5]

Previous: Finalize Support Hub Connectivity [page 25]

Next: Apply Final Corrections [page 29]

Related Information

SAP Note 2250709
Solution Manager 7.2: End-User Roles and Authorizations Corrections as of SP01 and higher

SAP Note 2525987
Internal Server Error, SoapFaultCode:5 Server Error or Timeout error (ICM_HTTP_TIMEOUT) in jobs using the asynchronous channel

2.14 Apply Final Corrections

After you have completed the upgrade tasks, there are handful of SAP Notes that you must implement and some related activities to work through.

Service Data Control Center (SDCCN) – Universally Relevant (for Example, for SAP EarlyWatch Alert)

You cannot update to the new support backbone infrastructure on ST-PI plug-in levels lower than ST-PI 740 SP09 (equivalent to ST-PI 2008_1_[700-710] SP19) and ST-A/PI plug-in levels lower than ST-A/PI 01T* SP01. Once your SAP Solution Manager systems are on sufficiently high plug-in versions, proceed as follows.

If your SAP Solution Manager 7.2 SP 5 system is running together with ST-PI 740 SP11, implement the following SAP Note:

2802999 – *SDCCN activation fails without errors or red icons in Migrate tab*

Then call transaction **SDCCN** and check whether the *Migrate* tab appears. If so, follow the instructions there.

If your SAP Solution Manager 7.2 system is running together with ST-PI 740 SP09 or SP10, see New communication channel to SAP Backbone for transaction SDCCN and follow the instructions for your Support Package.

Also implement SAP Notes 2760811 (*Self Diagnosis: Alert 025 gives wrong alert after migrated SDCCN to new Support Hub*) and 2744825 (*Self-Diagnosis: Alert 211 - Changes for SDCC_OSS Shutdown*) to avoid false positives in the SAP Solution Manager Self-Diagnosis framework.

Service Content Update – Universally Relevant

This application ensures that the contents of SAP's services and monitoring infrastructure remain up-to-date and secure. Deploy the correction to it by implementing the following SAP Notes:

- 2714210 – *New communication channel to SAP Backbone for Service Content Update*
- 2722875 – *Recommended corrections to resolve issues with the new communication channel in Service content update*

Parent topic: Step-by-Step Checklist [page 5]

Previous: Check Jobs Using the New Connections [page 26]

Related Information

SAP Note 2880999

SAP Backbone connectivity update - Alert 00188 in Self-Diagnosis is no longer valid

3 Functions and Scenarios Impacted by the Support Backbone Update

For information about the functions and scenarios that are affected by the update to the support backbone, see the section *Which SAP Solution Manager scenarios are impacted?* at SAP Support Backbone Update.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP