ABSTRACT

Installation Guide

AWS CONNECTOR FOR SAP

Table of Contents

PREREQUISITES 3

ACTIONS TO DO IN AWS 3

CLOUDFORMATION. 3

ACTIONS TO DO IN SAP. 7

DOWNLOAD ADD-ON 7
LOGON TO CLIENT 000. 7
SAINT 7
CHECK HTTPS SERVICE. 22
STRUST 22
FIRST RUN OF /LNKAWS/AWS_STRUST. 22
PROGRAMMING JOB /LNKAWS/AWS_STRUST. 29
SICF, SERVICE AWSCONNECTOR_S3 34
AUTHORIZATIONS DETAILS 35

ACTIONS TO DO IN AWS CONNECTOR MANAGER 40

CREDENTIALS. 42
CREATE BUCKET. 42
SSF CONFIGURATION. 45
CONFIGURATION OF YOUR OWN SSL CERTIFICATE 46
MONITORING SETTINGS (SCMSMO) 51

CONCLUSION 55

REVISIONES

Versión	Autor	Fecha
v1.0	Linke – Gerard Lagalina	01/05/2019

Prerequisites

To run AWS Connector in your SAP system, following prerequisites should be met:

- SAP Netweaver 7.0 or higher (SAP_BASIS 700 0028 SAPKB70028)
- SAP Kernel release 720 or higher
- SAP Cryptolib properly installed
- System configured properly to run ABAP Webdynpros (check OSS note 1088717 and mind the host file)
- ICM Services HTTP and HTTPS configured and active
- Connectivity to the Internet (either directly or through a Proxy properly configured).
- To install the add-on, a user with enough privileges (please read Authorizations).

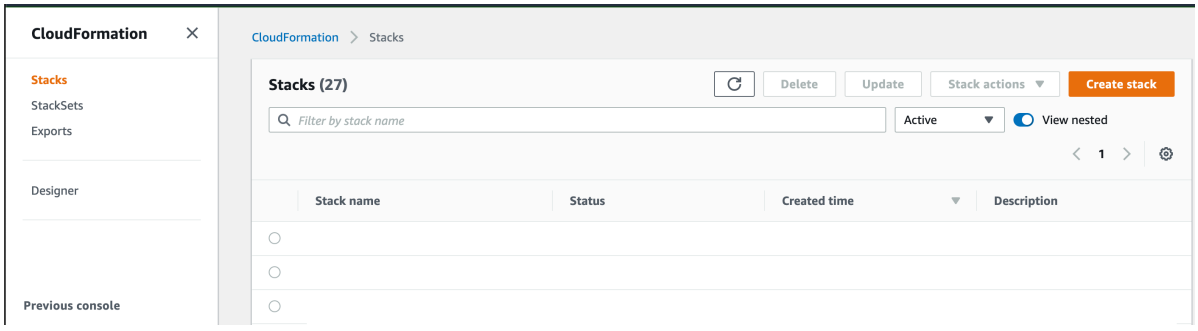
Actions to do in AWS

CloudFormation.

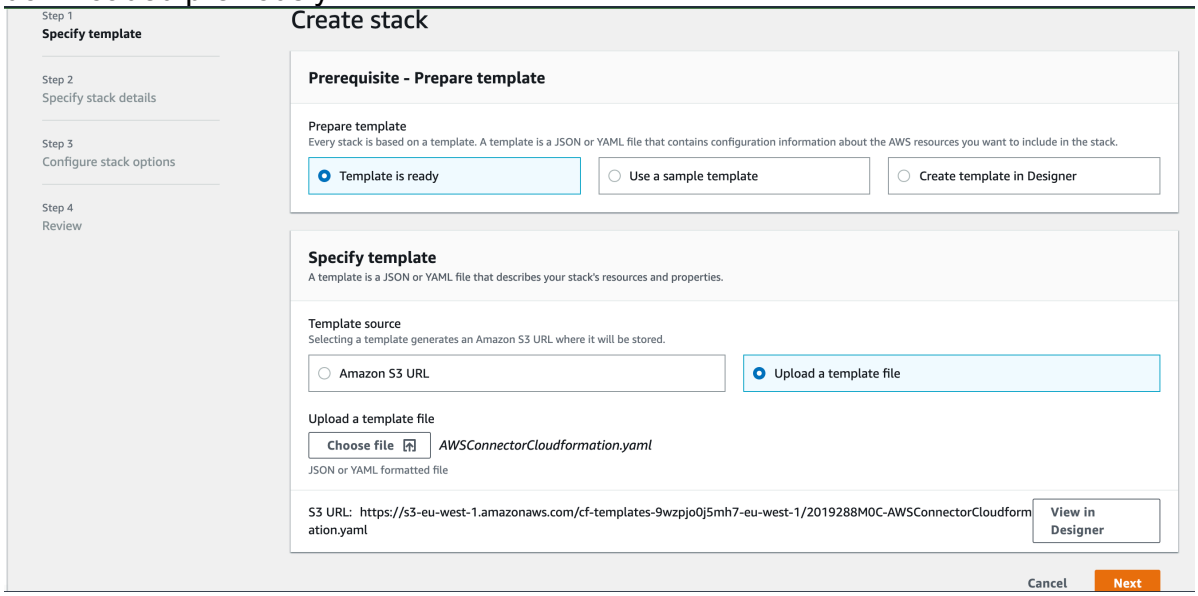
First step is download the CloudFormation Template from this link:

https://s3-eu-west-1.amazonaws.com/docs.linkeit.com/repo/awsconnector/AWSConnectorCloudformation.yaml

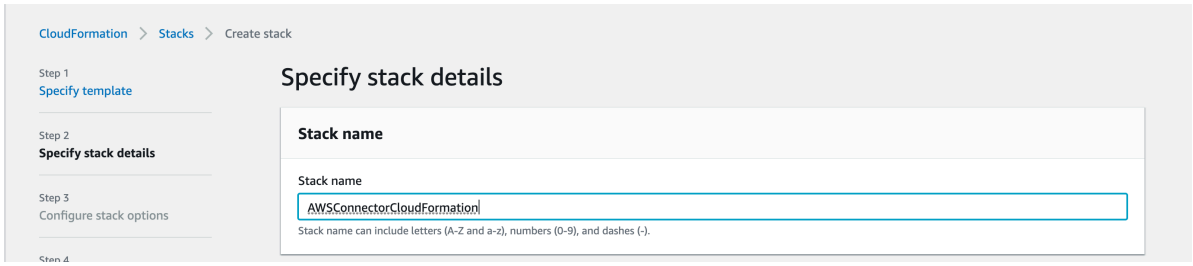
Go to the CloudFormation services on AWS console and press the Create stack Button.



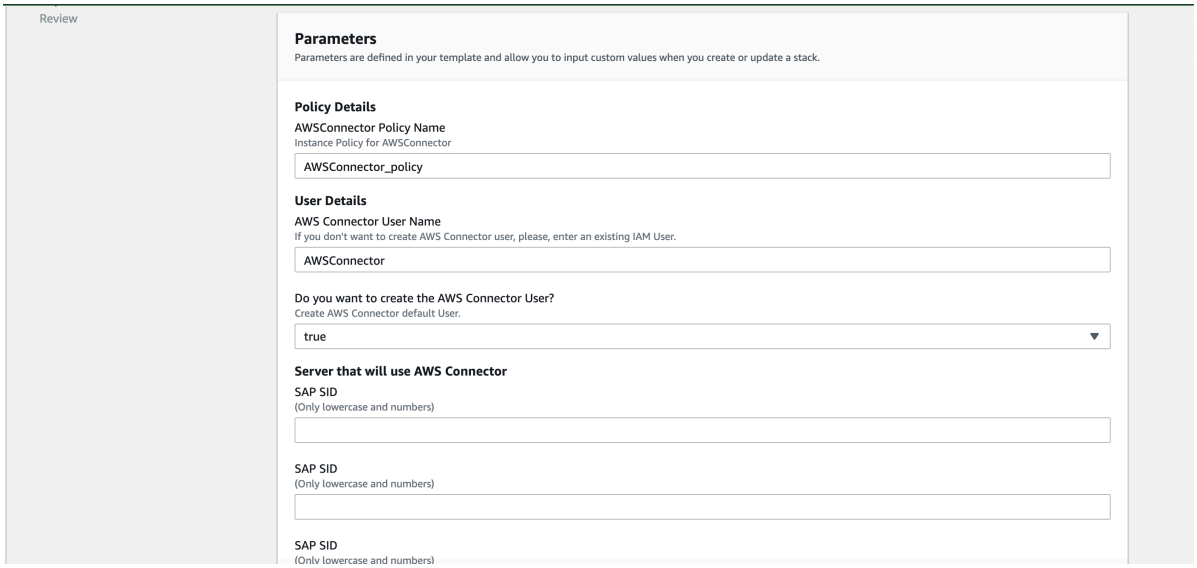
In prepare template select the option “Template is ready”.
in specify template menu, select the “upload a template file” and chose the yaml file downloaded previously.



In specify stack details menu, insert name “AWSConnectorCloudFormation” in field stack name.



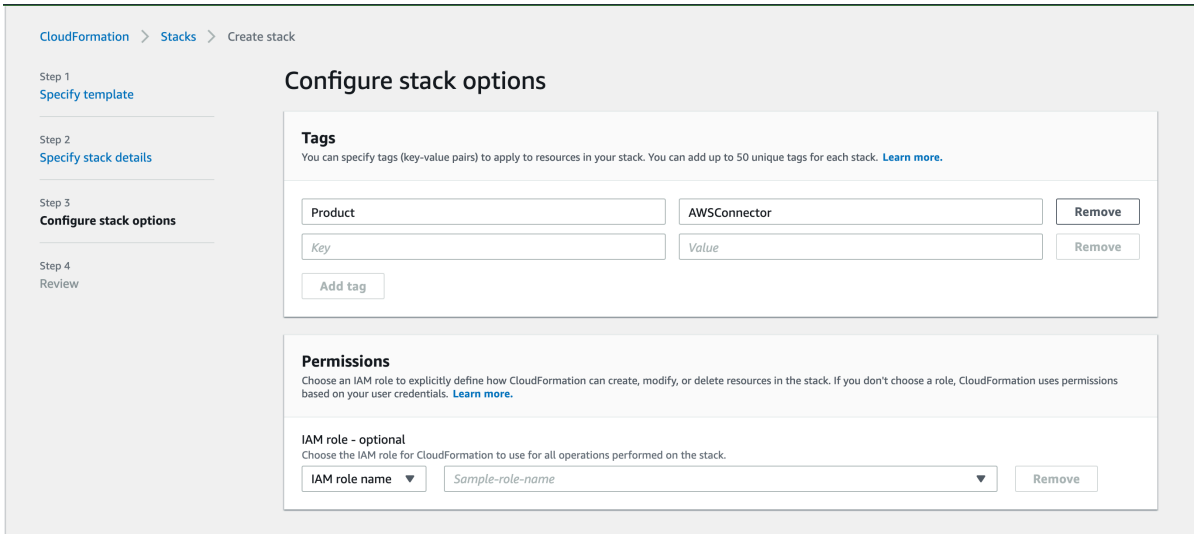
In parameters menu, insert SAP SID value (only lowercase and numbers).



Add one tag with these values:

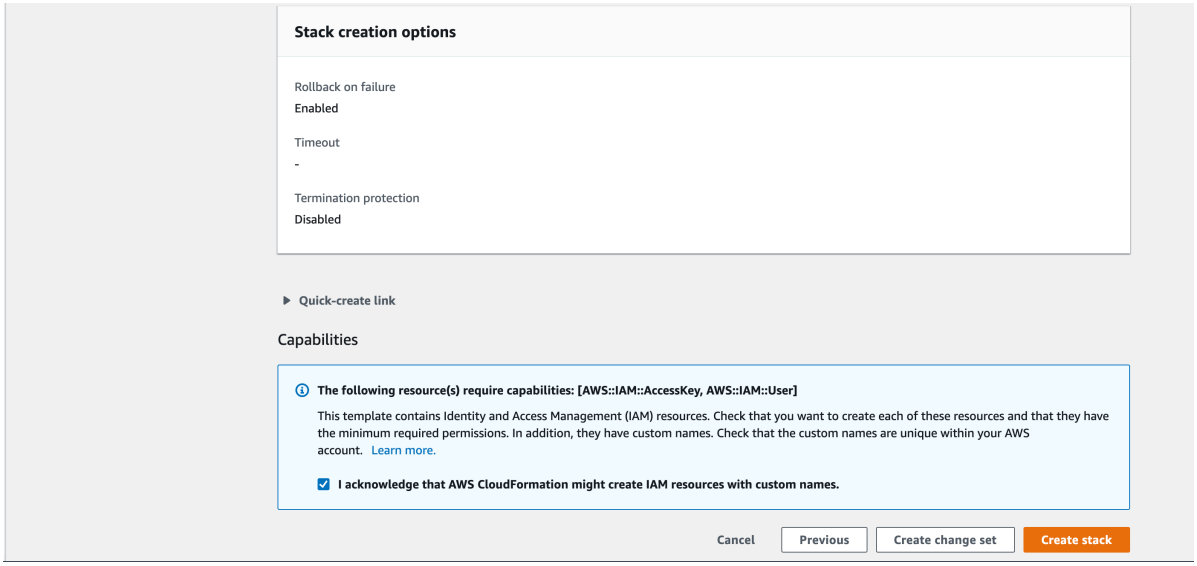
Key = Product

Value = AWSConnector

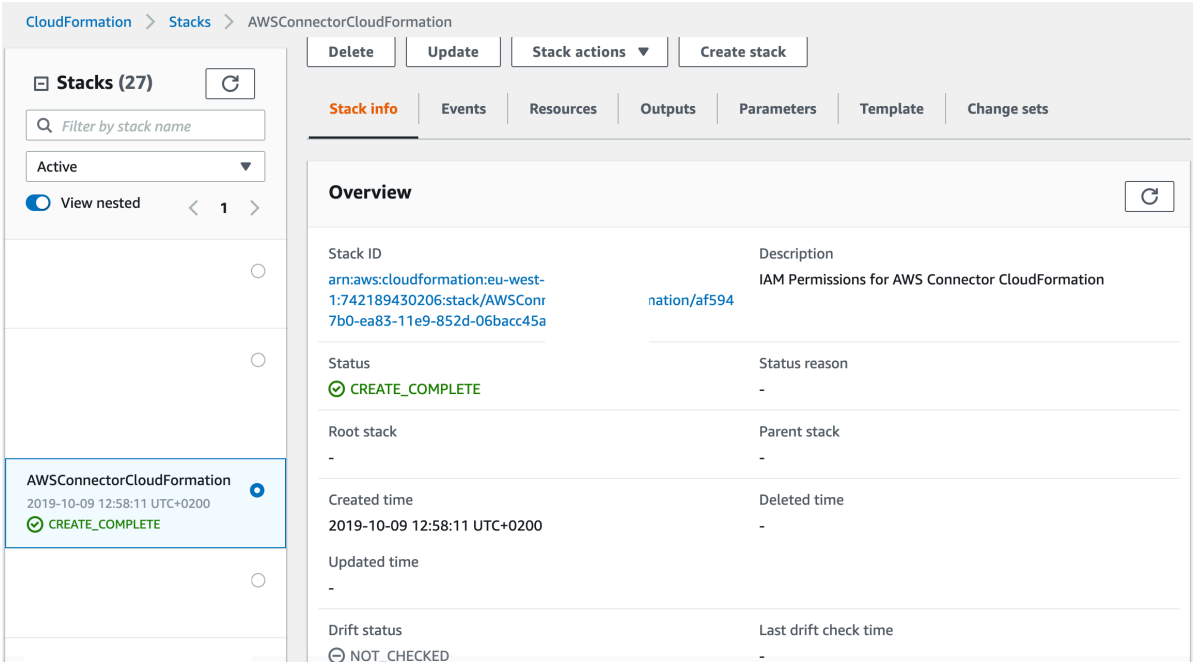


In Review AWSConnectorCloudFormation step, check the option “I acknowledge that AWS CloudFormation might create IAM resources with custom names.”.

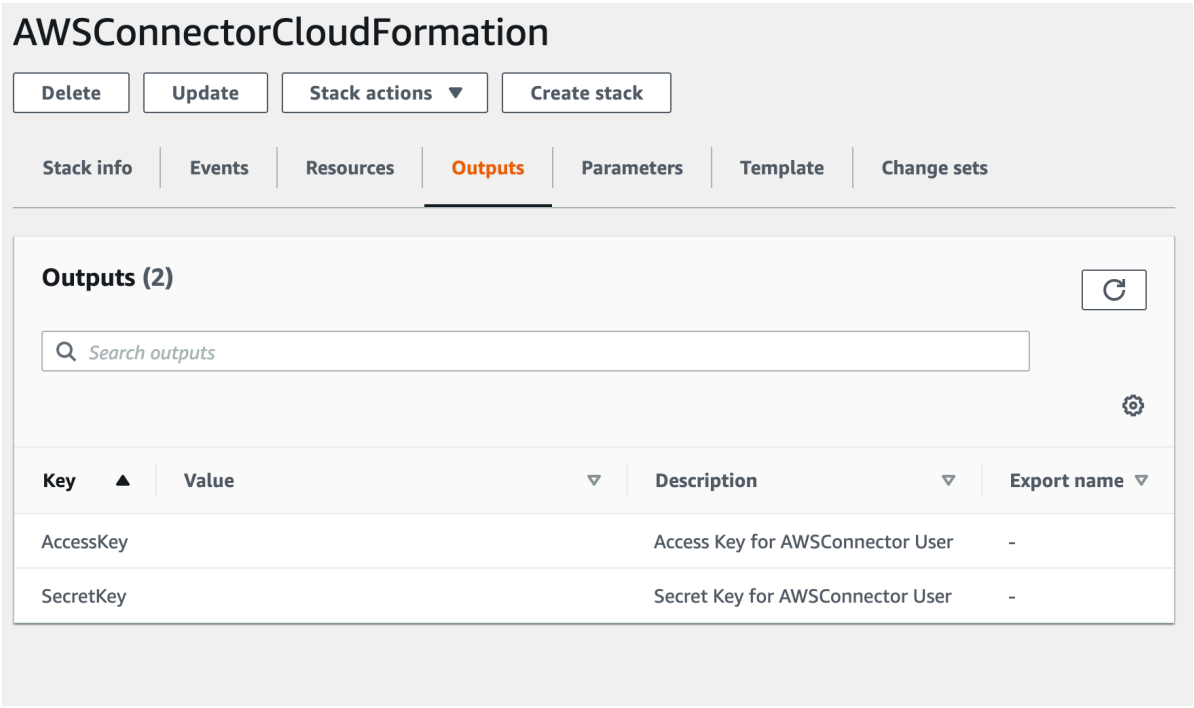
Press “create stack” button.



When the stack is created successfully a screen similar to this will be displayed.



In Outputs menu, you can see the AccessKey and the SecretKey. These keys should be used later in credentials tab on AWS Connector management transaction.



Actions to do in SAP.

Download Add-on.

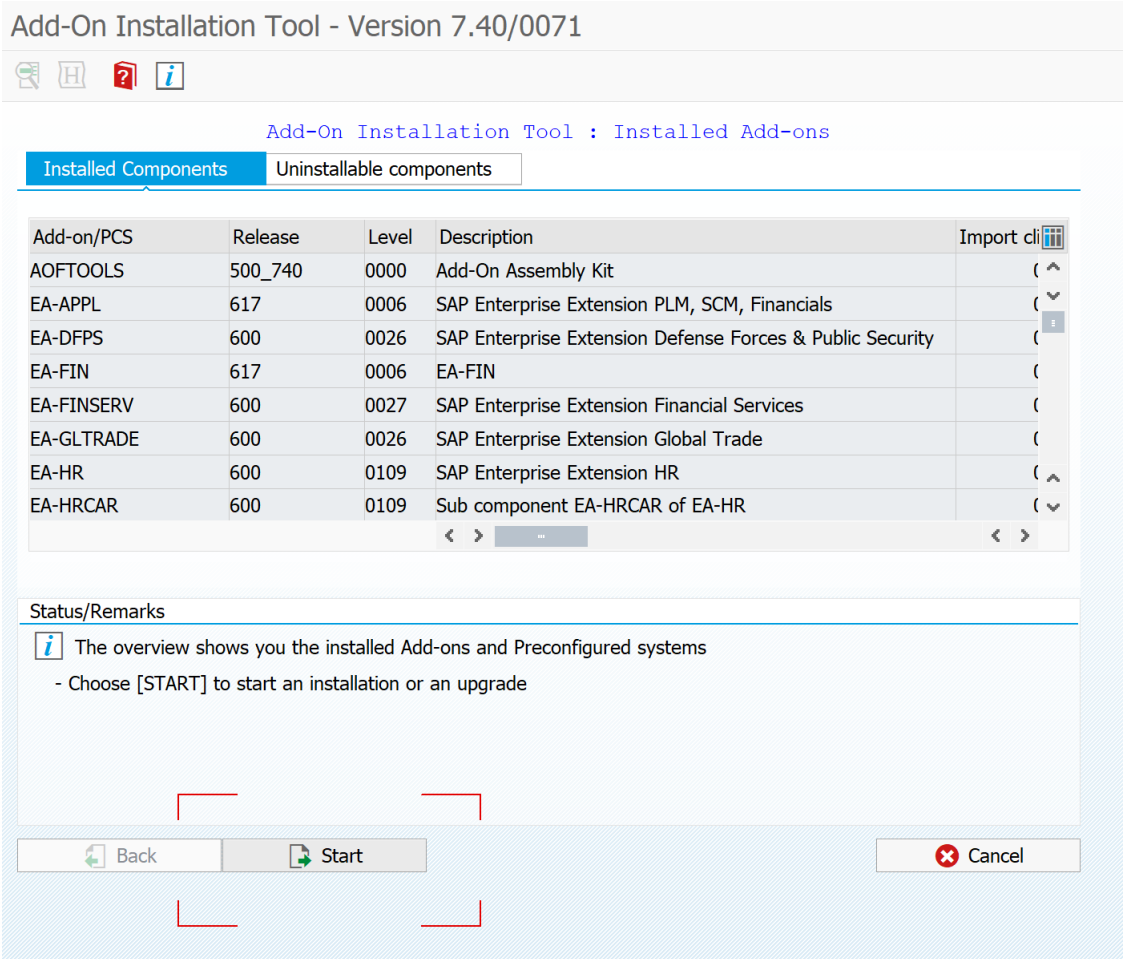
Download Add-on from this link: https://s3-eu-west-1.amazonaws.com/docs.linkeit.com/repo/awsconnector/D040020760607_0000016.PAT

Logon to client 000.

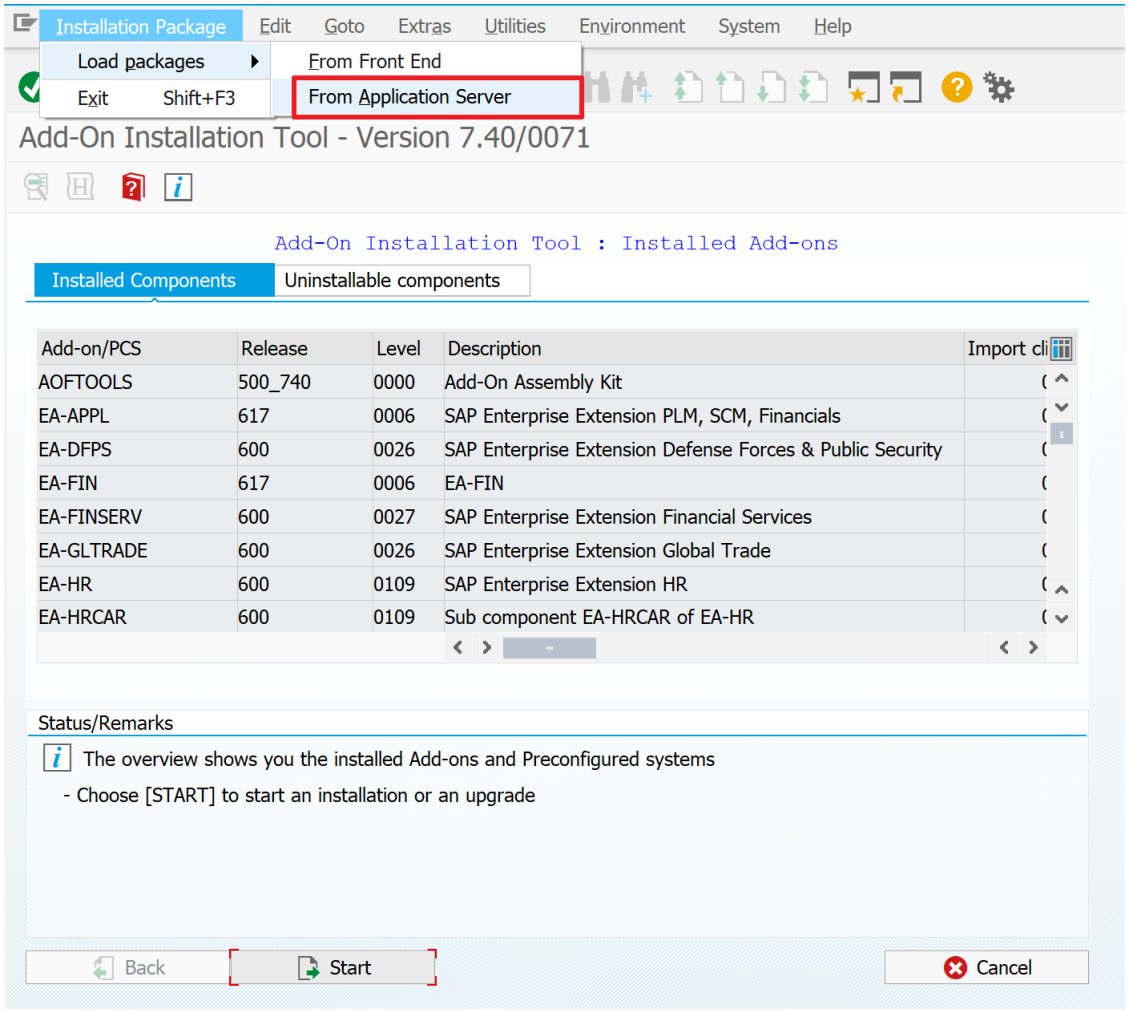
Installation of AWS Connector must be done in client 000.

SAINT.

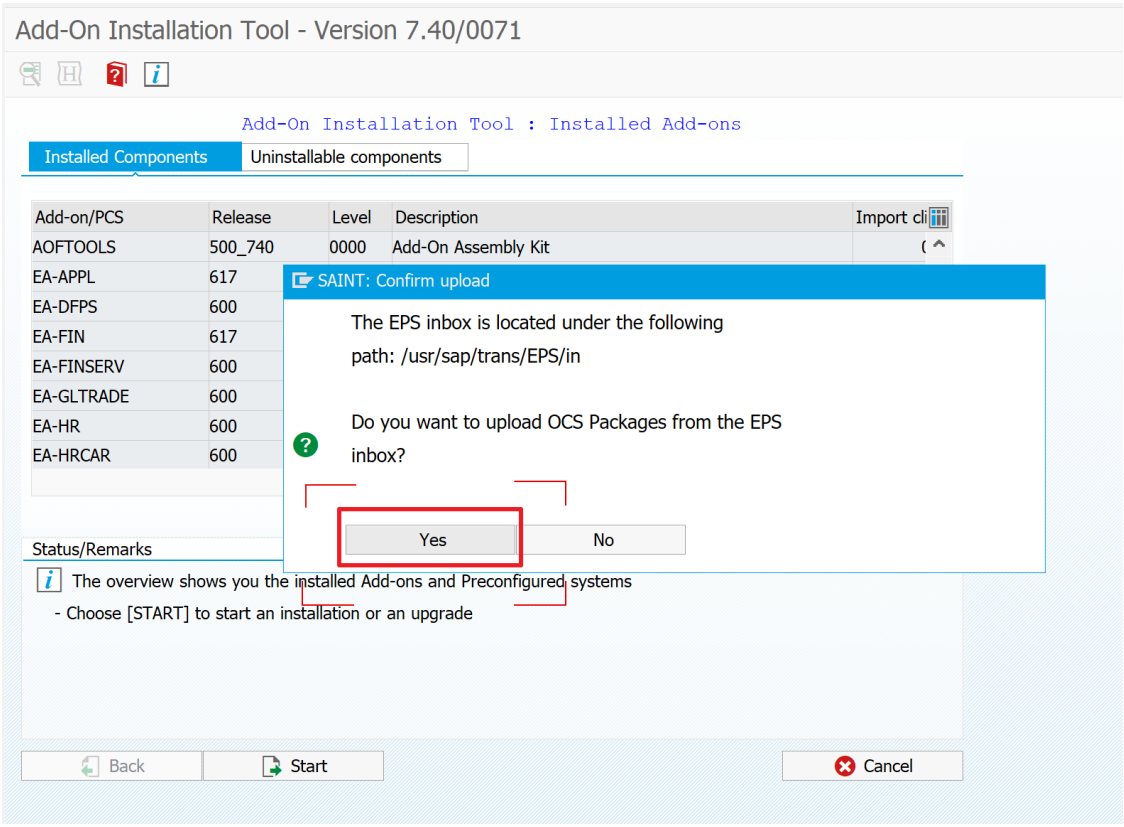
Go to transaction **SAINT**.



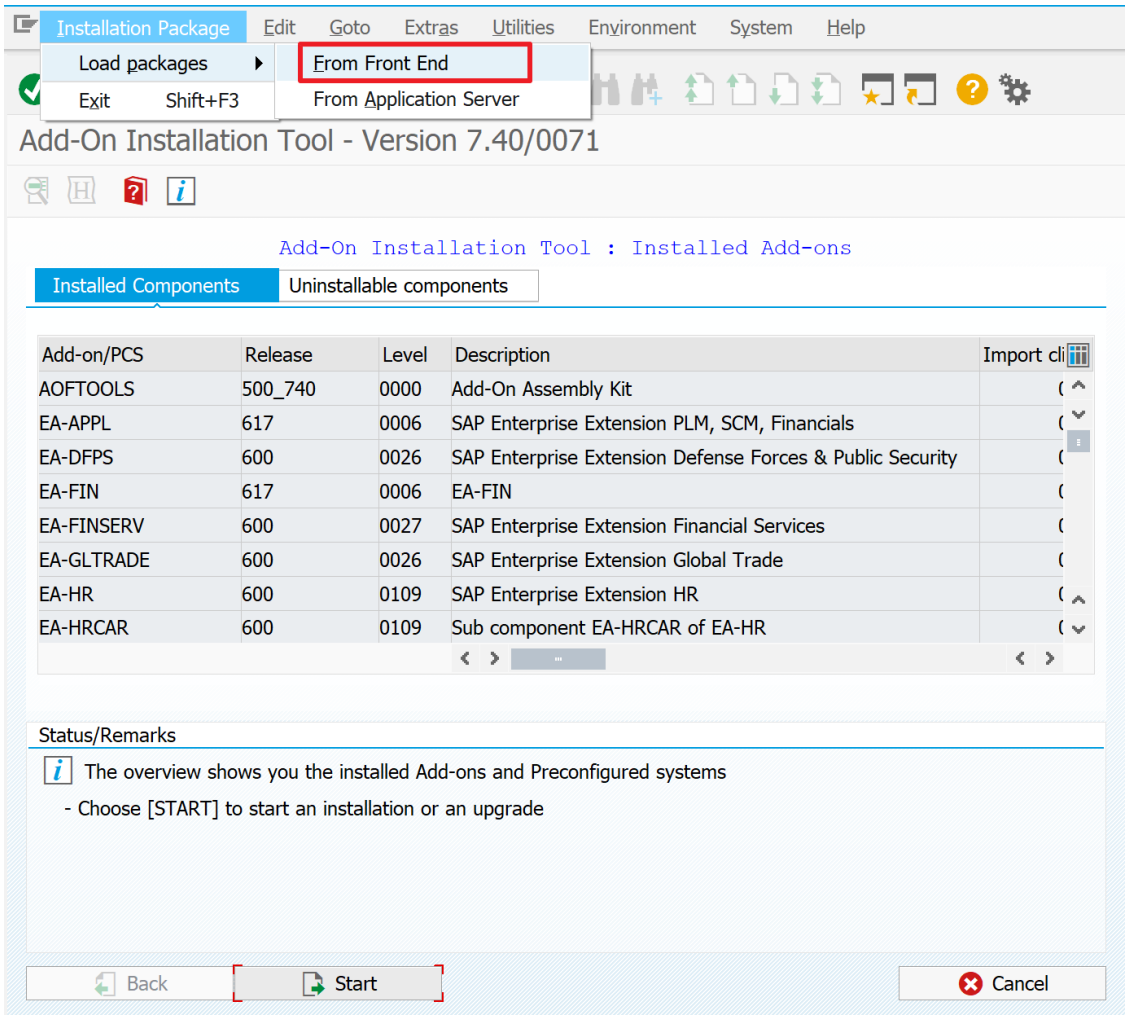
Installation Package menu -> Load package -> From Application Server.



In the pop up that appears press the yes button.

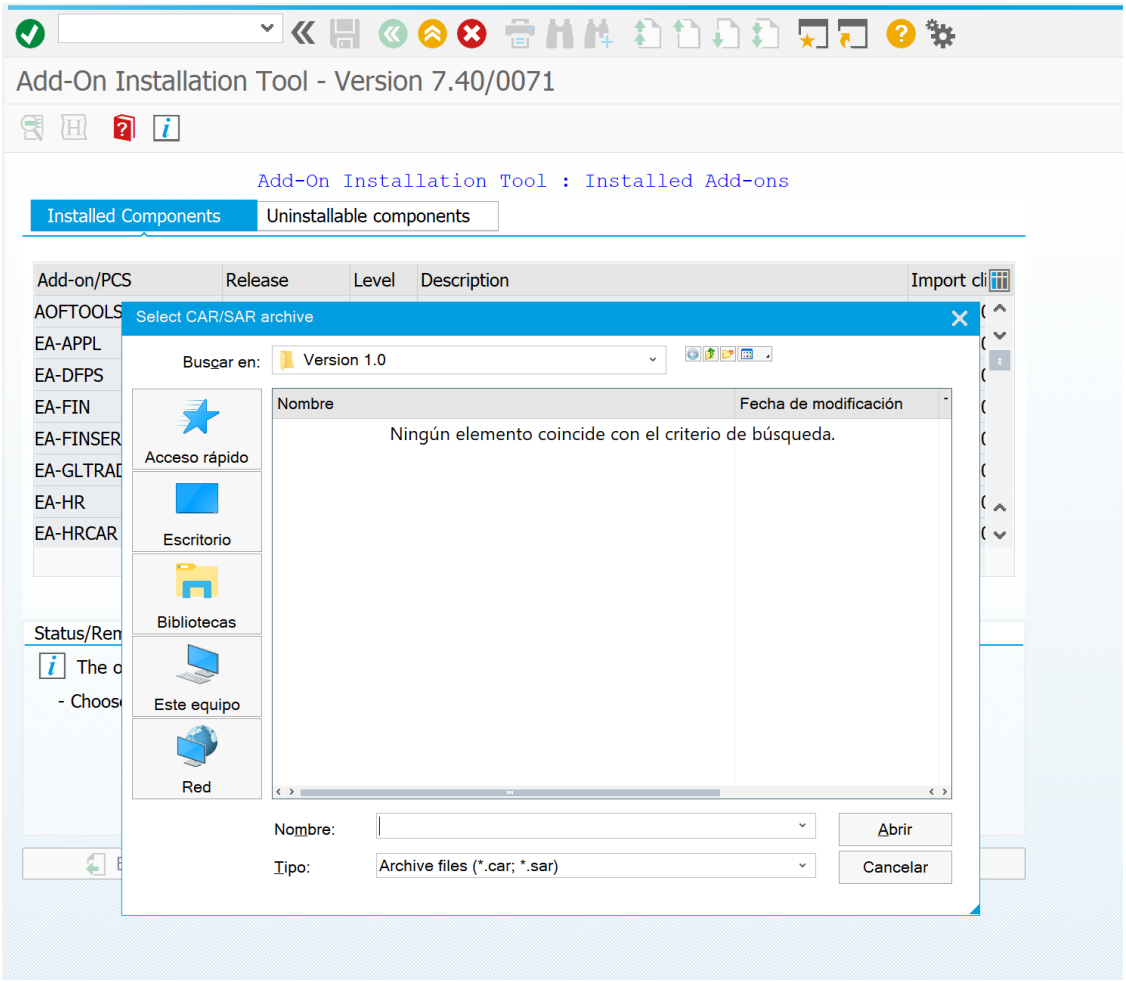

Add-On Installation Tool - Version 7.40/0071
Add-On Installation Tool : Installed Add-ons
Installed Components
Uninstallable components
Add-on/PCS
Release
Level
Description
Import cli
AOFTOOLS
500_740
0000
Add-On Assembly Kit
EA-APPL
617
EA-DFPS
600
EA-FIN
617
EA-FINSERV
600
EA-GLTRADE
600
EA-HR
600
EA-HRCAR
600
SAINT: Confirm upload
The EPS inbox is located under the following
path: /usr/sap/trans/EPS/in
Do you want to upload OCS Packages from the EPS
inbox?
Yes
No
Status/Remarks
The overview shows you the installed Add-ons and Preconfigured systems
- Choose [START] to start an installation or an upgrade
Back
Start
Cancel

Or also the add-on can be install from Frontend. Installation Package menu -> Load package -> From Front end.

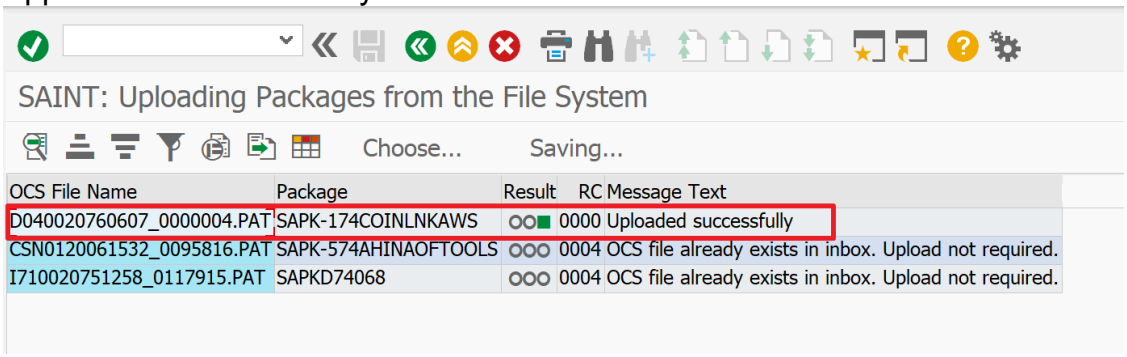


It

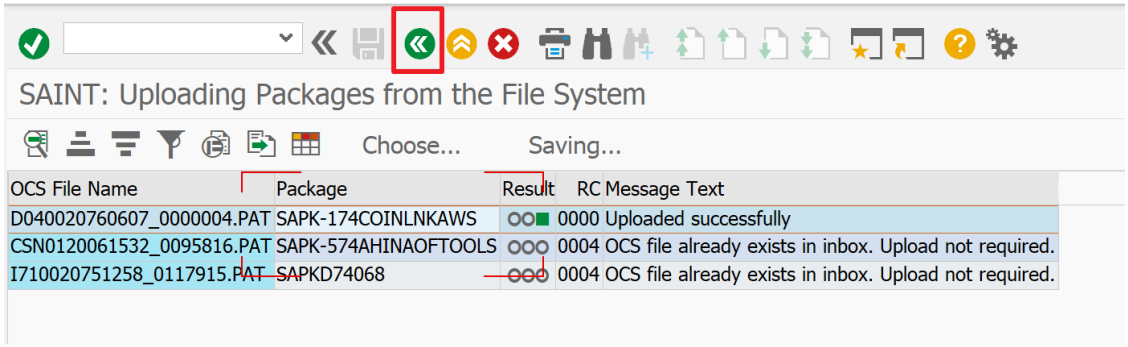
Select the .car/.sar file.



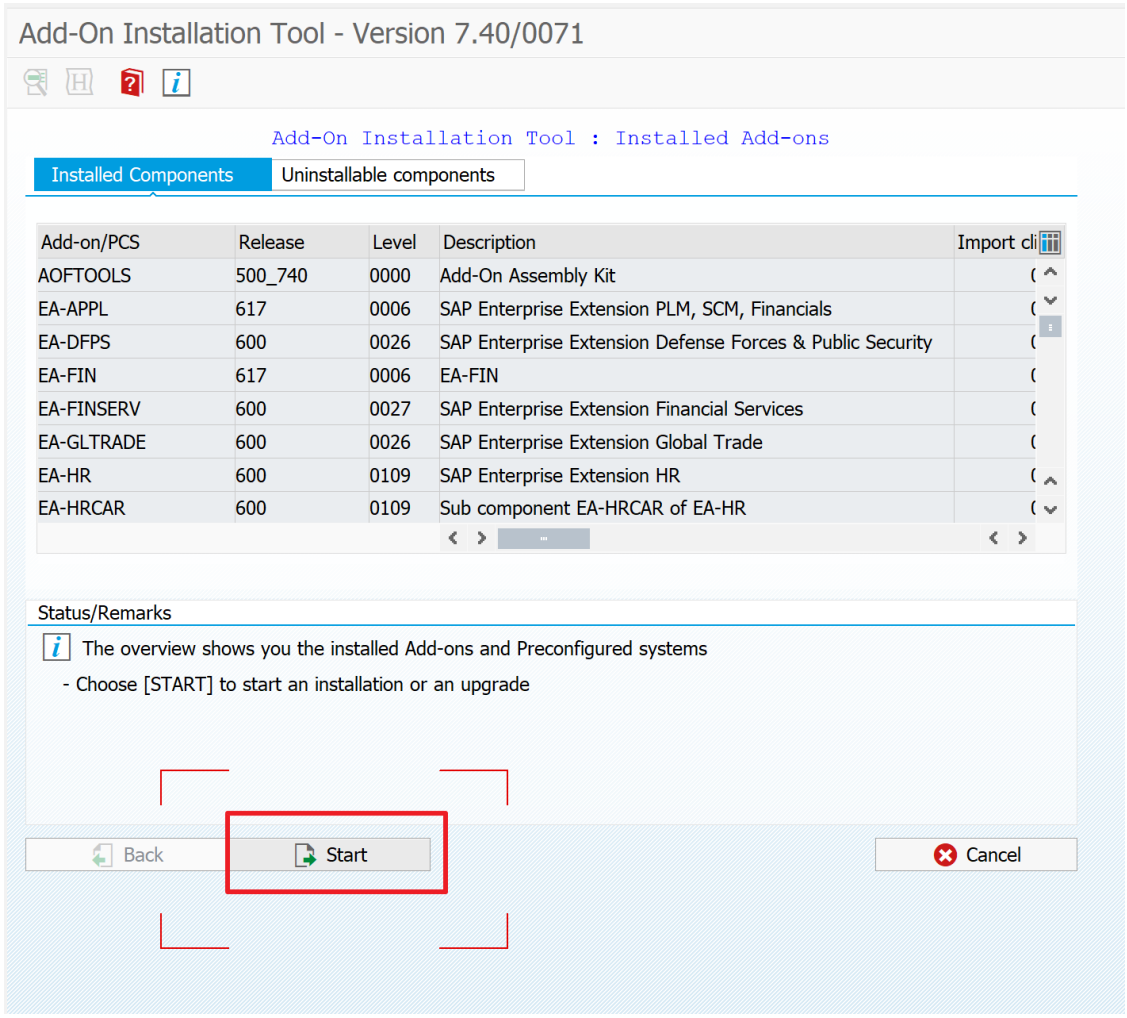
Appears a screen where you can see downloaded file.



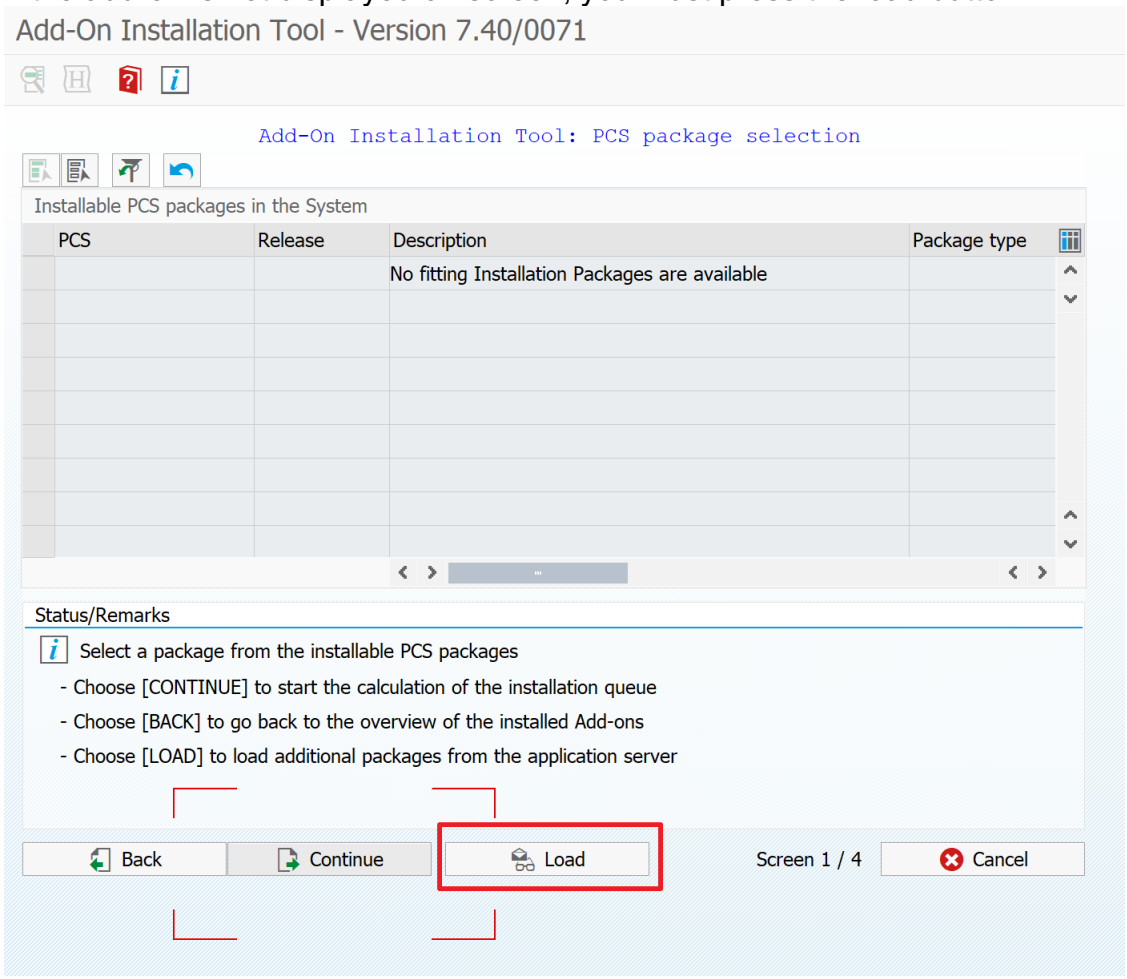
Press the back button.



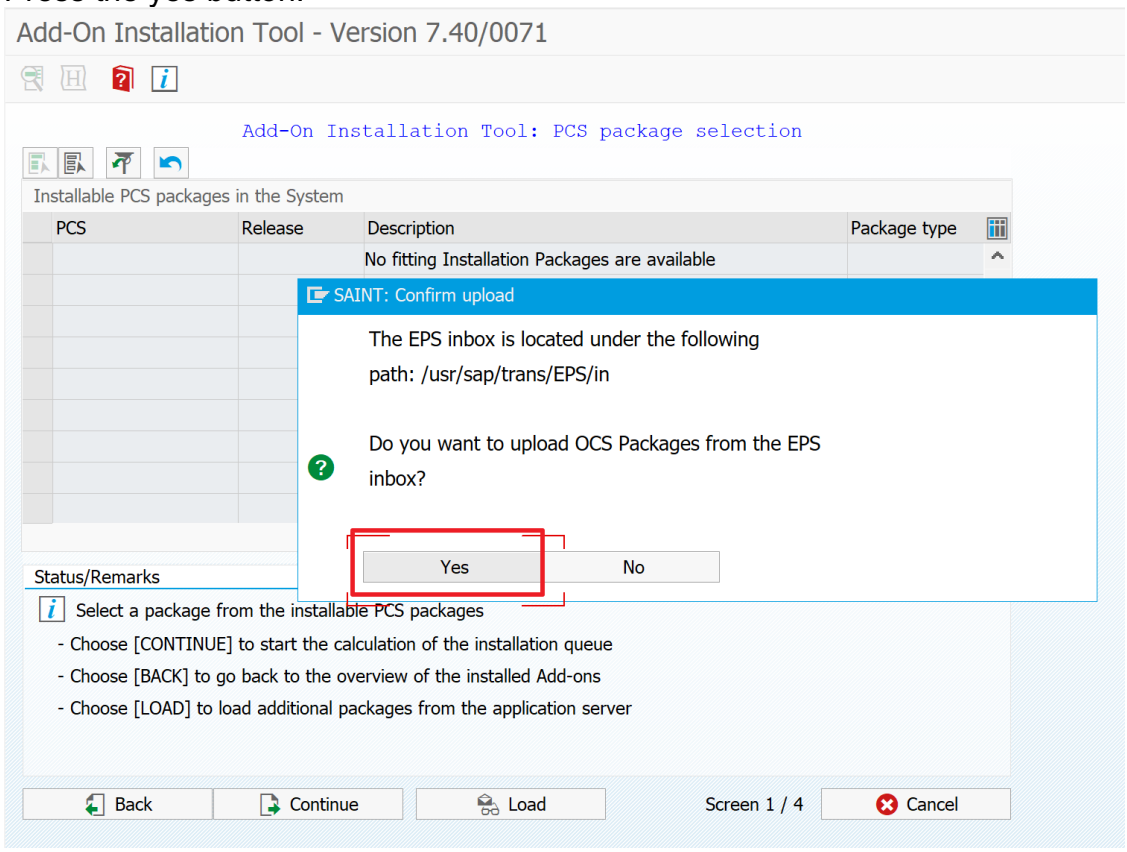
Press the start button.



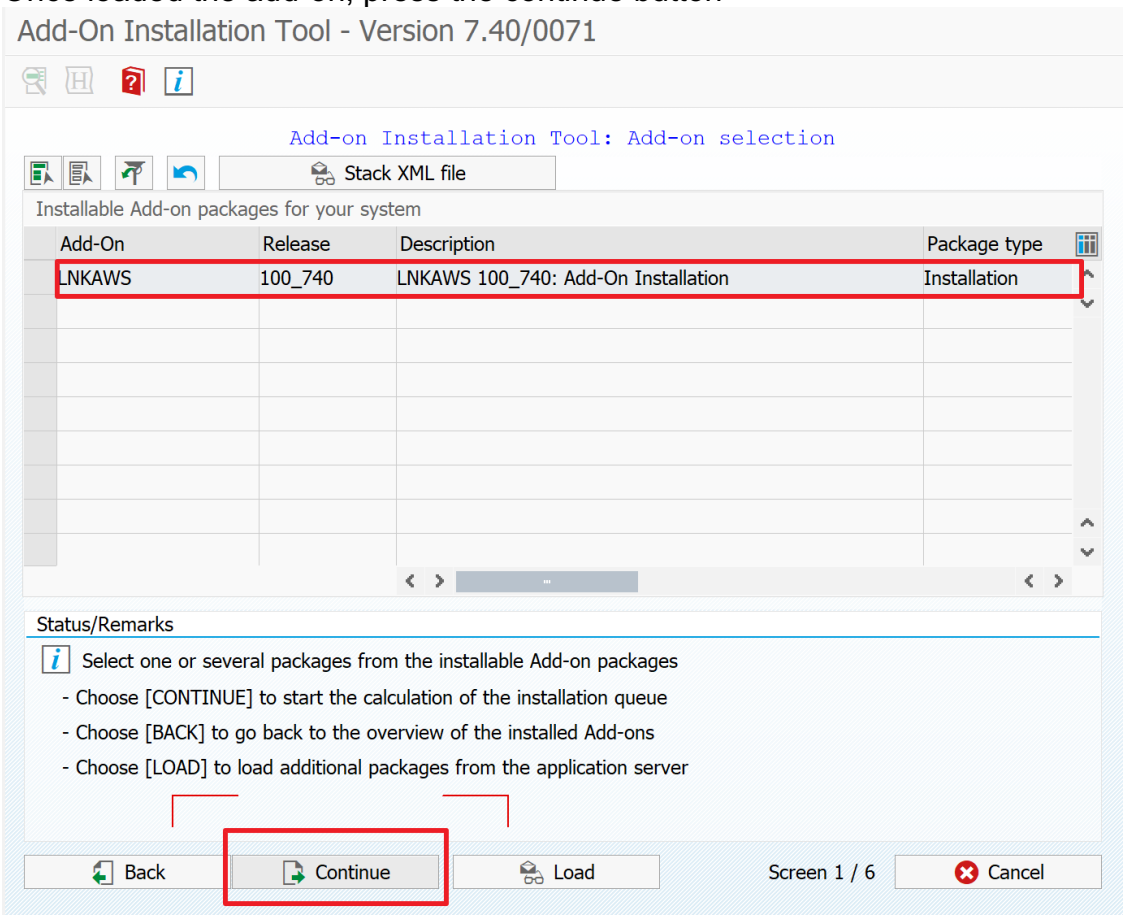
If the add-on is not displayed on screen, you must press the load button.



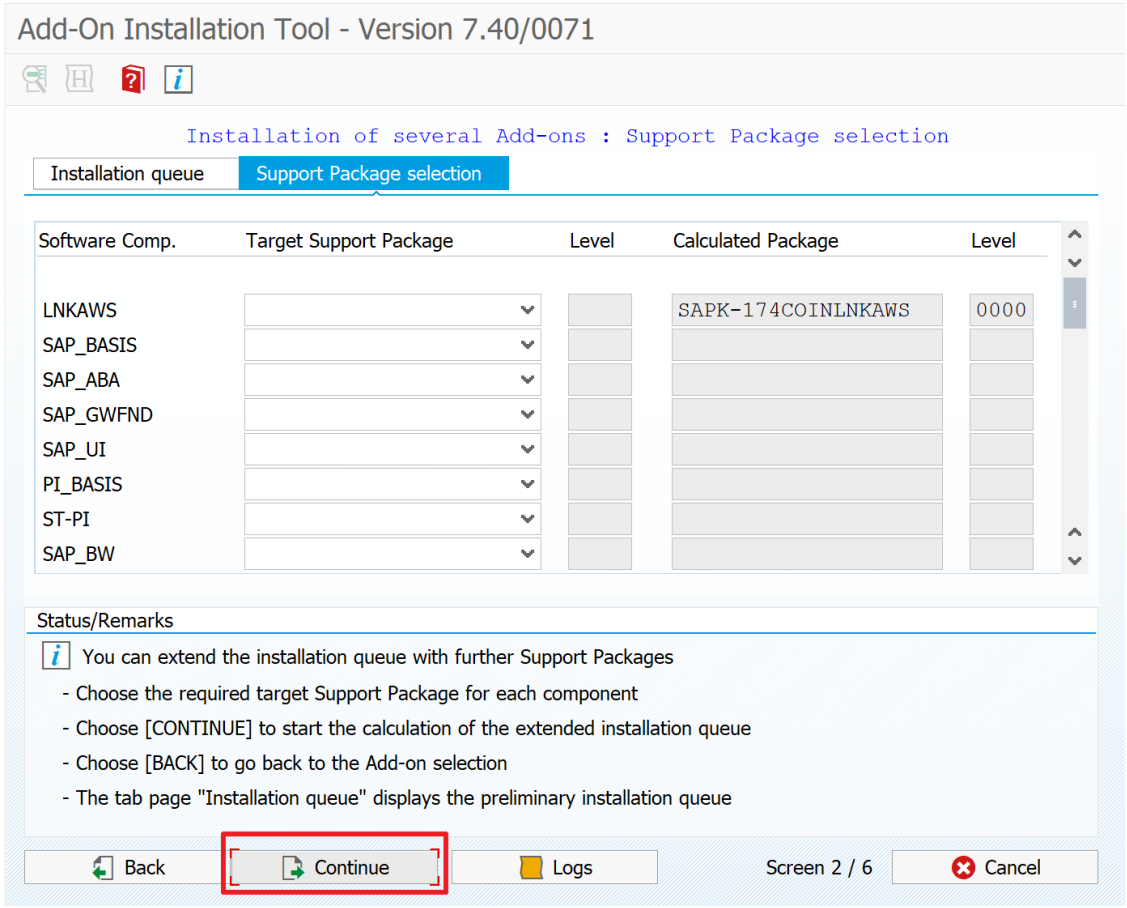
Press the yes button.



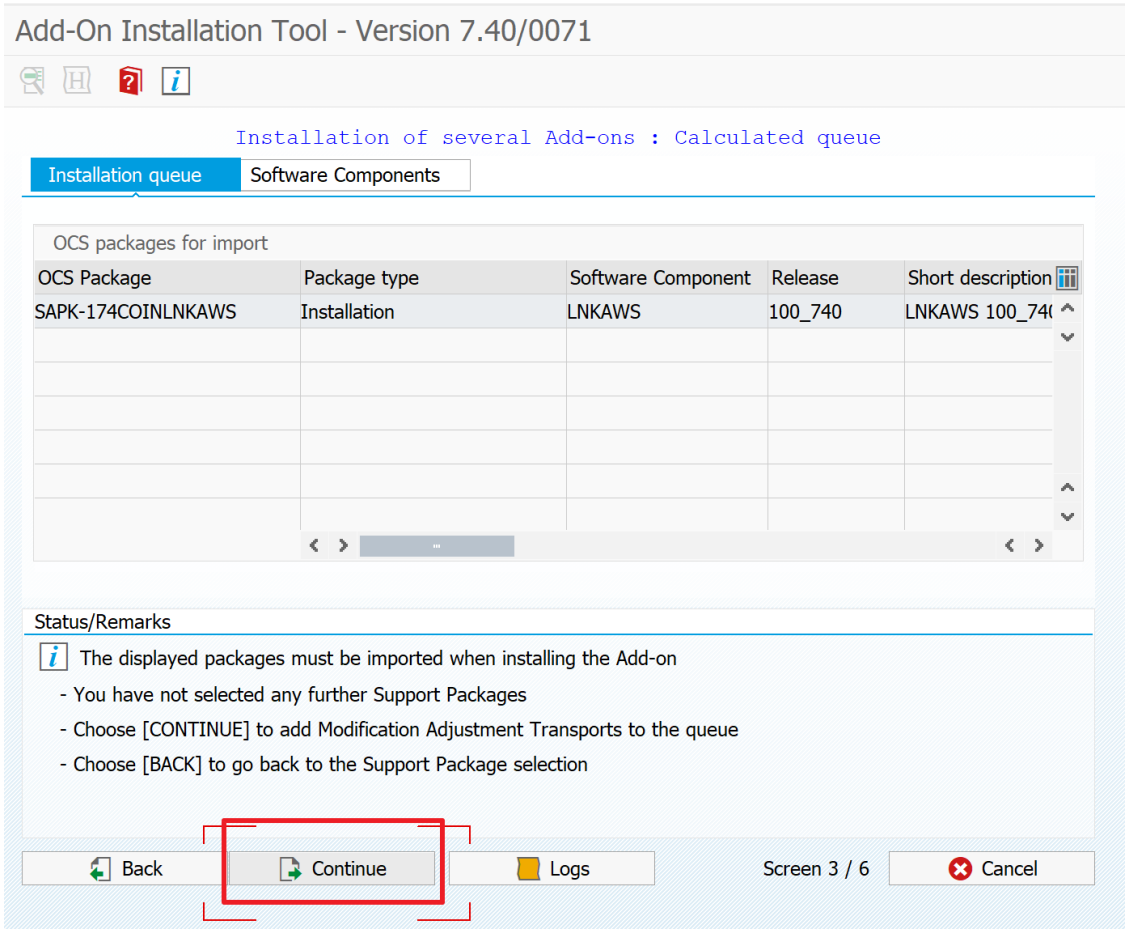
Once loaded the add-on, press the continue button



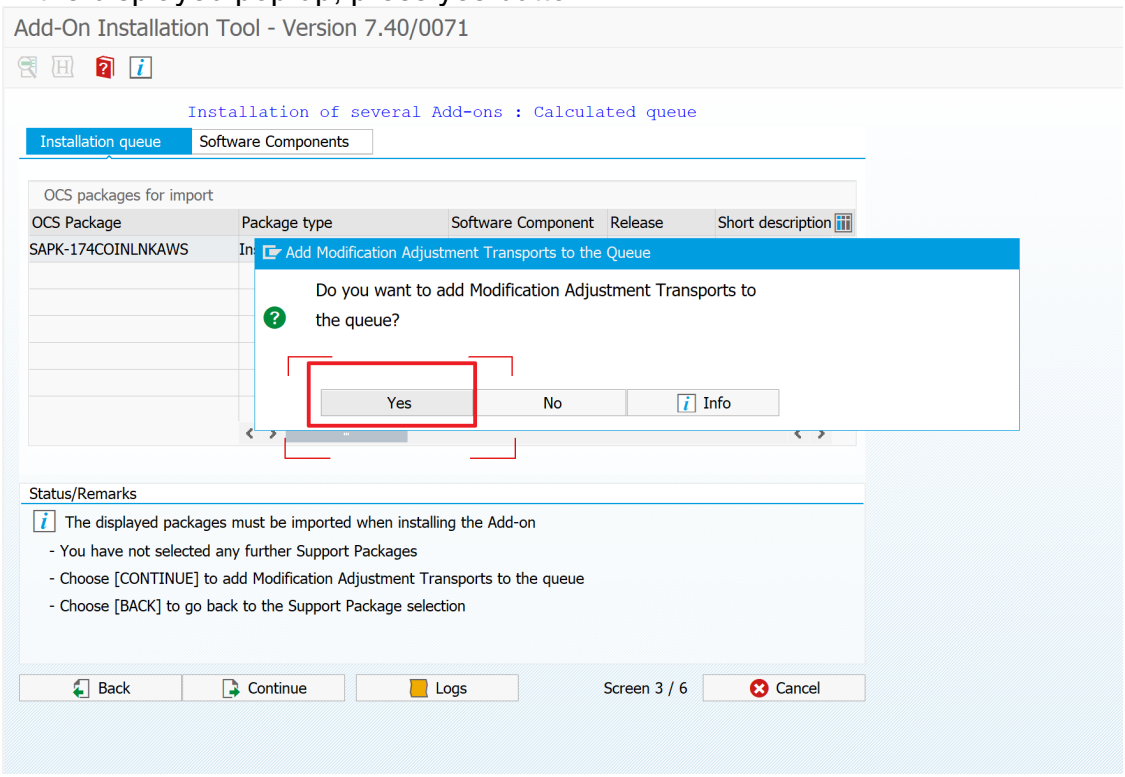
Press the continue button.



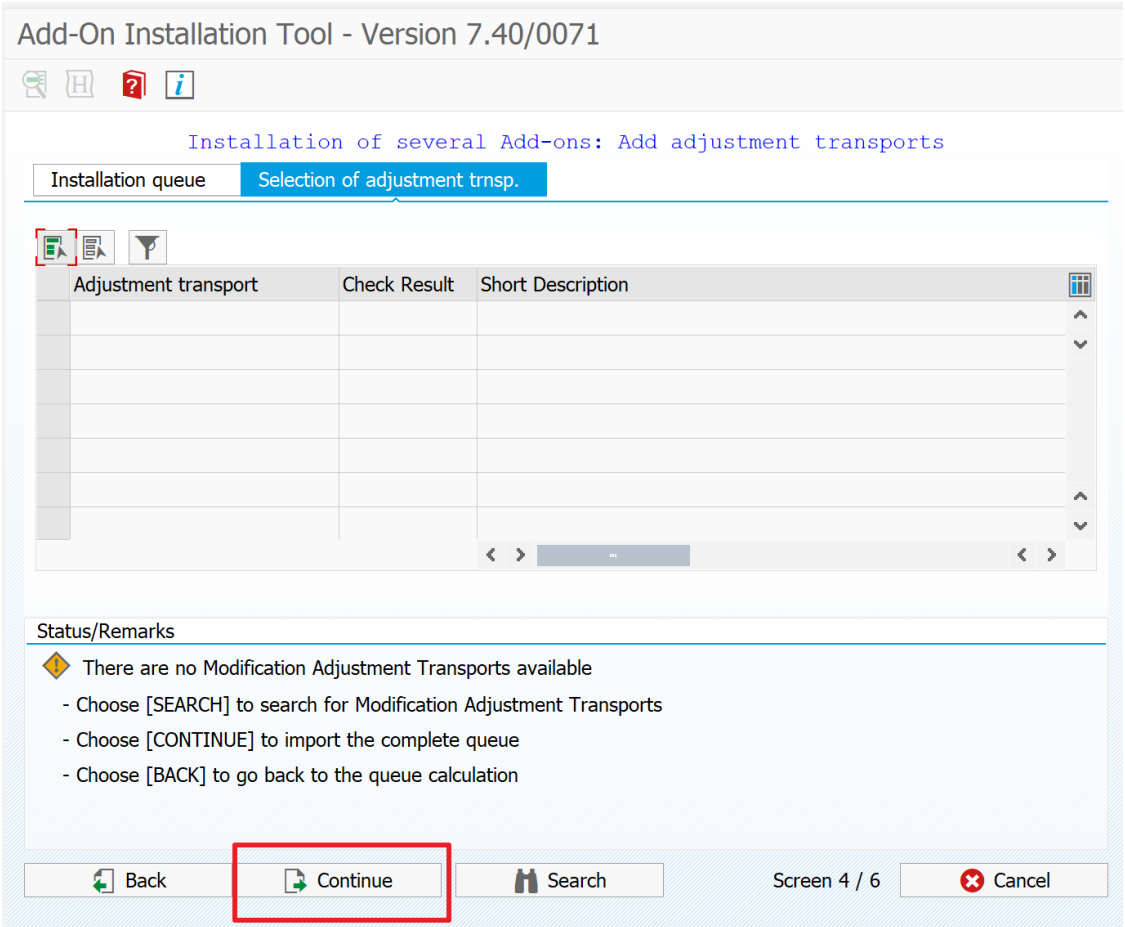
Press the continue button.



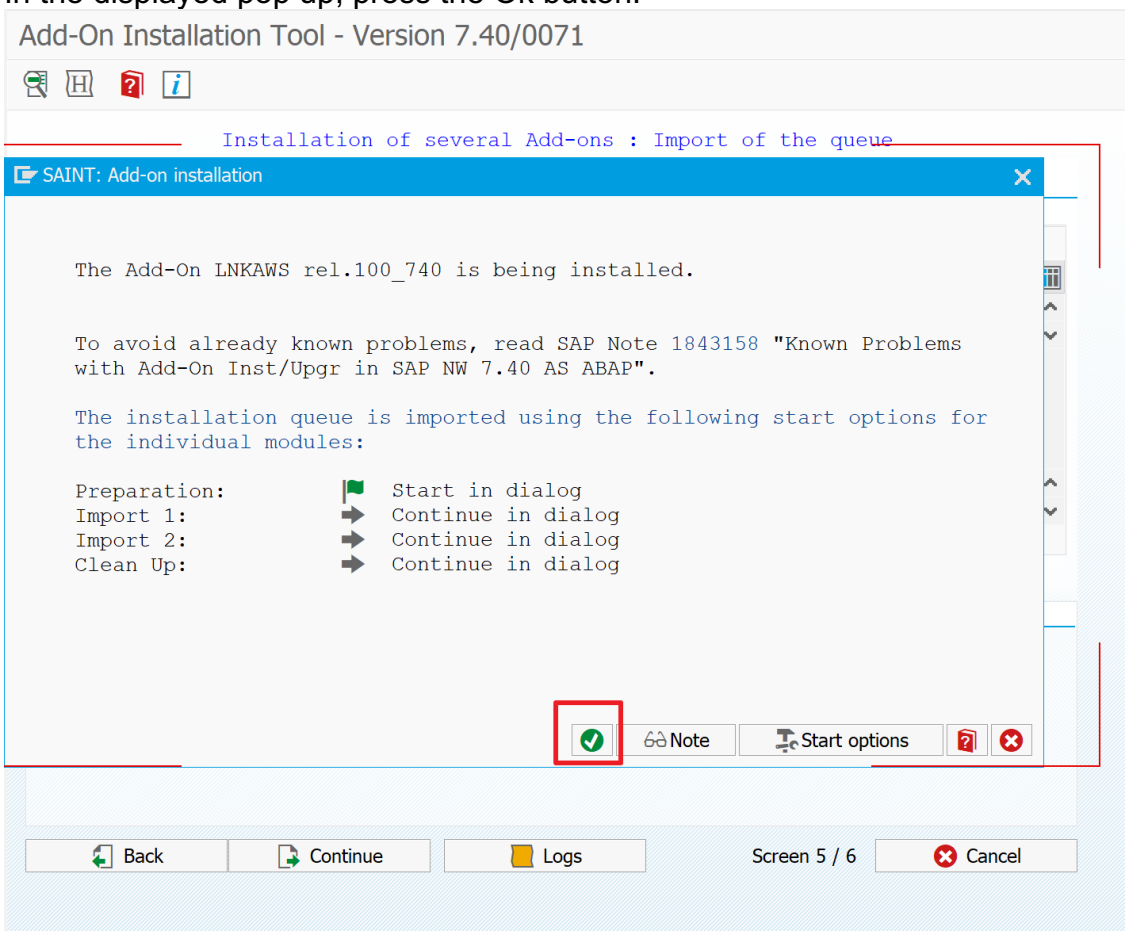
In the displayed pop up, press yes button.



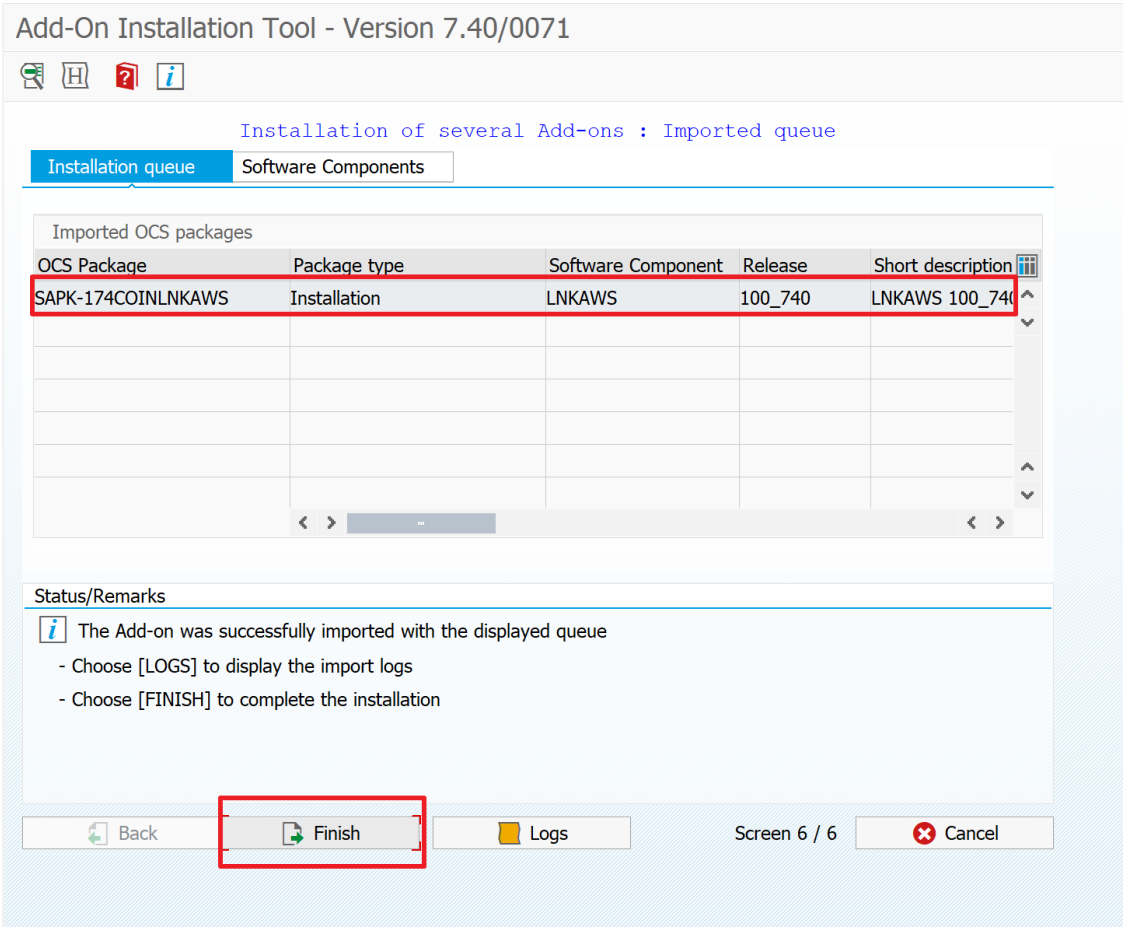
Press continue button.



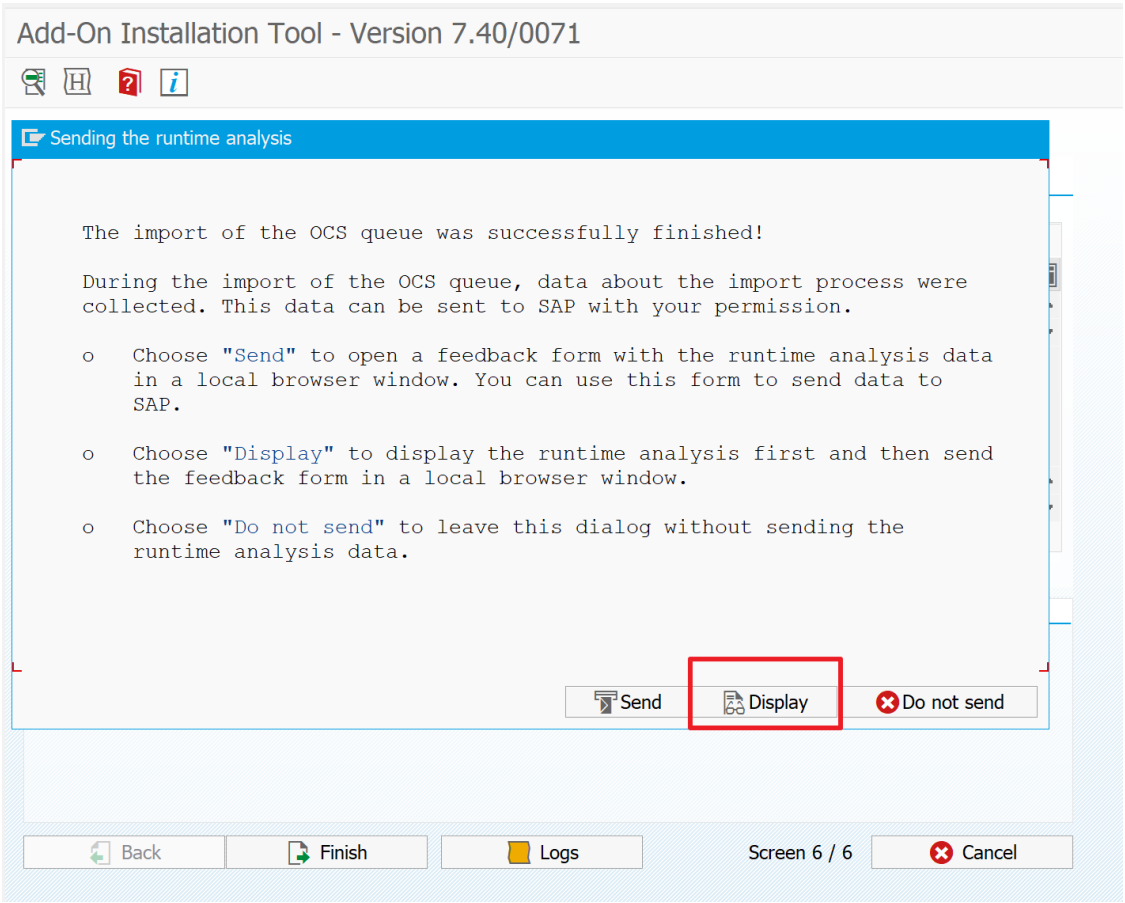
In the displayed pop up, press the Ok button.



Press finish button.

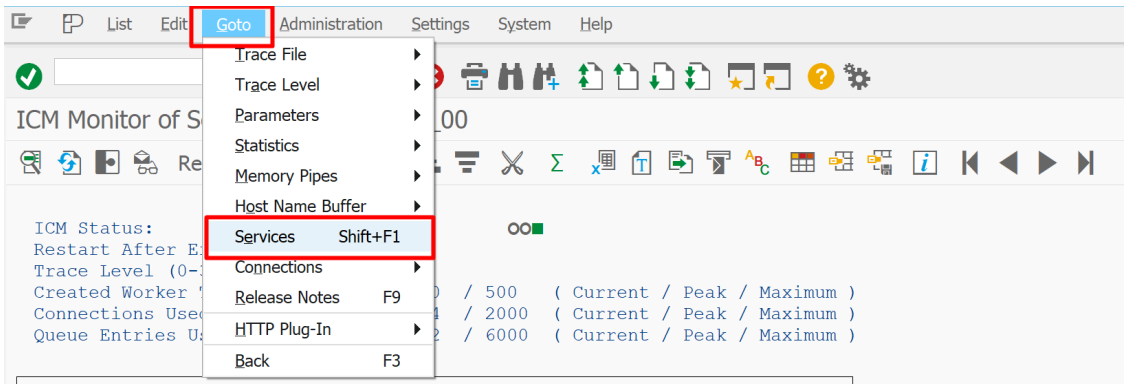


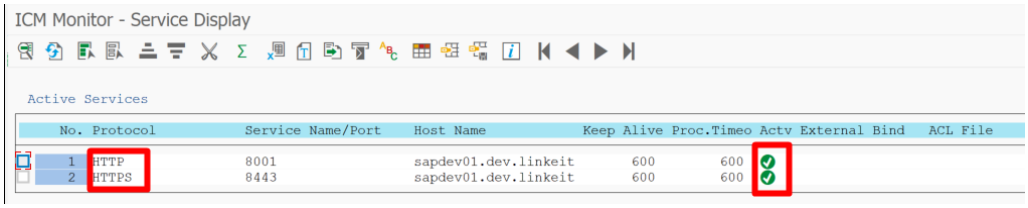
In the sending the runtime analysis pop-up, you can press the display button or do not send button.



Check HTTPS service.

Ensure HTTP and HTTPS services are existing and active.
Go to transaction **SMICM**.





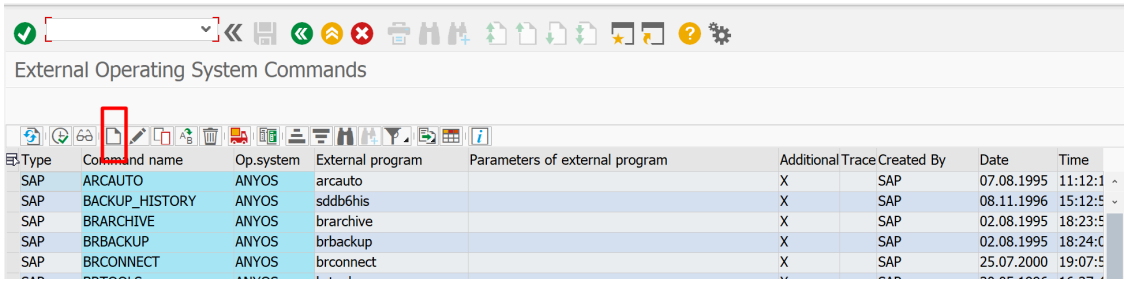
STRUST

First run of /LNKAWS/AWS_STRUST.

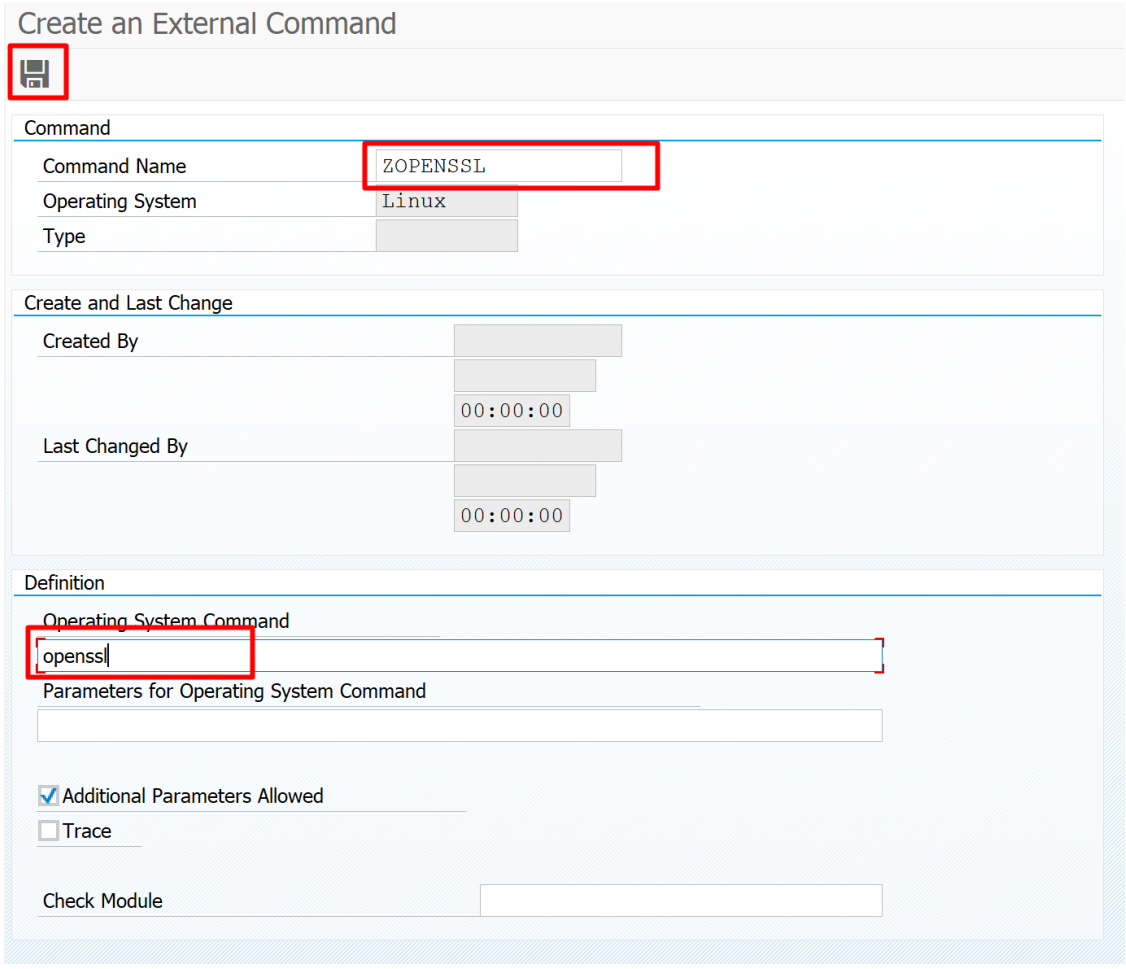
The system must be configured to add to STRUST in SSL client the AWS certificates.
This is automatically done with transaction /LNKAWS/AWS_STRUST.
A preparation must be done priori running /LNKAWS/AWS_STRUST. Run transaction SM69.

If the operating system is Linux:

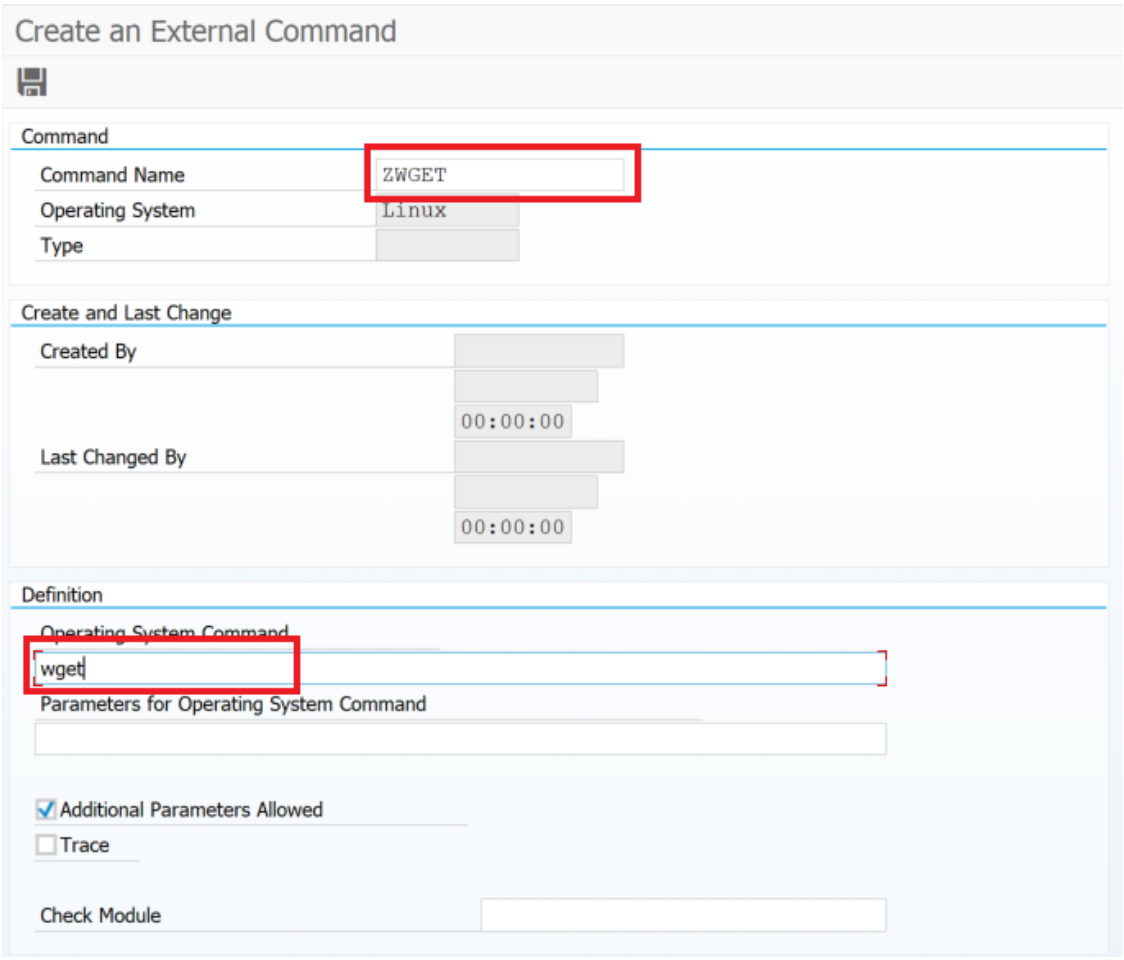
Create a new command:


External Operating System Commands
Type Command name Op.system External program Parameters of external program Additional Trace Created By Date Time
SAP ARCAUTO ANYOS arcauto X SAP 07.08.1995 11:12:1
SAP BACKUP_HISTORY ANYOS sddb6his X SAP 08.11.1996 15:12:5
SAP BRARCHIVE ANYOS brarchive X SAP 02.08.1995 18:23:5
SAP BRBACKUP ANYOS brbackup X SAP 02.08.1995 18:24:0
SAP BRCONNECT ANYOS brconnect X SAP 25.07.2000 19:07:5

OpenSSL.

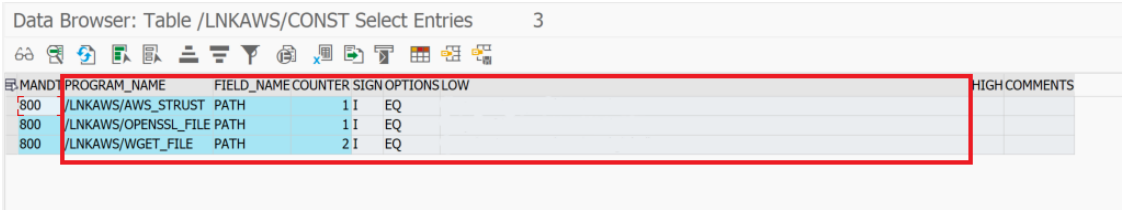

Create an External Command
Command
Command Name ZOPENSSL
Operating System Linux
Type
Create and Last Change
Created By
00:00:00
Last Changed By
00:00:00
Definition
Operating System Command
openssl
Parameters for Operating System Command
Additional Parameters Allowed
Trace
Check Module

Wget.

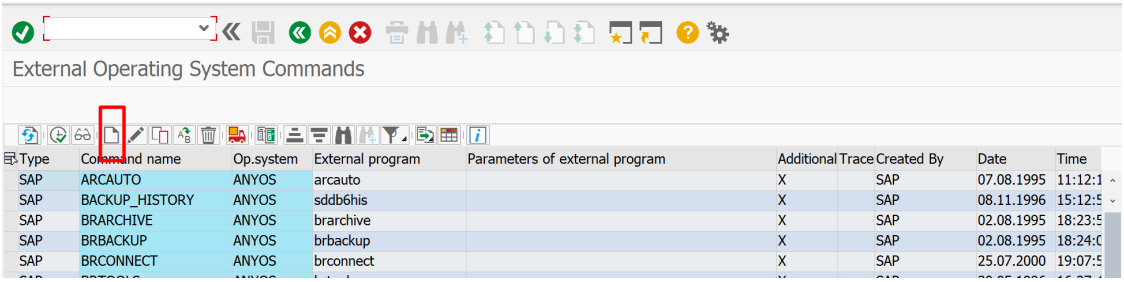

Create an External Command
Command
Command Name
ZWGET
Operating System
Linux
Type
Create and Last Change
Created By
00:00:00
Last Changed By
00:00:00
Definition
Operating System Command
wget
Parameters for Operating System Command
Additional Parameters Allowed
Trace
Check Module

If the operating system is Windows:

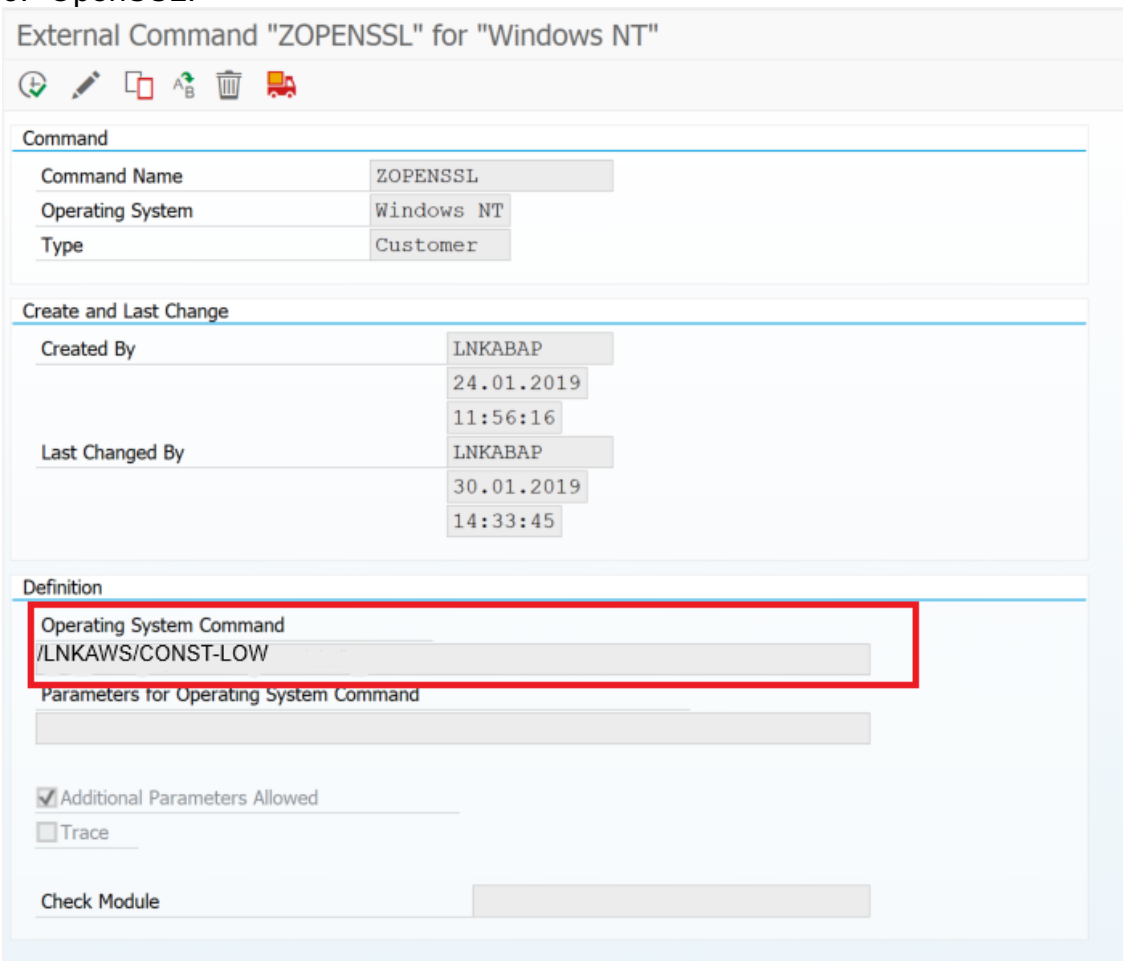
1.- Configure path in the /LNKAWS/CONST table (SM30): The Low field informs the path where you want to store the openSSL and Wget executables. The data to be entered in the table are the following:



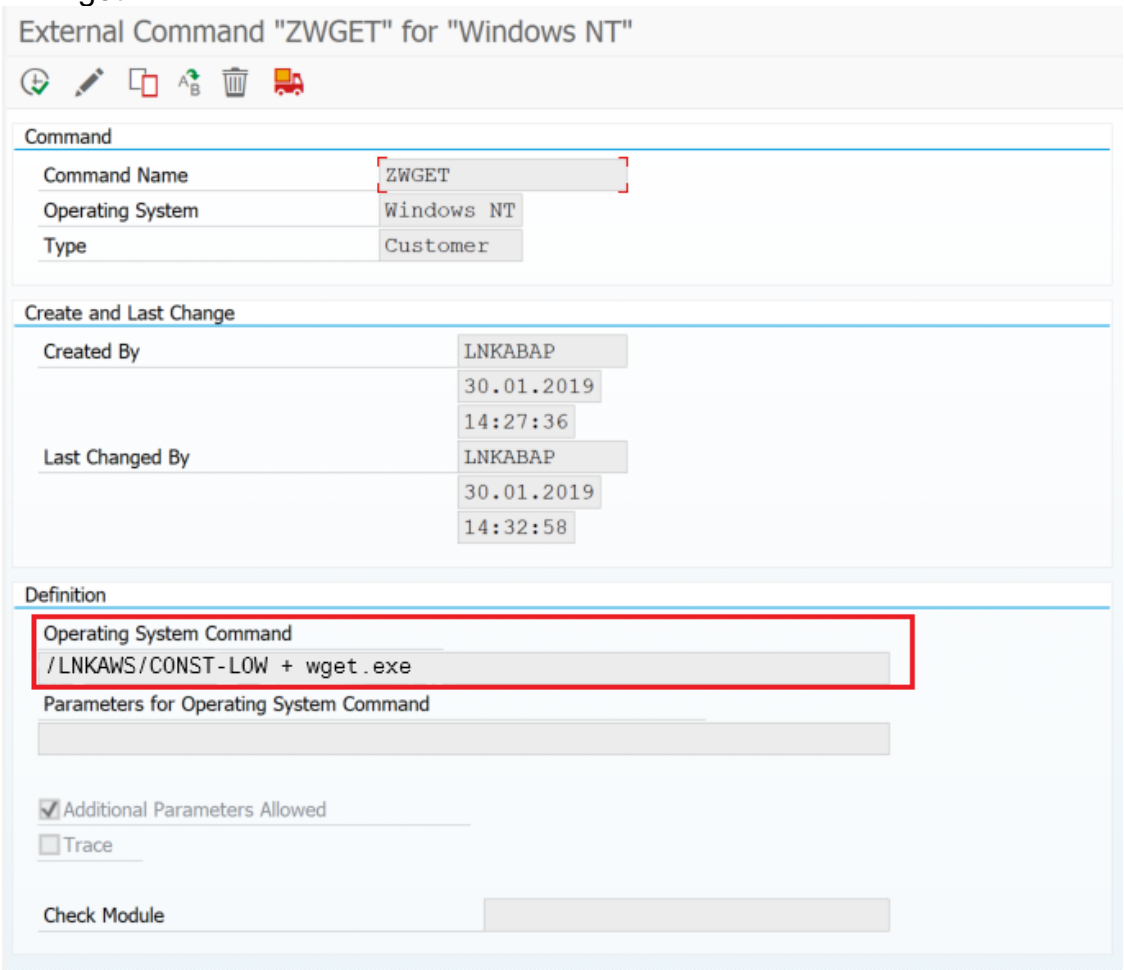
2.- Create a new command:



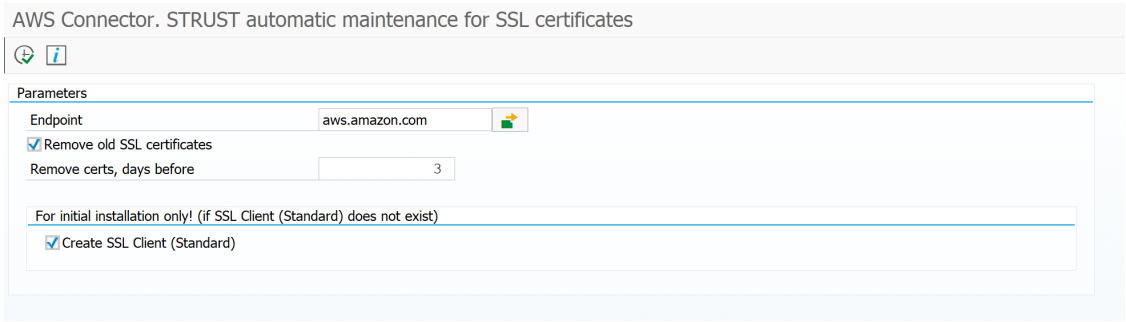
3.- OpenSSL.



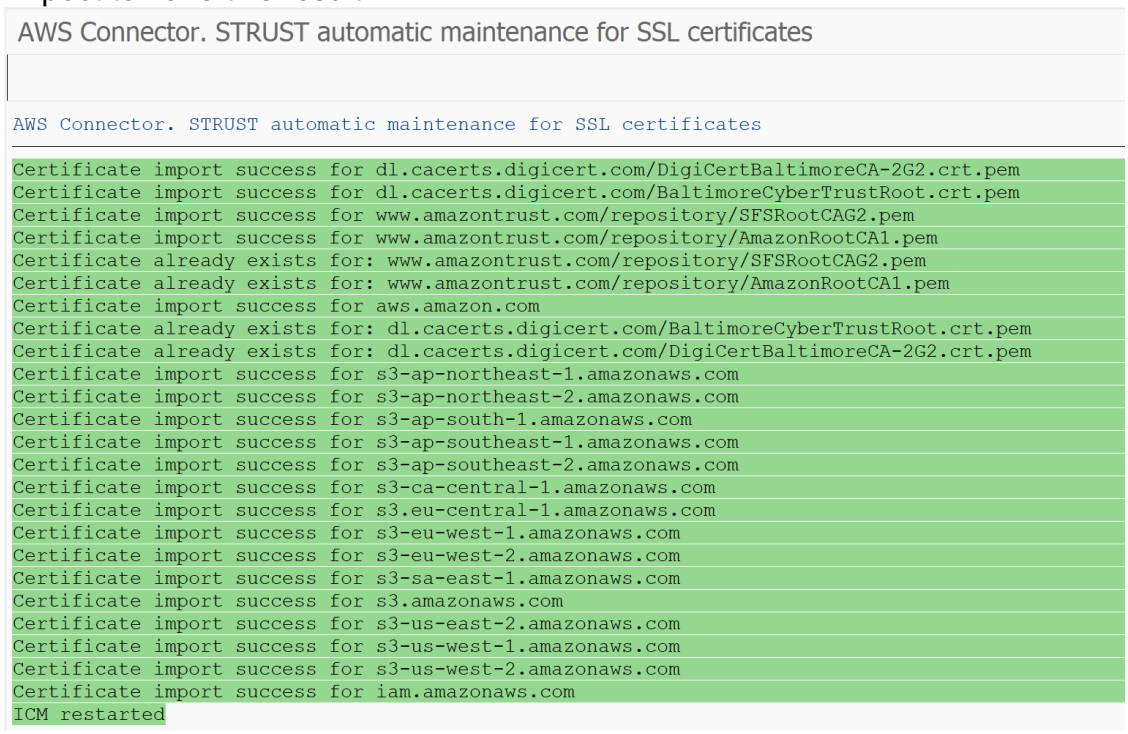
4.- Wget.


External Command "ZWGET" for "Windows NT"
Command
Command Name
ZWGET
Operating System
Windows NT
Type
Customer
Create and Last Change
Created By
LNKABAP
30.01.2019
14:27:36
Last Changed By
LNKABAP
30.01.2019
14:32:58
Definition
Operating System Command
/LNKAWS/CONST-LOW + wget.exe
Parameters for Operating System Command
Additional Parameters Allowed
Trace
Check Module

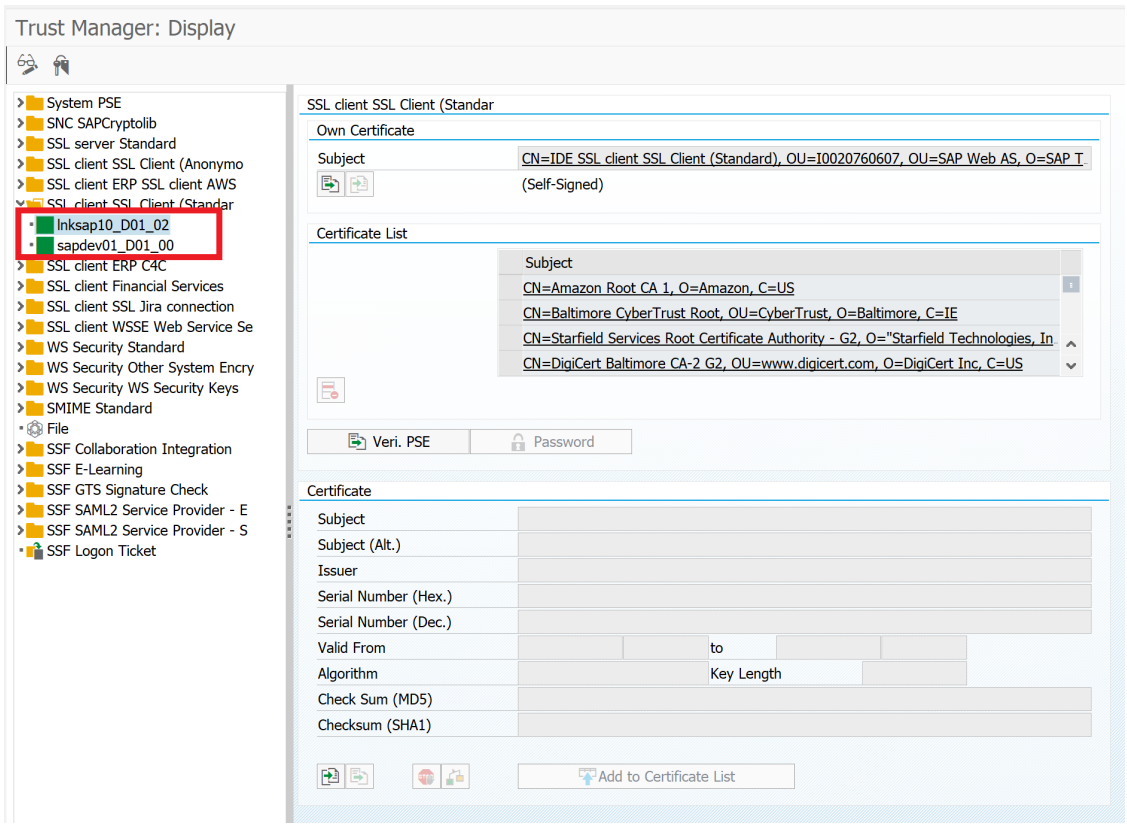
Once added ZOPENSSL and ZWGET to SM69, Run transaction /LNKAWS/AWS_STRUST with these parameters:



Expect to have this result:

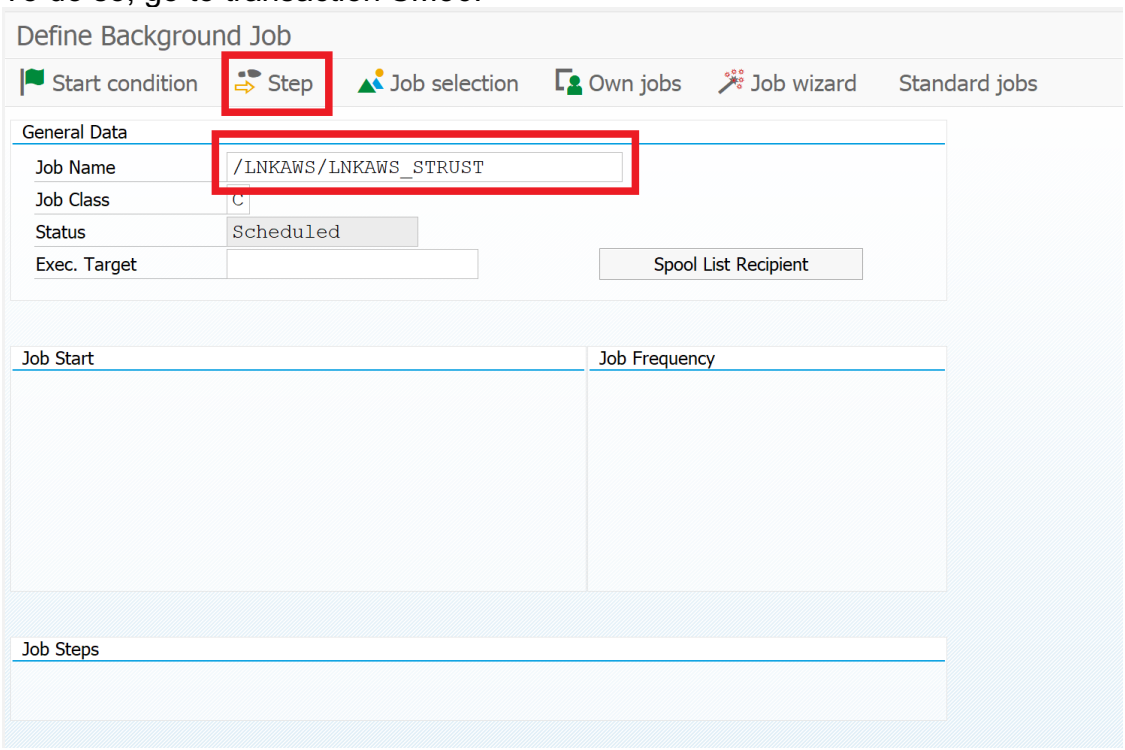


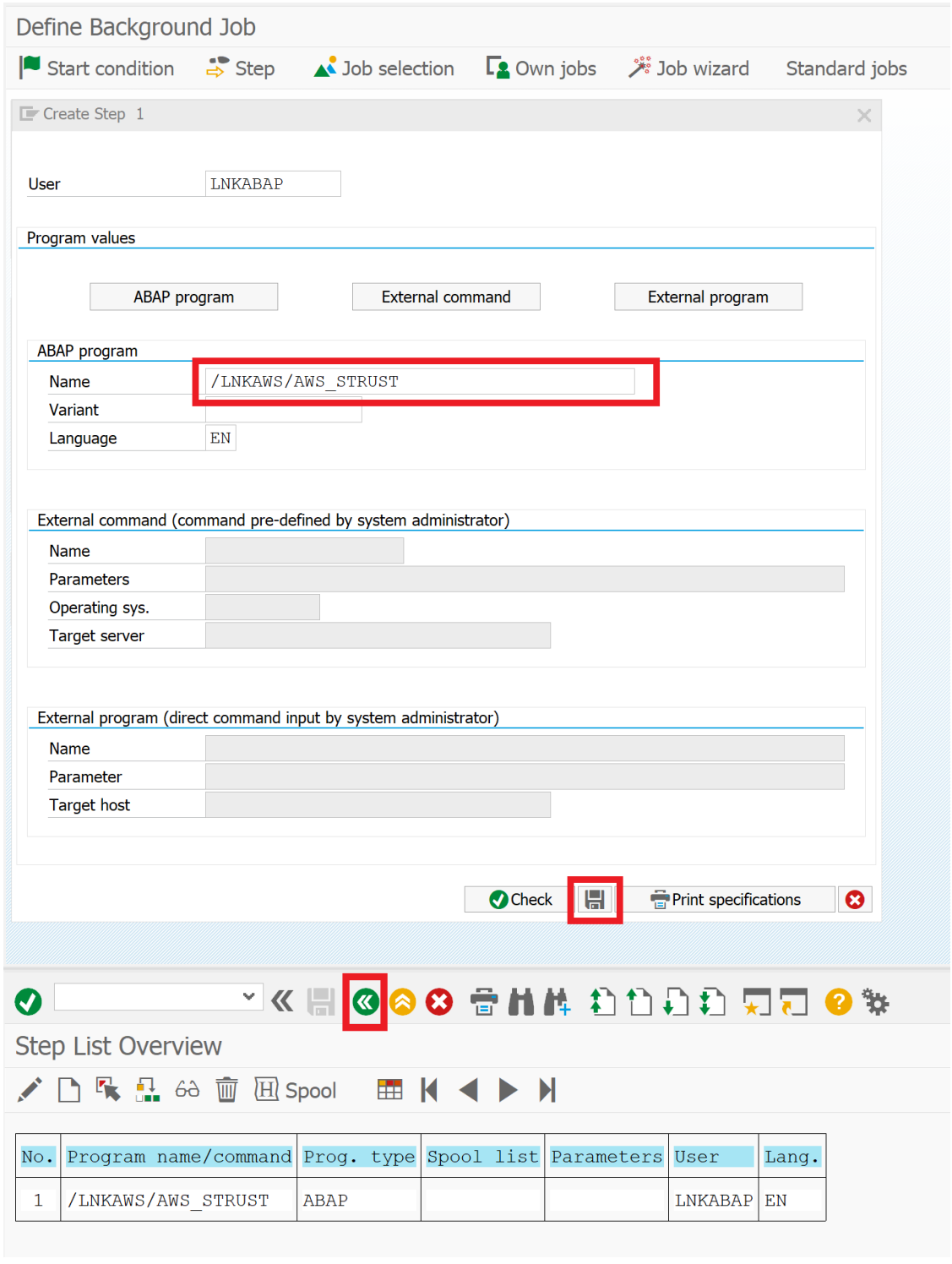
You can check the result in transaction STRUST:

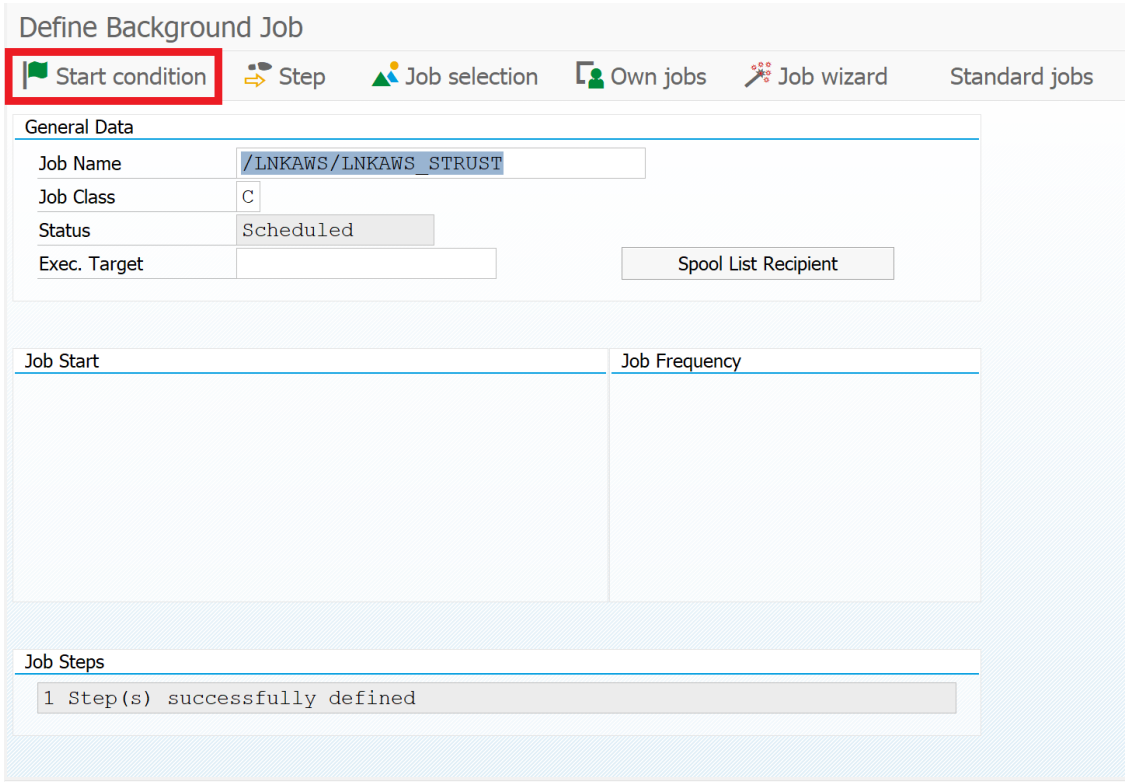


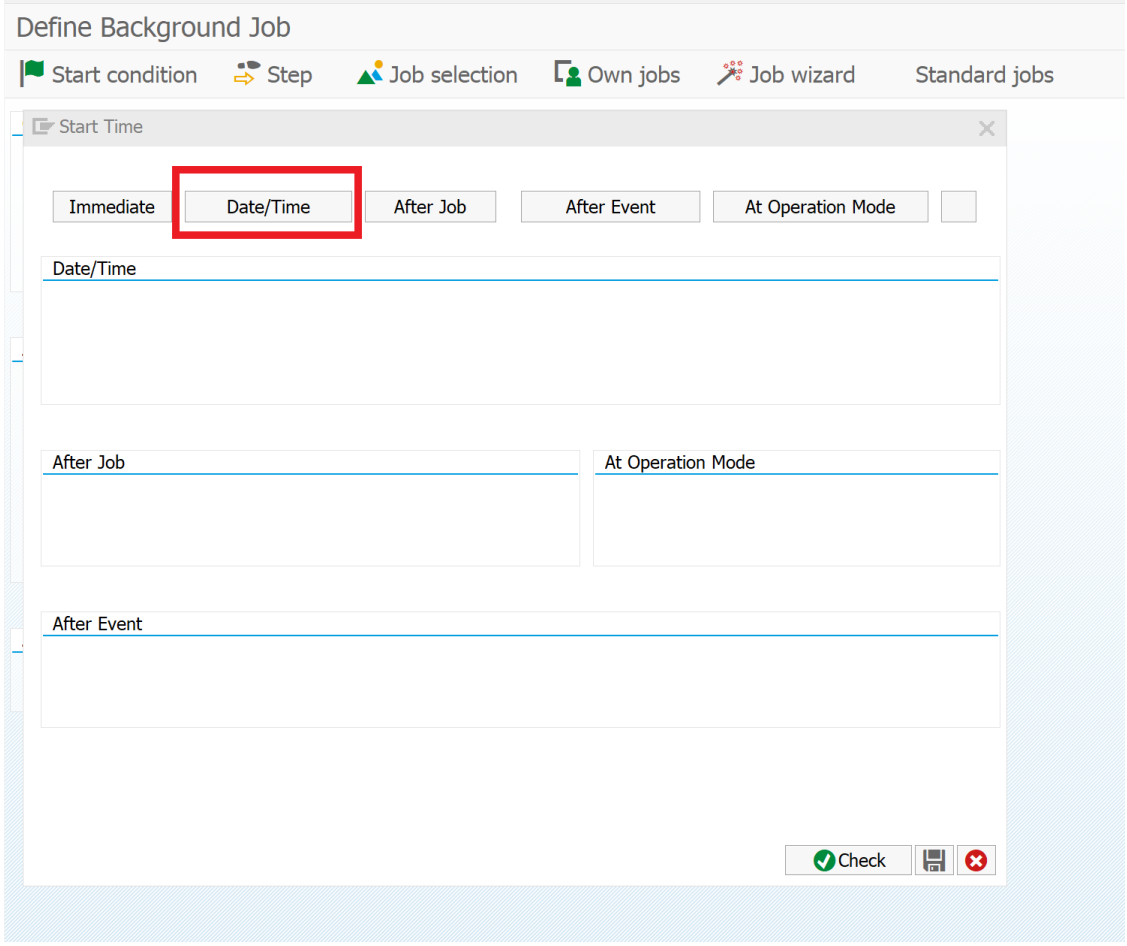
Programming job /LNKAWS/AWS_STRUST.

AWS certificates can be invalidated or can be expired.
If this happens, new certificate(s) must be installed in STRUST to ensure AWS Connector can run properly.
The program /LNKAWS/AWS_STRUST will take care of it.
We recommend programming a job /LNKAWS/AWS_STRUST on a daily basis.
To do so, go to transaction SM36:

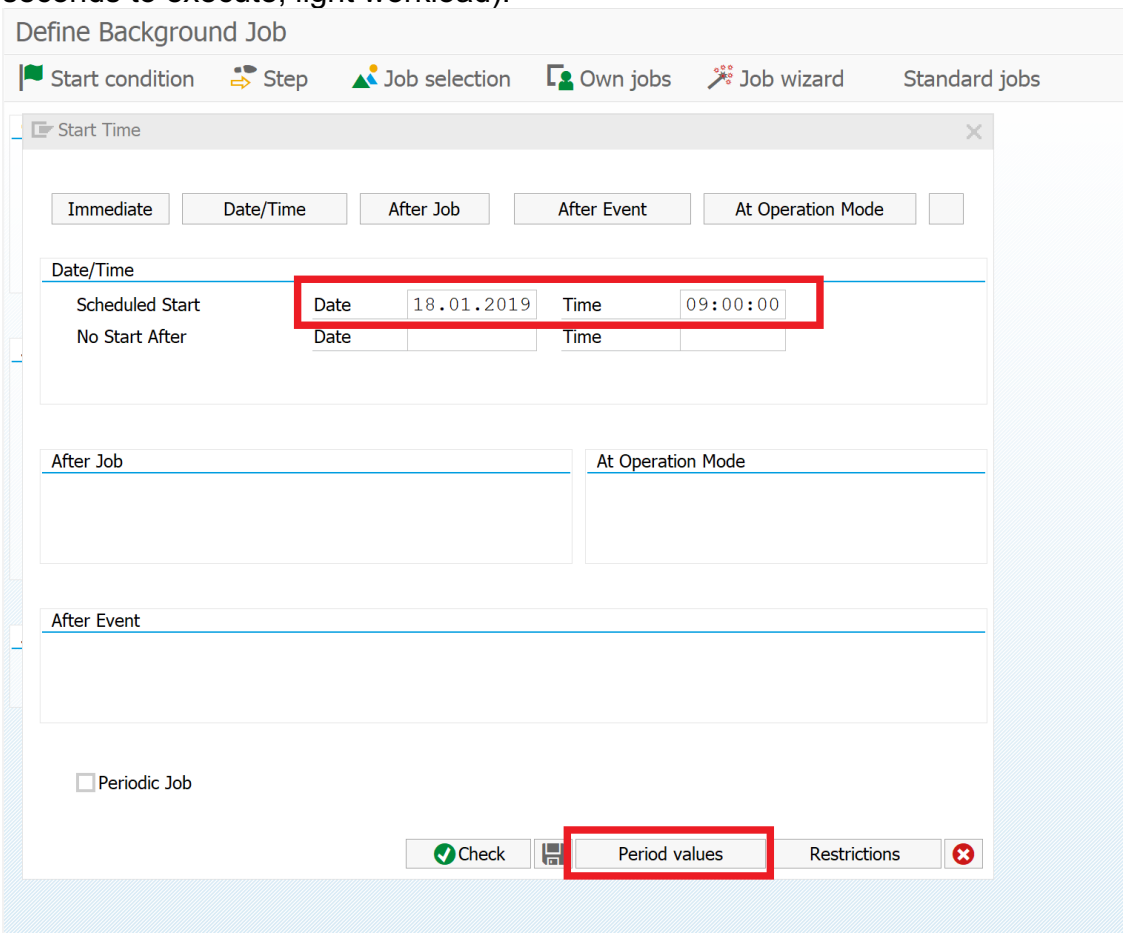



Define Background Job
Start condition
Step
Job selection
Own jobs
Job wizard
Standard jobs
Create Step 1
User
LNKABAP
Program values
ABAP program
External command
External program
ABAP program
Name
/LNKAWS/AWS_STRUST
Variant
Language
EN
External command (command pre-defined by system administrator)
Name
Parameters
Operating sys.
Target server
External program (direct command input by system administrator)
Name
Parameter
Target host
Check
Print specifications
Step List Overview
Spool
No.
Program name/command
Prog. type
Spool list
Parameters
User
Lang.
1
/LNKAWS/AWS_STRUST
ABAP
LNKABAP
EN

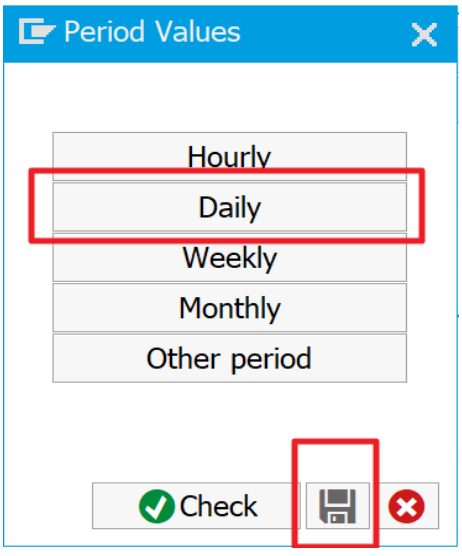

Define Background Job
Start condition
Step
Job selection
Own jobs
Job wizard
Standard jobs
General Data
Job Name
/LNKAWS/LNKAWS_STRUST
Job Class
C
Status
Scheduled
Exec. Target
Spool List Recipient
Job Start
Job Frequency
Job Steps
1 Step(s) successfully defined


Define Background Job
Start condition
Step
Job selection
Own jobs
Job wizard
Standard jobs
Start Time
Immediate
Date/Time
After Job
After Event
At Operation Mode
Date/Time
After Job
At Operation Mode
After Event
Check

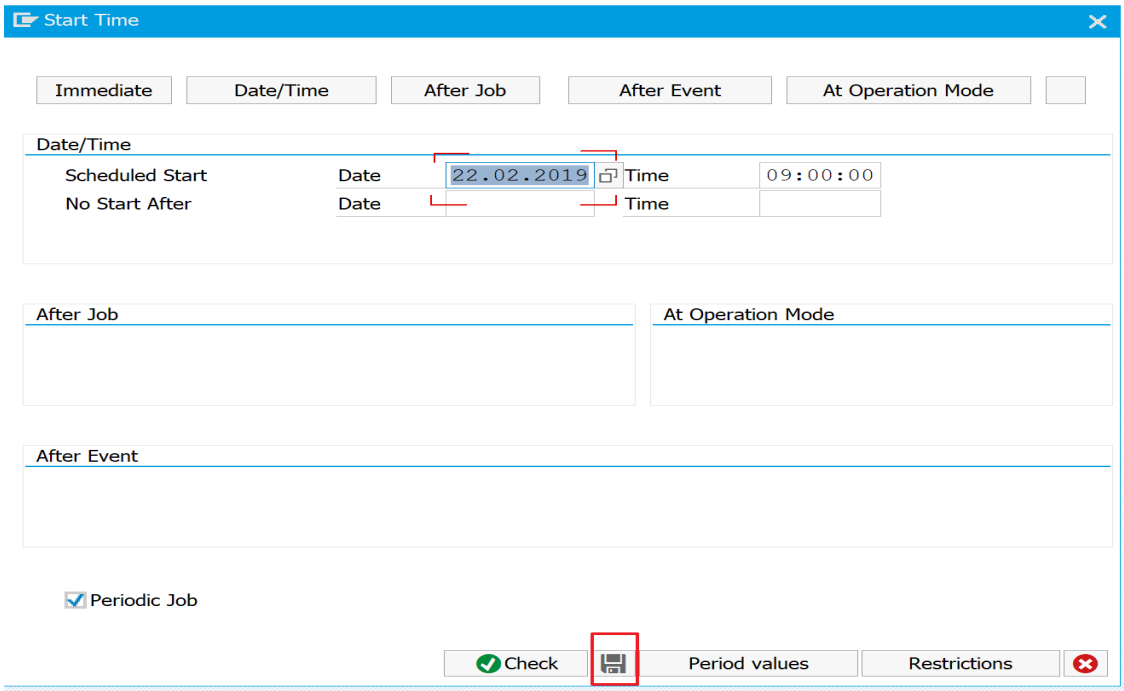
Inform the next day and the time you wish this job to run (the job takes a few seconds to execute, light workload).



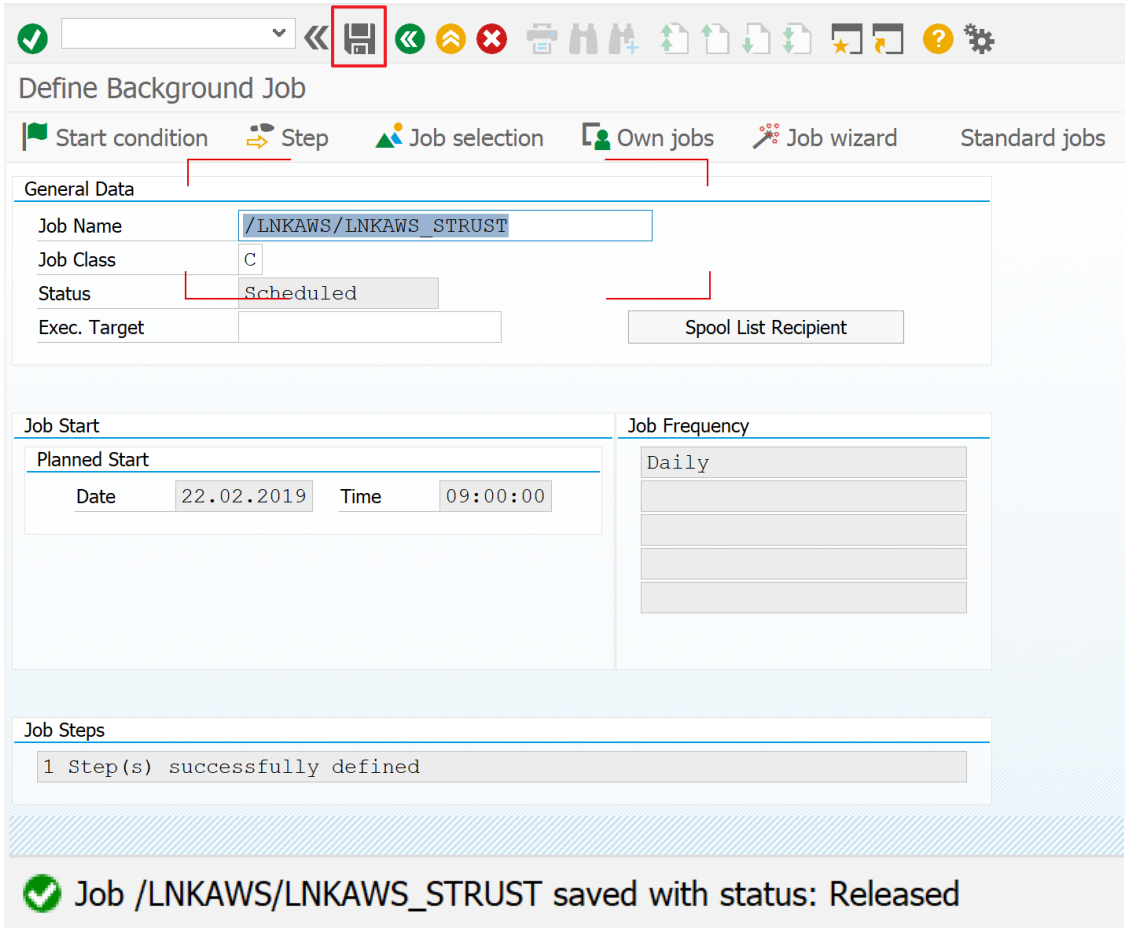
Choose daily period



Save



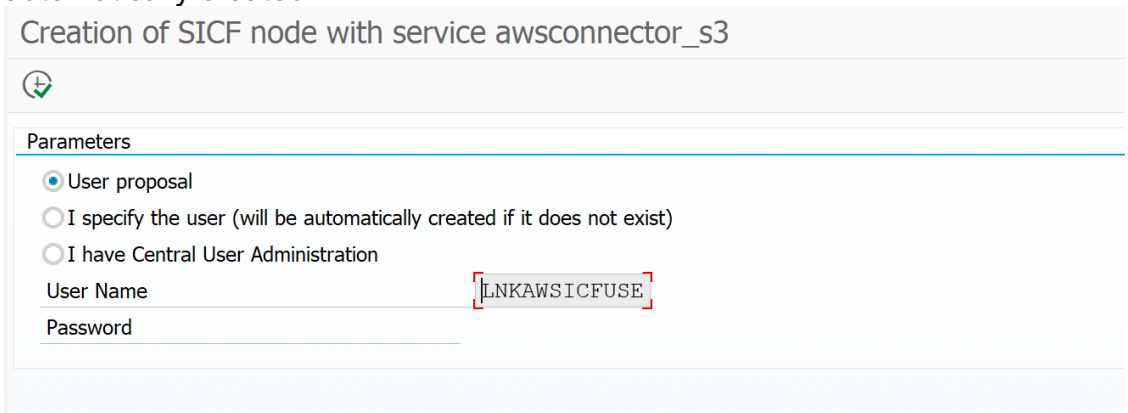
And save



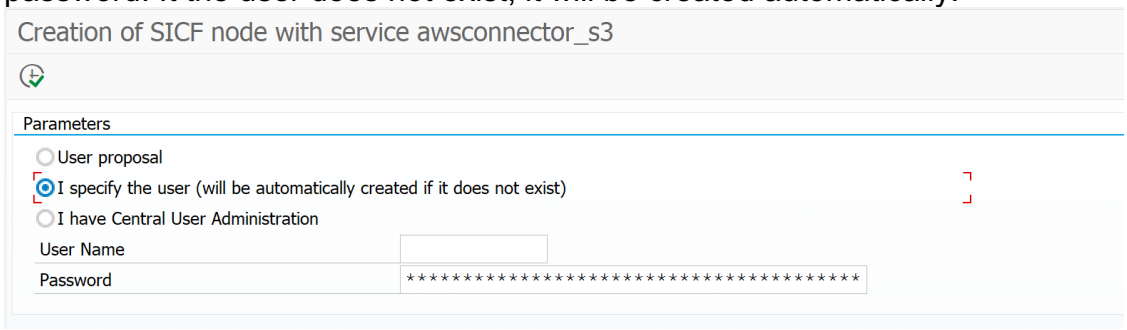
SICF, service awsconnector_s3

Run transaction /N/LNKAWS/SICF.
With this transaction, the SICF service awsconnector_s3 will be created and optionally the user for the service.
A selection screen will appear with a 3 options radio button.

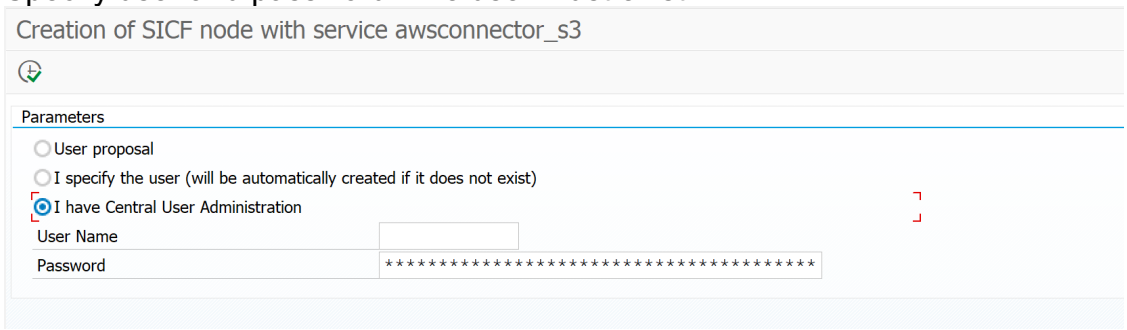
User proposal. The proposed user is LNKAWSICFUSE. This user will be automatically created.



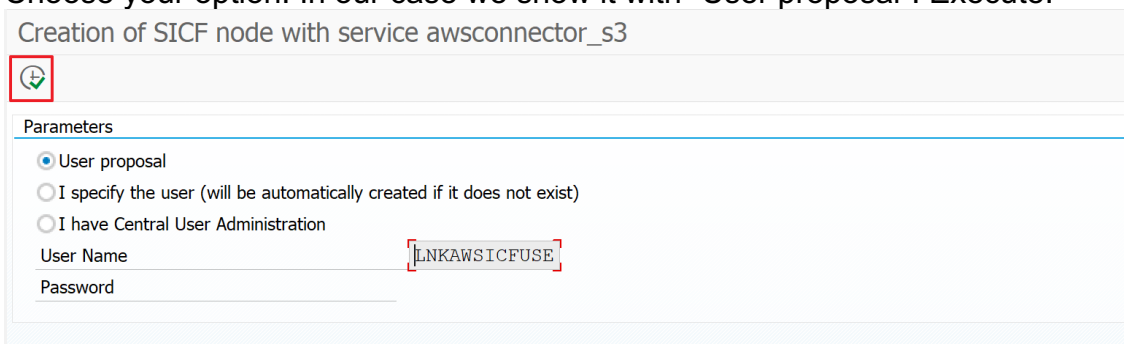
I specify the user. The Username and password fields open. Specify user and password. It the user does not exist, it will be created automatically.



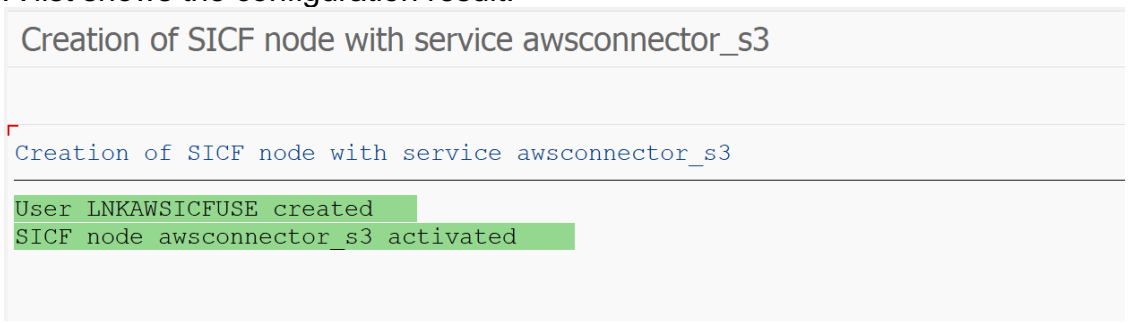
I have Central User Administrator. The Username and password fields open. Specify user and password. The user must exist.



Choose your option. In our case we show it with “User proposal”. Execute.

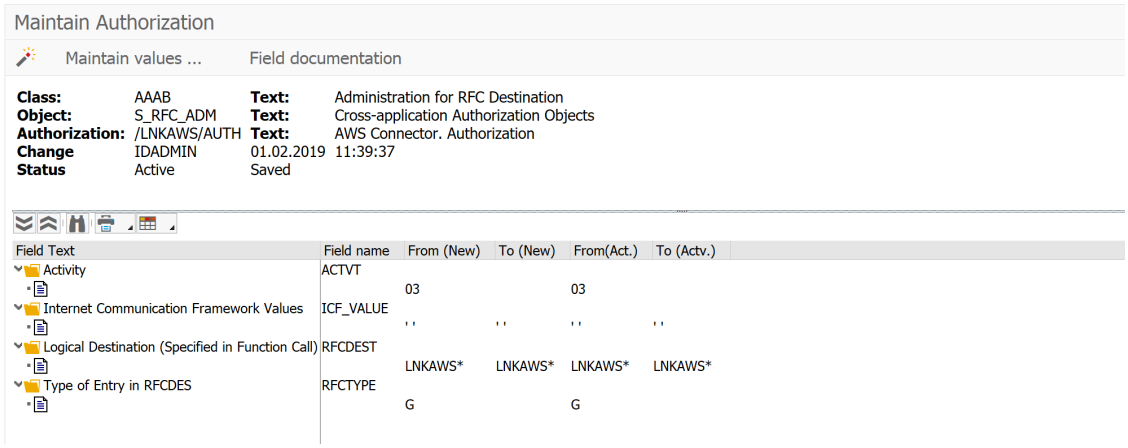


A list shows the configuration result.



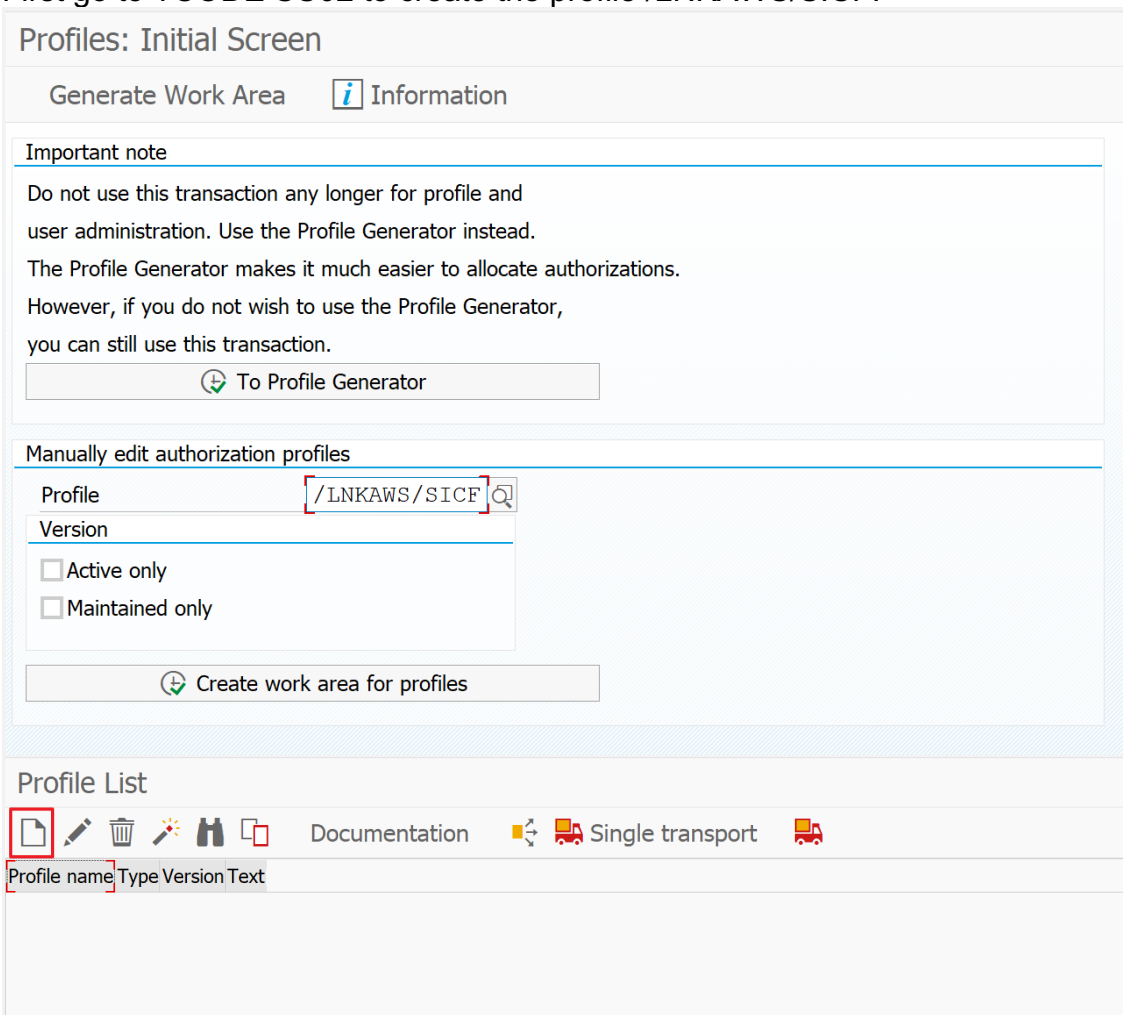
Authorizations details

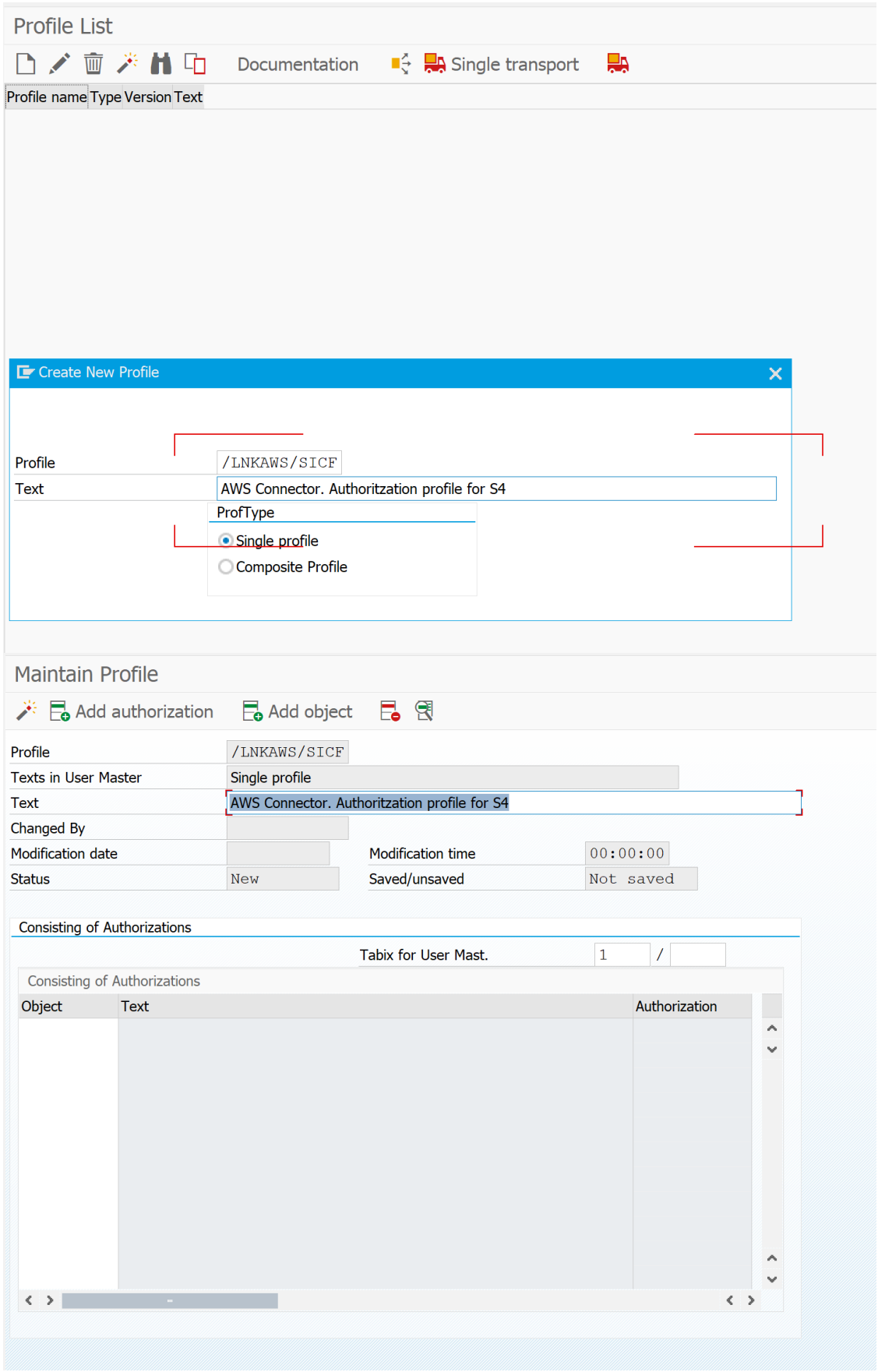
This is just to document what authorizations are given to the SICF user.
The user for the service must have authorization for the object S_RFC_ADM with these values:



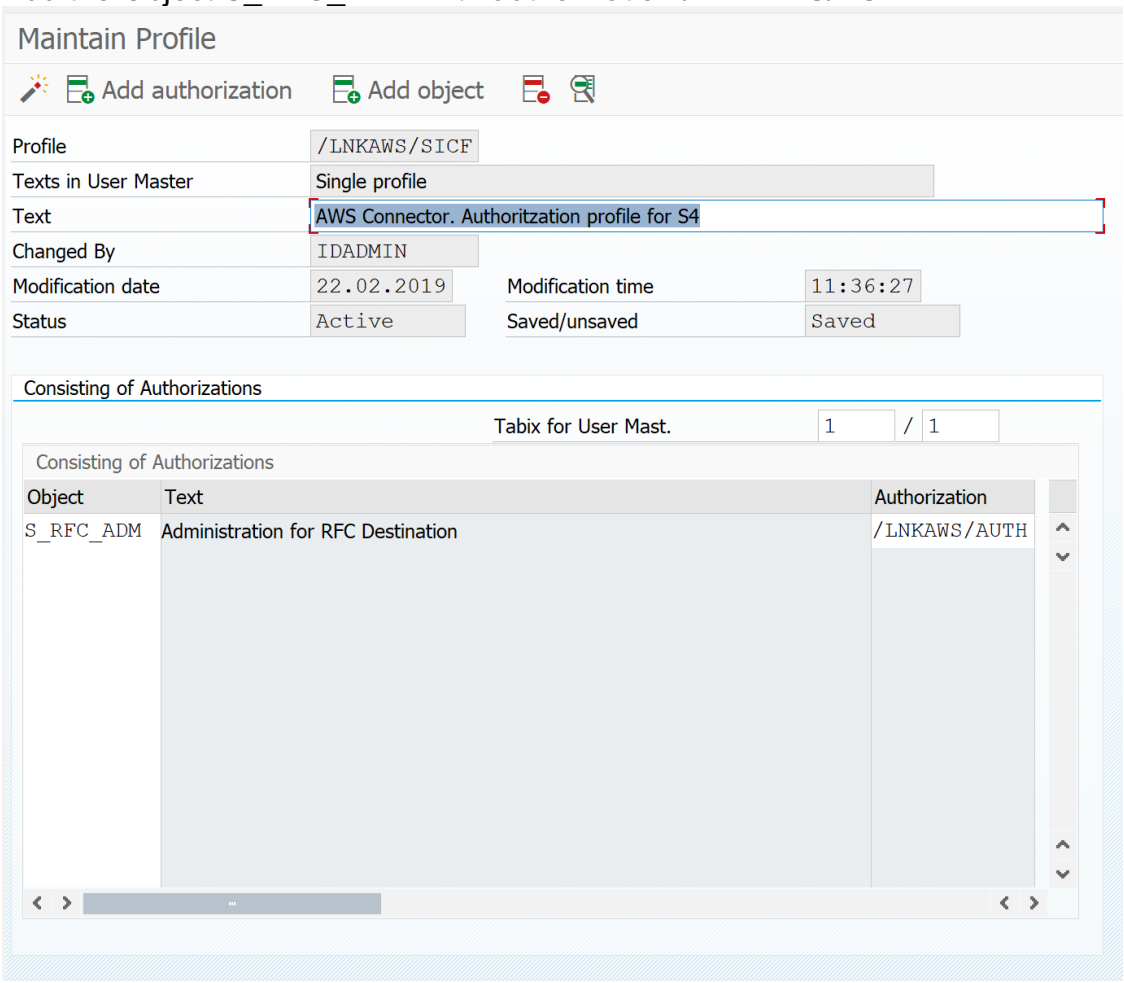
This is done in the profile /LNKAWS/SICF, which is automatically added to the service user.
In some cases we have realized that the profile is not created on an automatic way, so we have created it manually. In order to do this we follow next steps:

First go to TCODE SU02 to create the profile /LNKAWS/SICF.

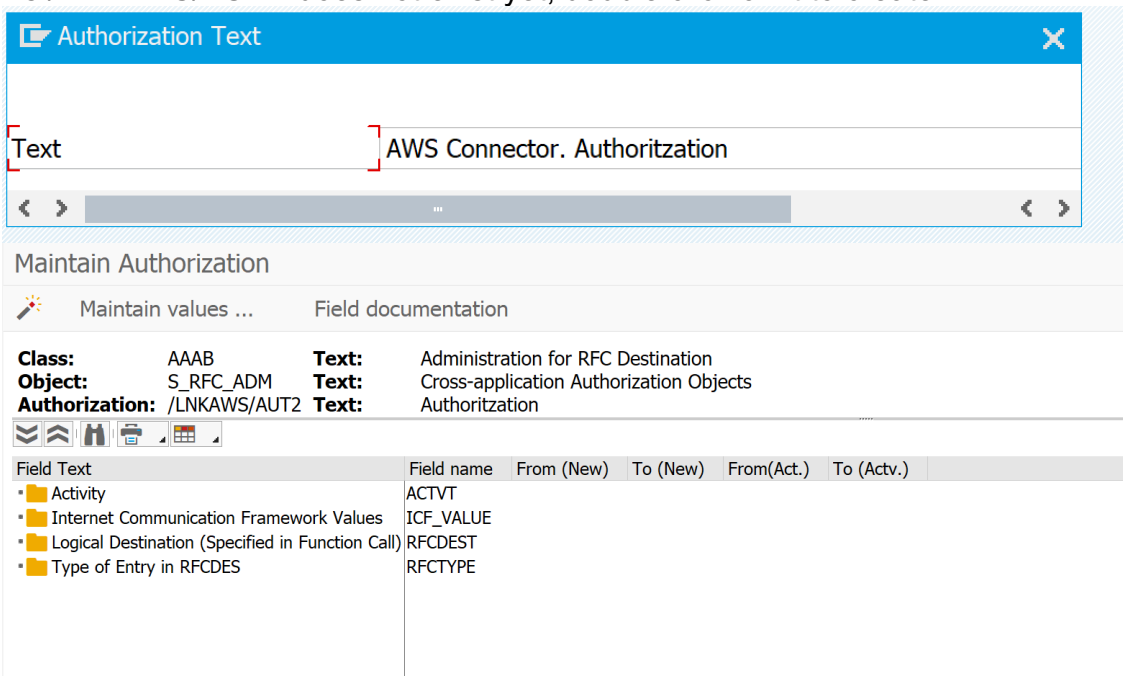



Profile List
Documentation
Single transport
Profile name
Type
Version
Text
Create New Profile
Profile
/LNKAWS/SICF
Text
AWS Connector. Authoritzation profile for S4
ProfType
Single profile
Composite Profile
Maintain Profile
Add authorization
Add object
Profile
/LNKAWS/SICF
Texts in User Master
Single profile
Text
AWS Connector. Authoritzation profile for S4
Changed By
Modification date
Modification time
00:00:00
Status
New
Saved/unsaved
Not saved
Consisting of Authorizations
Tabix for User Mast.
1
Consisting of Authorizations
Object
Text
Authorization

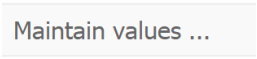
Add the Object S_RFC_ADM with authorization /LNKAWS/AUTH



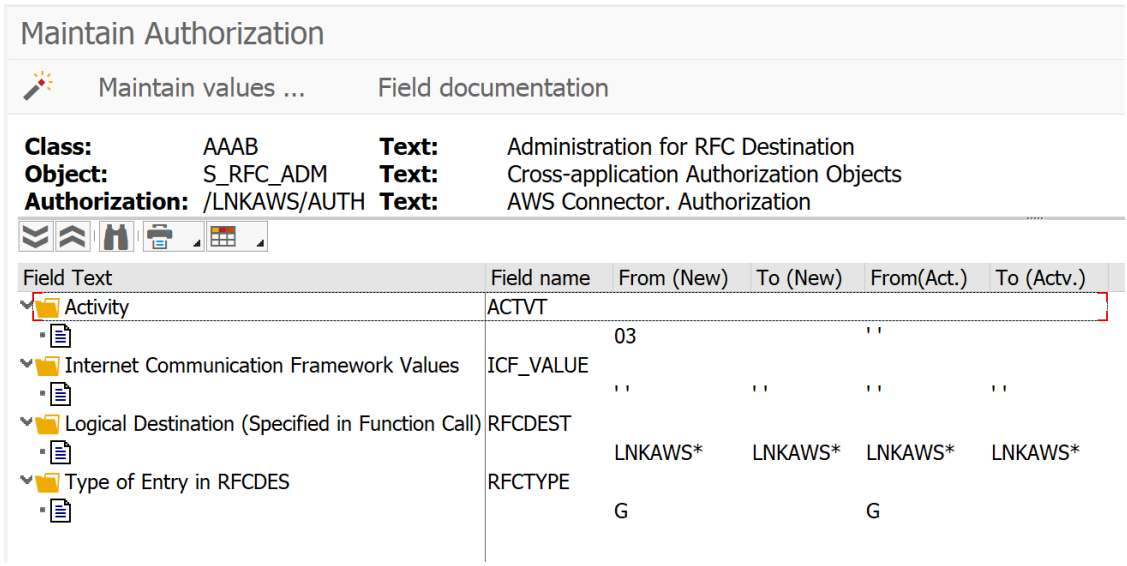
As /LNKAWS/AUTH does not exist yet, double click on it to create



Click on button

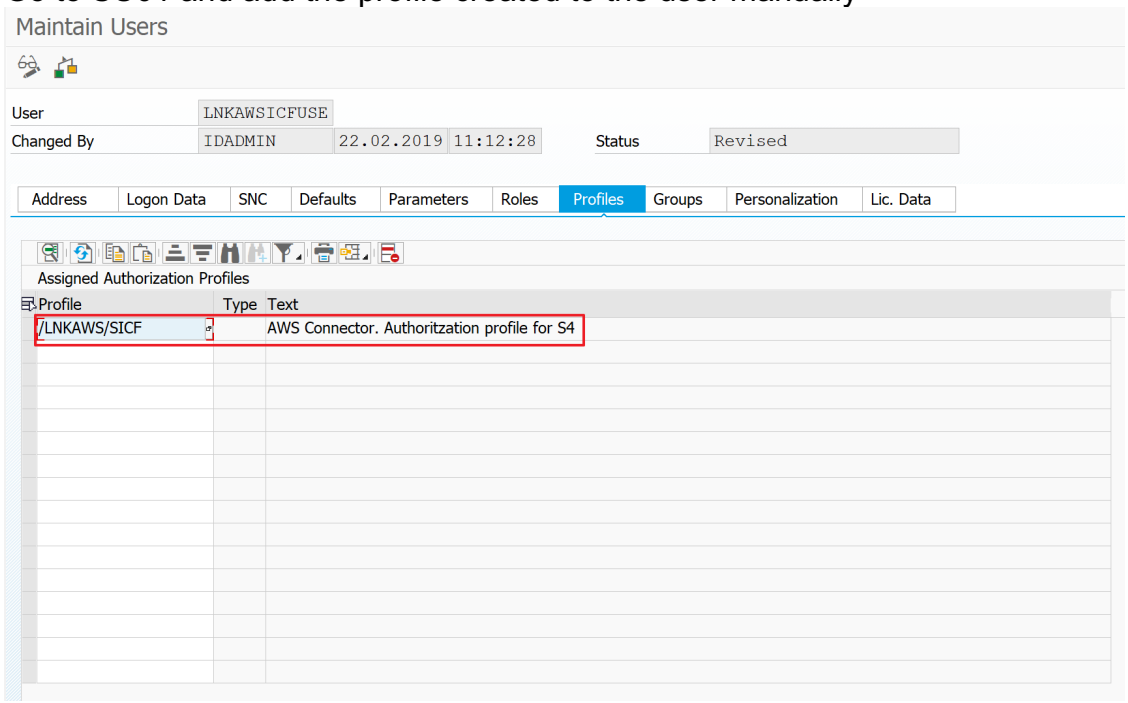


Include the needed values



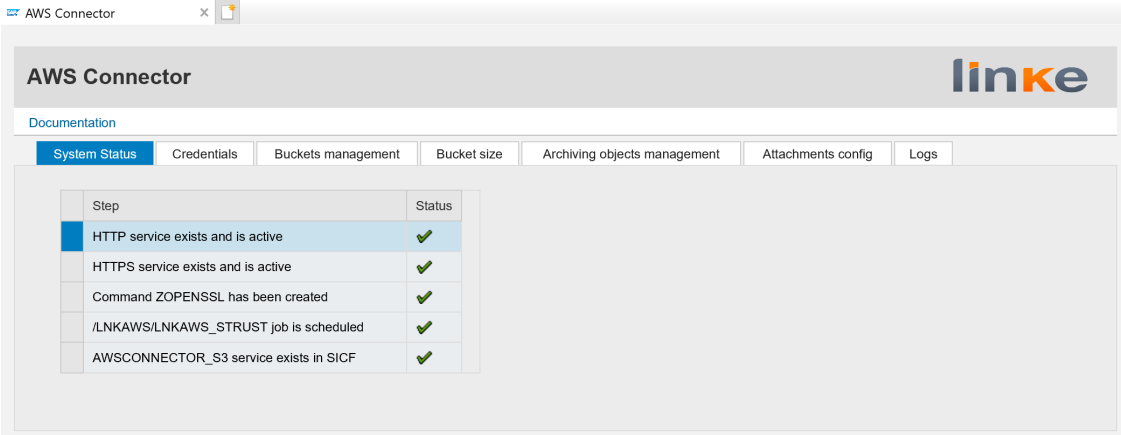
Save and Activate

Go to SU01 and add the profile created to the user manually

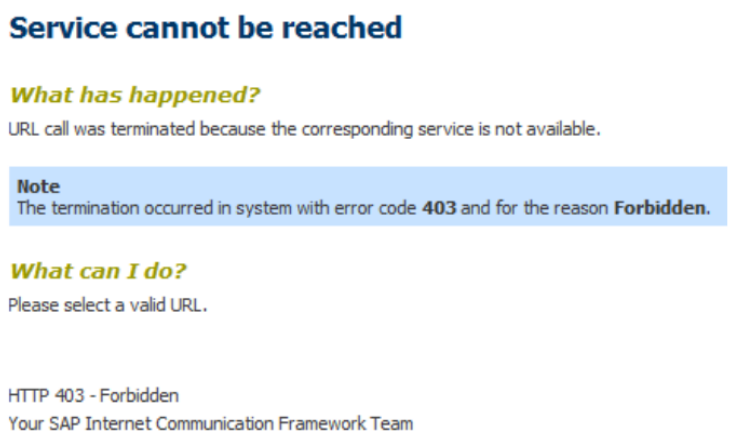


Actions to do in AWS Connector Manager

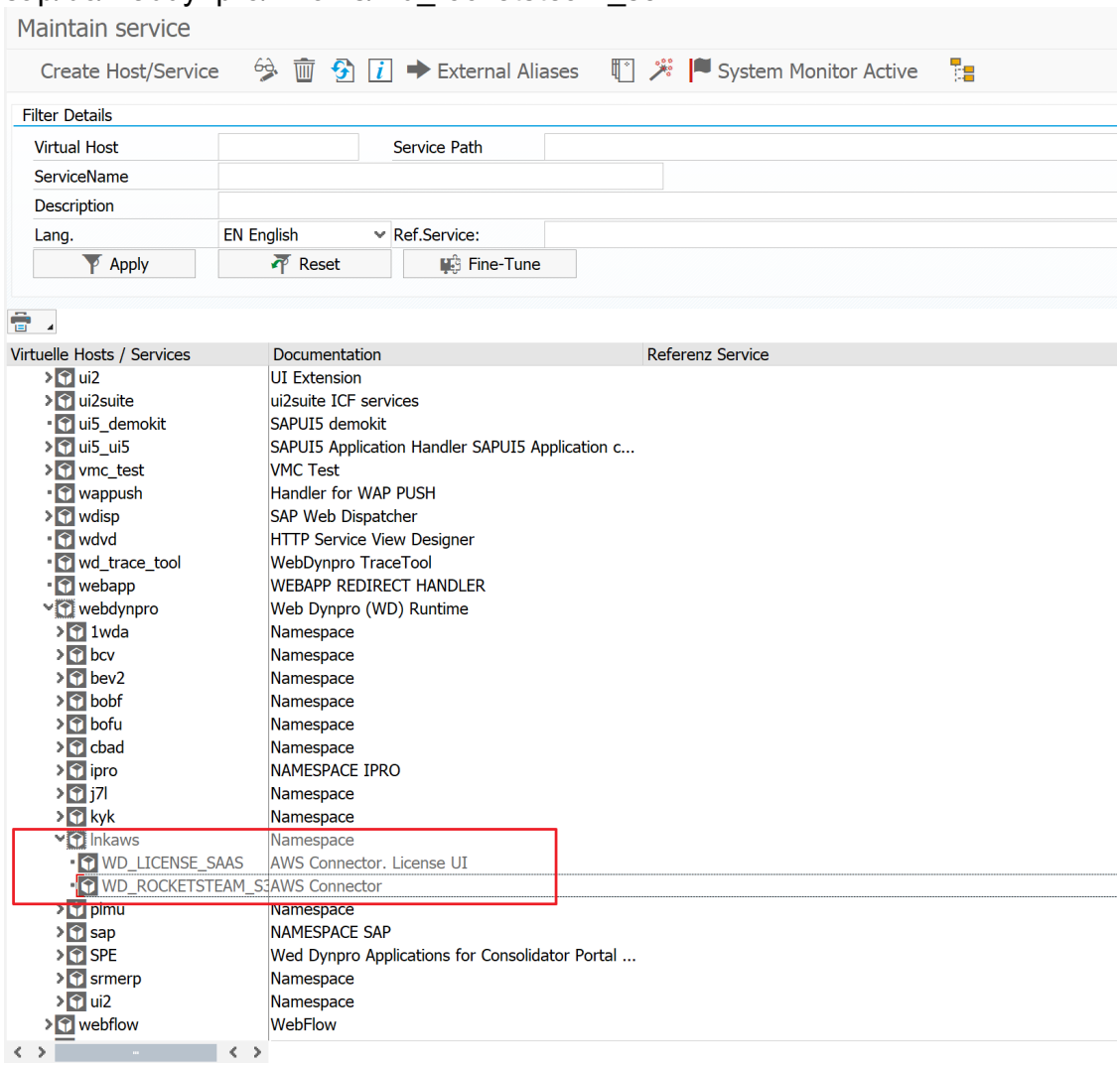
Run transaction /N/LNKAWS/S4MANAGER



Note: In case Service cannot be reached when running transaction /N/LNKAWS/S4MANAGER:

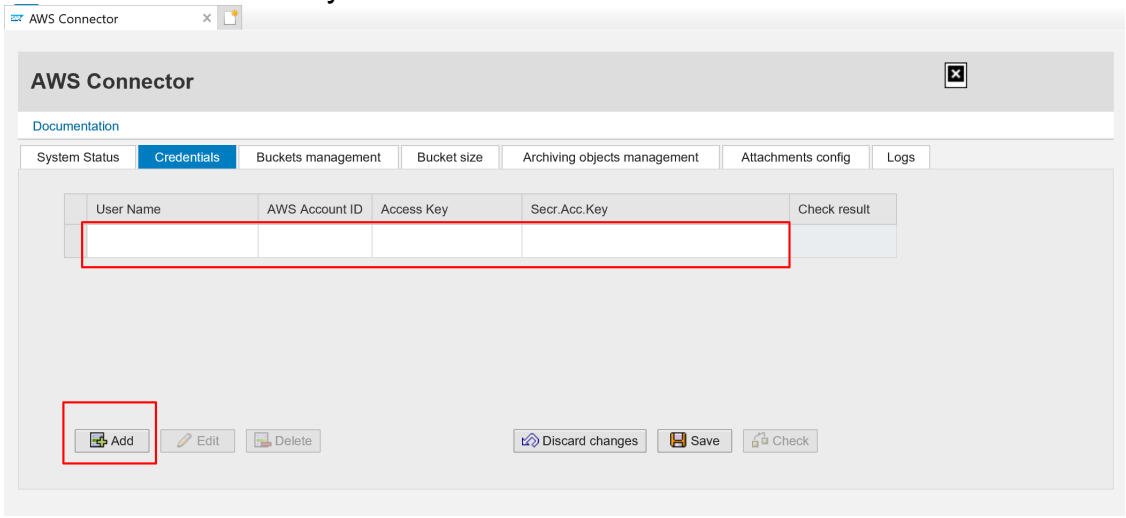


Go to SICF and activate the service in sap/bc/webdynpro/lnkaws/wd_rocketsteam_s3:

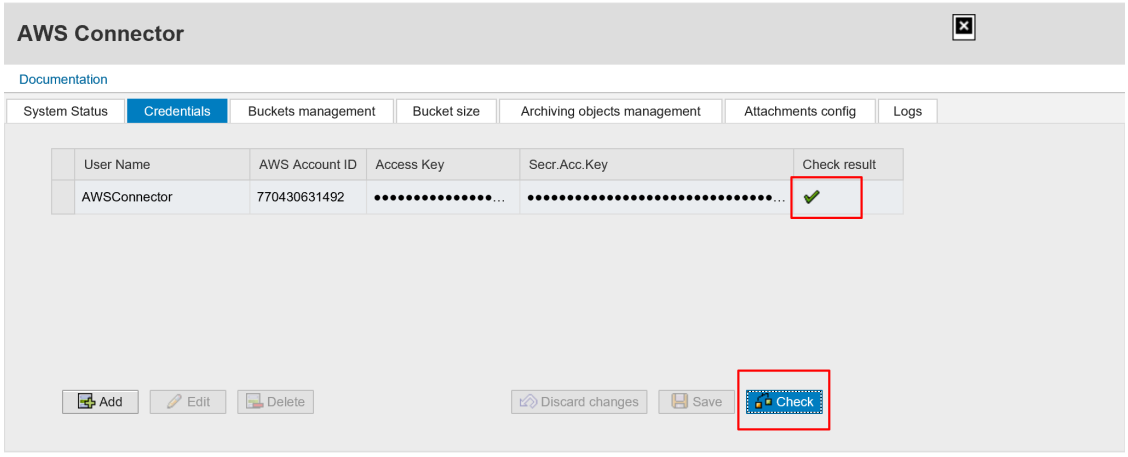


Credentials.

In Credentials tab add your credentials



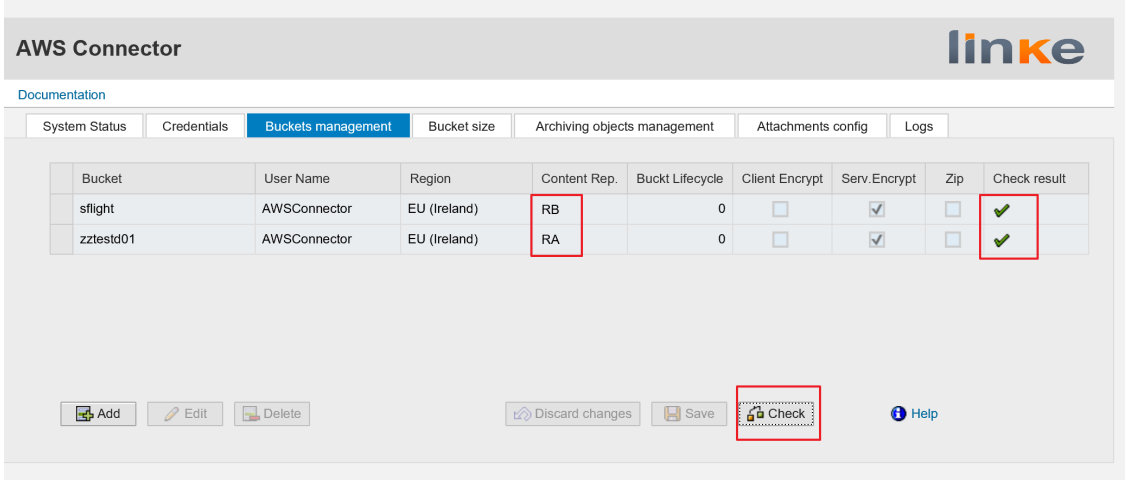
Press Check to check the credentials



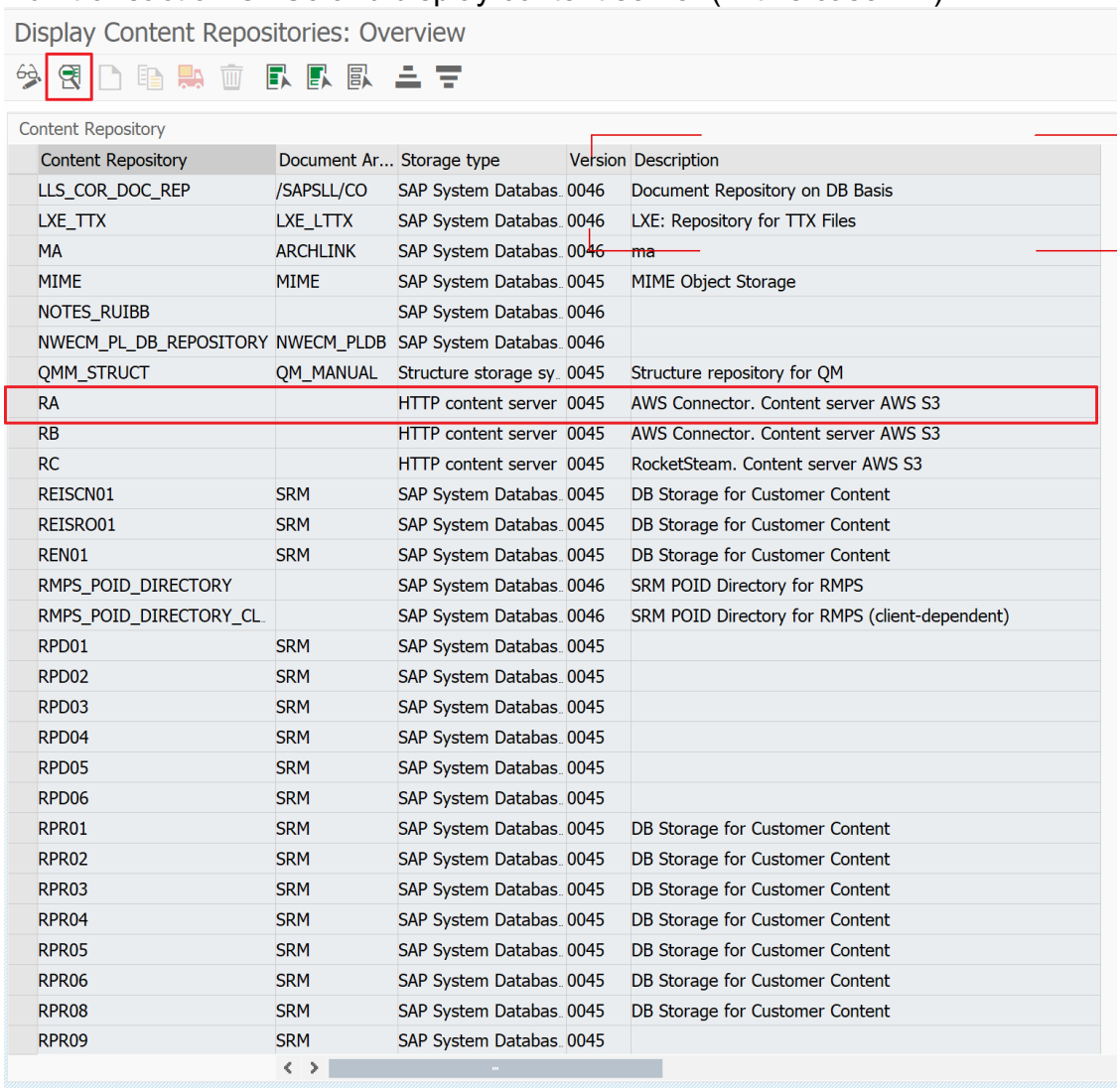
Proceed with Buckets Management tab, and Attachments config.

Create bucket.

In Buckets Management create a bucket. Mind the bucket prefix.
Once created press Check. Check result should be okay.

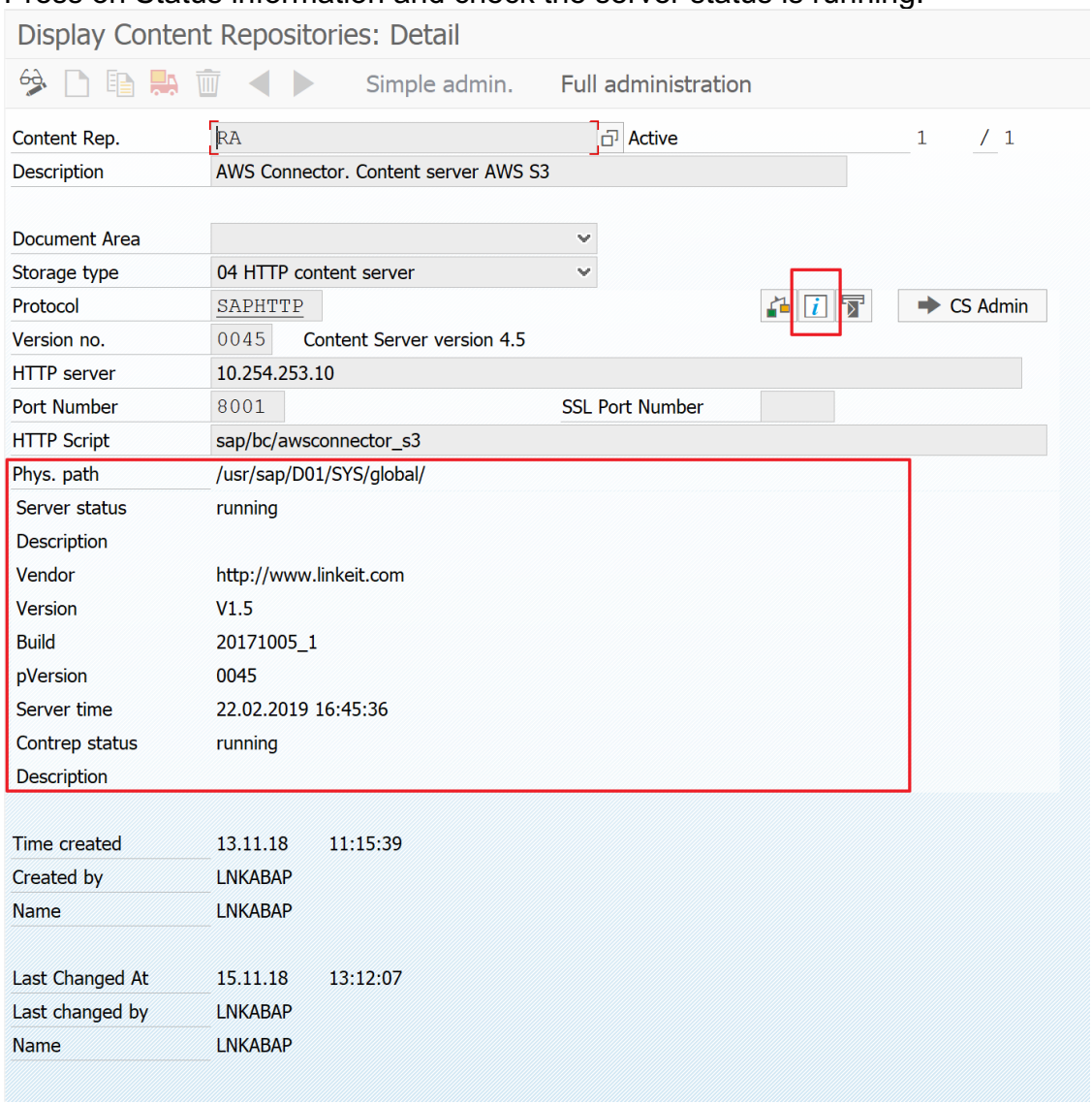


Look at the Content Rep created (this will usually be RA, but may be another in case RA is already existing). This will be used to check the content server.
Check the content server.
Run transaction OAC0 and display content server (in this case RA)

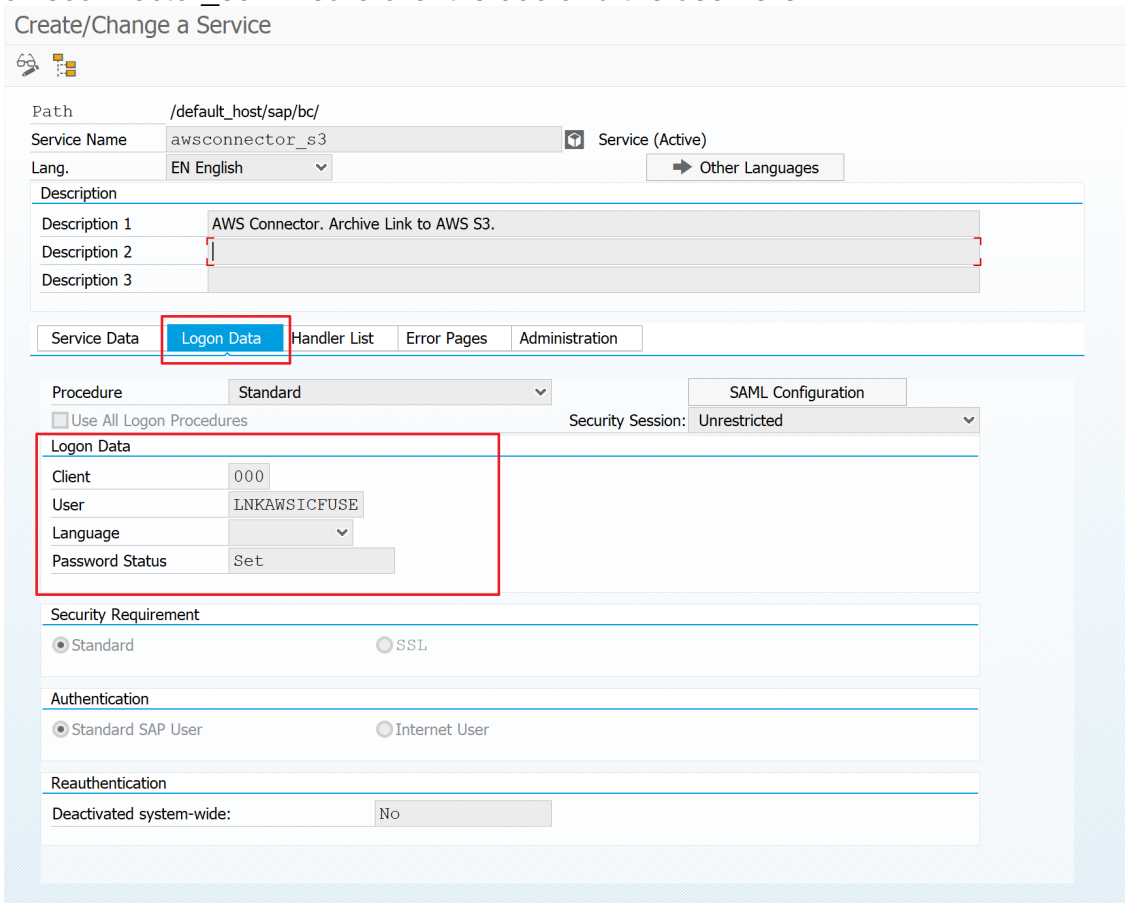


Content Repository	Document Ar...	Storage type	Version	Description
LLS_COR_DOC_REP	/SAPSLL/CO	SAP System Databas...	0046	Document Repository on DB Basis
LXE_TTX	LXE_LTTX	SAP System Databas...	0046	LXE: Repository for TTX Files
MA	ARCHLINK	SAP System Databas...	0046	ma
MIME	MIME	SAP System Databas...	0045	MIME Object Storage
NOTES_RUIBB		SAP System Databas...	0046	
NWECM_PL_DB_REPOSITORY	NWECM_PLDB	SAP System Databas...	0046	
QMM_STRUCT	QM_MANUAL	Structure storage sy...	0045	Structure repository for QM
RA		HTTP content server	0045	AWS Connector. Content server AWS S3
RB		HTTP content server	0045	AWS Connector. Content server AWS S3
RC		HTTP content server	0045	RocketSteam. Content server AWS S3
REISCN01	SRM	SAP System Databas...	0045	DB Storage for Customer Content
REISRO01	SRM	SAP System Databas...	0045	DB Storage for Customer Content
REN01	SRM	SAP System Databas...	0045	DB Storage for Customer Content
RMPS_POID_DIRECTORY		SAP System Databas...	0046	SRM POID Directory for RMPS
RMPS_POID_DIRECTORY_CL...		SAP System Databas...	0046	SRM POID Directory for RMPS (client-dependent)
RPD01	SRM	SAP System Databas...	0045	
RPD02	SRM	SAP System Databas...	0045	
RPD03	SRM	SAP System Databas...	0045	
RPD04	SRM	SAP System Databas...	0045	
RPD05	SRM	SAP System Databas...	0045	
RPD06	SRM	SAP System Databas...	0045	
RPR01	SRM	SAP System Databas...	0045	DB Storage for Customer Content
RPR02	SRM	SAP System Databas...	0045	DB Storage for Customer Content
RPR03	SRM	SAP System Databas...	0045	DB Storage for Customer Content
RPR04	SRM	SAP System Databas...	0045	DB Storage for Customer Content
RPR05	SRM	SAP System Databas...	0045	DB Storage for Customer Content
RPR06	SRM	SAP System Databas...	0045	DB Storage for Customer Content
RPR08	SRM	SAP System Databas...	0045	DB Storage for Customer Content
RPR09	SRM	SAP System Databas...	0045	

Press on Status information and check the server status is running.

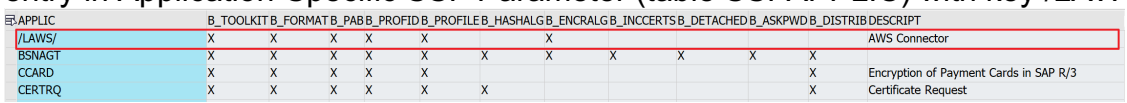


Note: In case server status is not running, check the user in the service SICF awsconnector_s3. Ensure client is 000 and the user is OK.



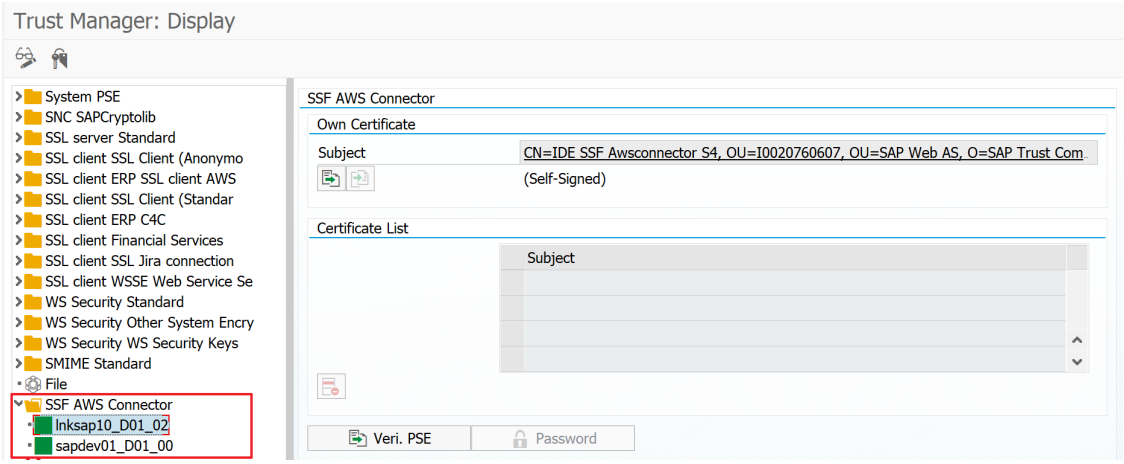
SSF configuration.

You can skip SSF configuration in case you do not plan to use Client Encrypt.
If you plan to use the option “Client Encrypt”, SSF is used to encrypt the files before uploading to AWS S3, and decrypt it after downloading from AWS S3.
In this way, the files stored in AWS S3 can only be retrieved by your system.
Automatic configuration SSF will be automatically configured as soon as you create your first Bucket with the option “Client Encrypt”. AWS Connector creates an entry in Application-Specific SSF Parameter (table SSFAPPLIC) with key /LAWS/:



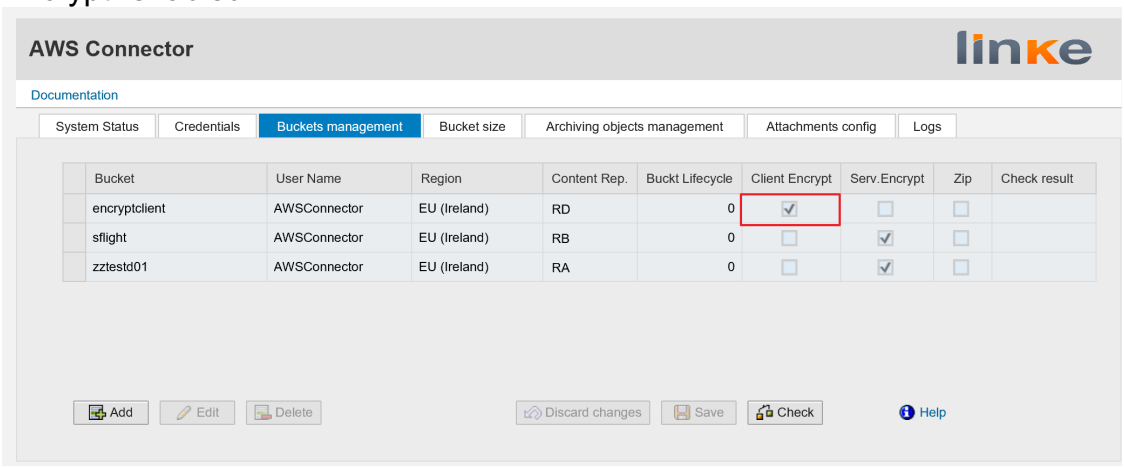
APPLIC	B_TOOLKIT	B_FORMAT	B_PAB	B_PROFID	B_PROFILE	B_HASHALG	B_ENCRALG	B_INCCERTS	B_DETACHED	B_ASKPWD	B_DISTRIB	DESCRIPT
/LAWS/	X	X	X	X	X		X					AWS Connector
BSNAGT	X	X	X	X	X	X	X	X	X	X	X	
CCARD	X	X	X	X	X						X	Encryption of Payment Cards in SAP R/3
CERTRQ	X	X	X	X	X	X					X	Certificate Request

AWS Connector creates also in STRUST the PSE for SSF AWS Connector:

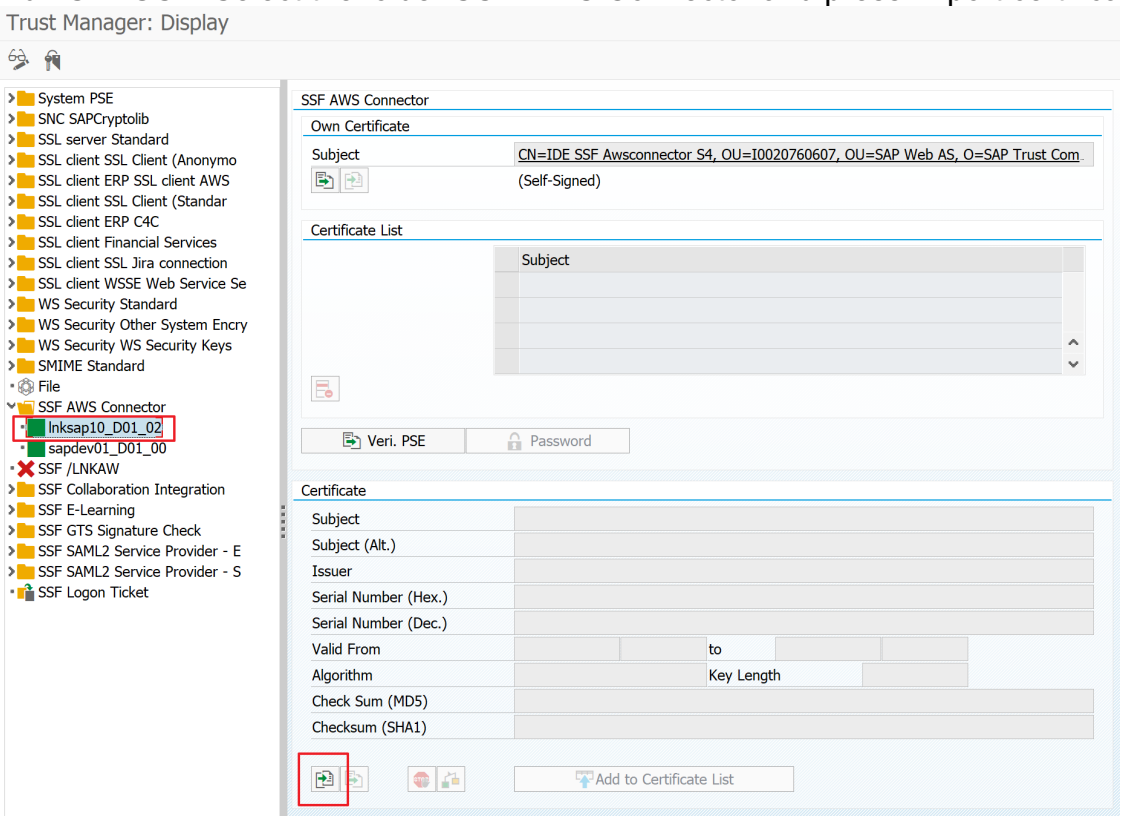


Configuration of your own SSL certificate

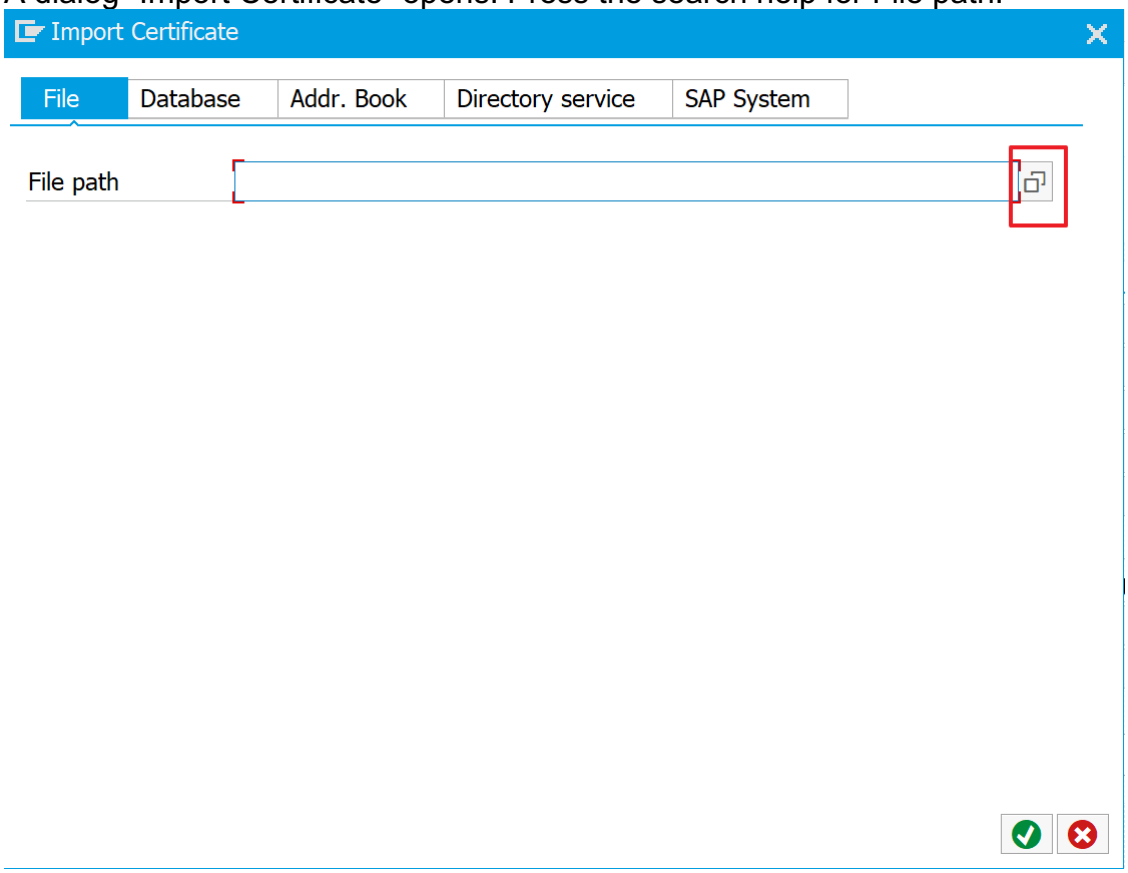
If you plan to use your own SSL certificate, you must follow this procedure.
Run transaction /N/LNKAWS/S4MANAGER and create a first bucket with “Client Encrypt” enabled:



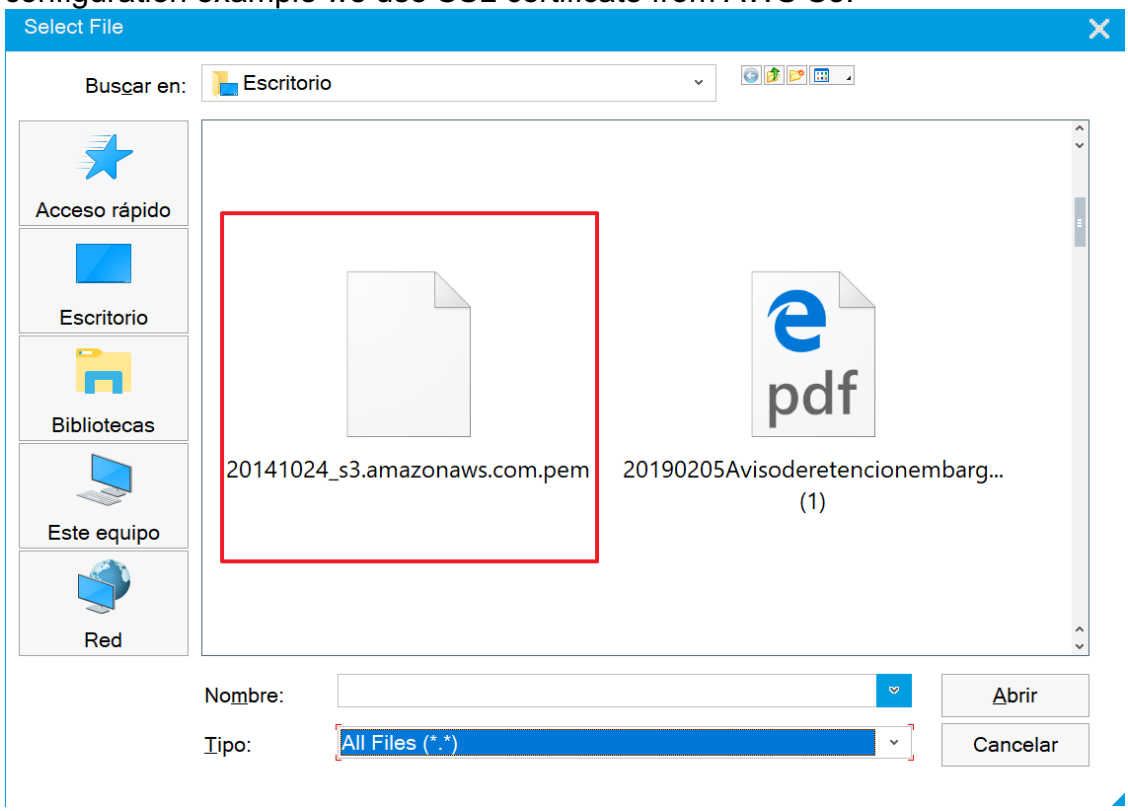
AWS Connector performs automatic configurations, explained above.
Run STRUST. Select the folder SSF AWS Connector and press Import certificate.



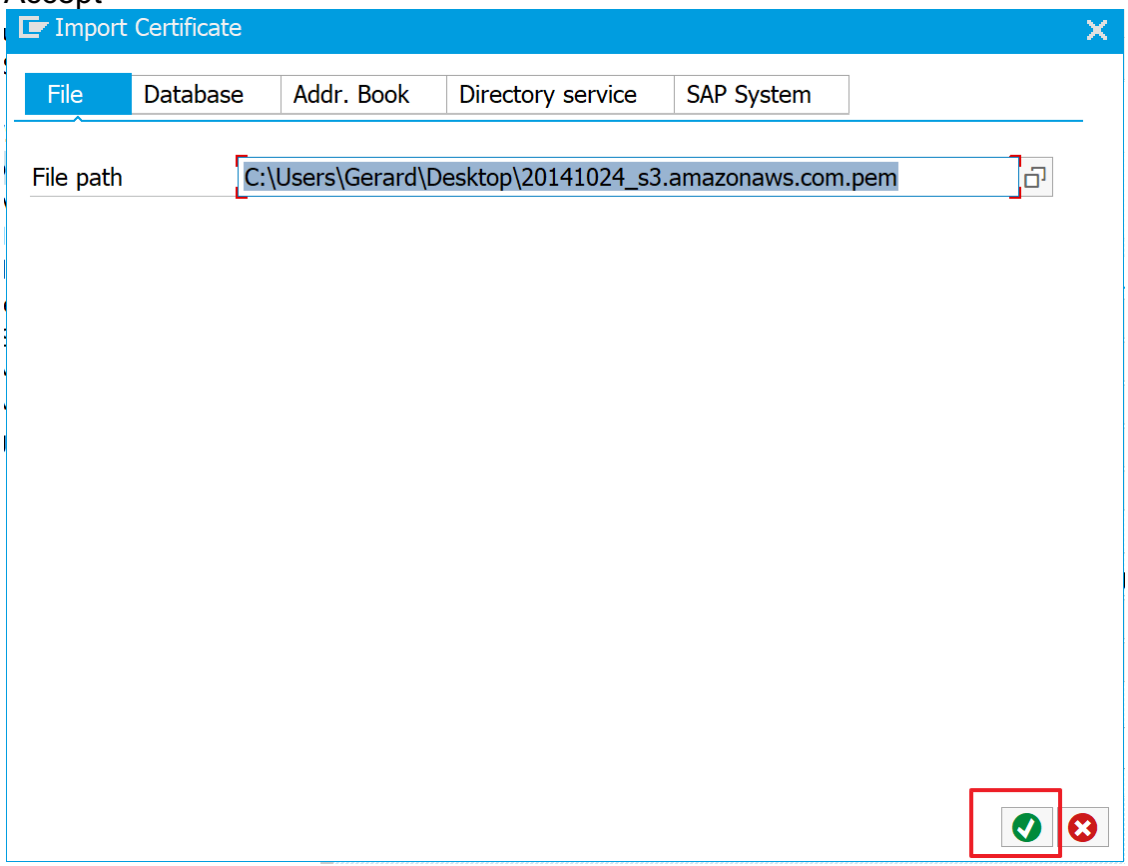
A dialog “Import Certificate” opens. Press the search help for File path.



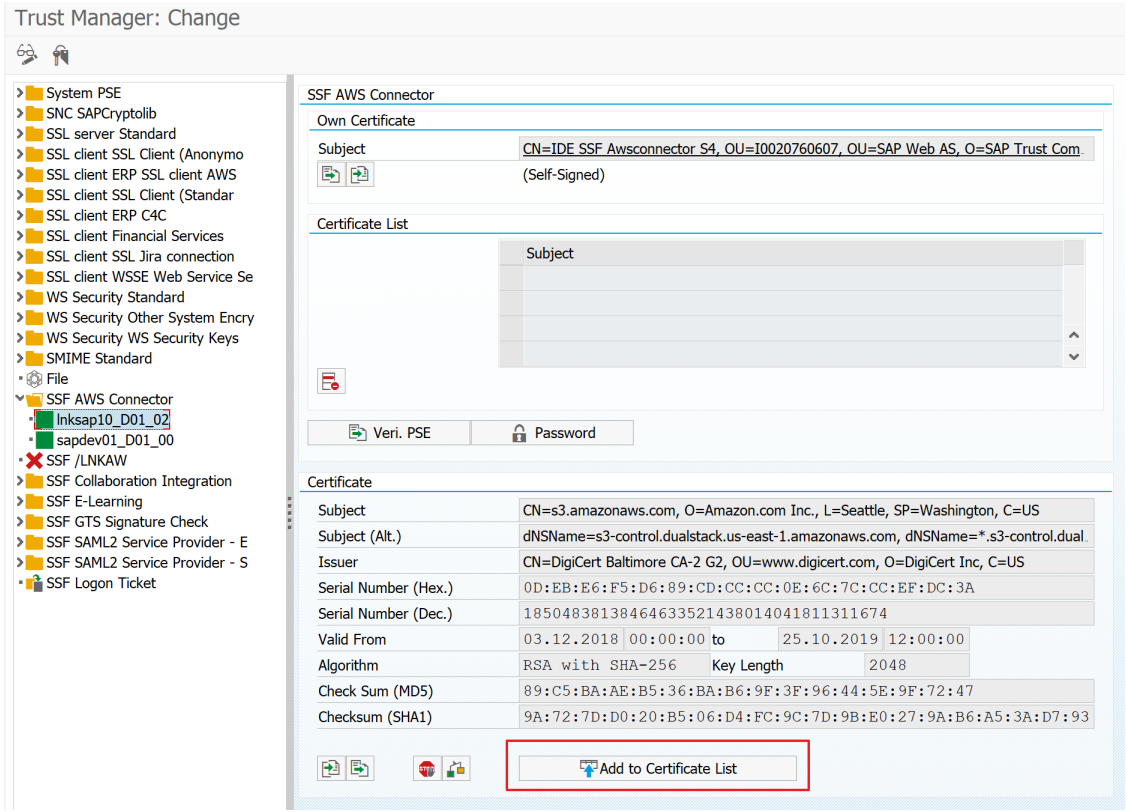
A file browser dialog opens. Choose a pem file containing your certificate. In this configuration example we use SSL certificate from AWS S3.



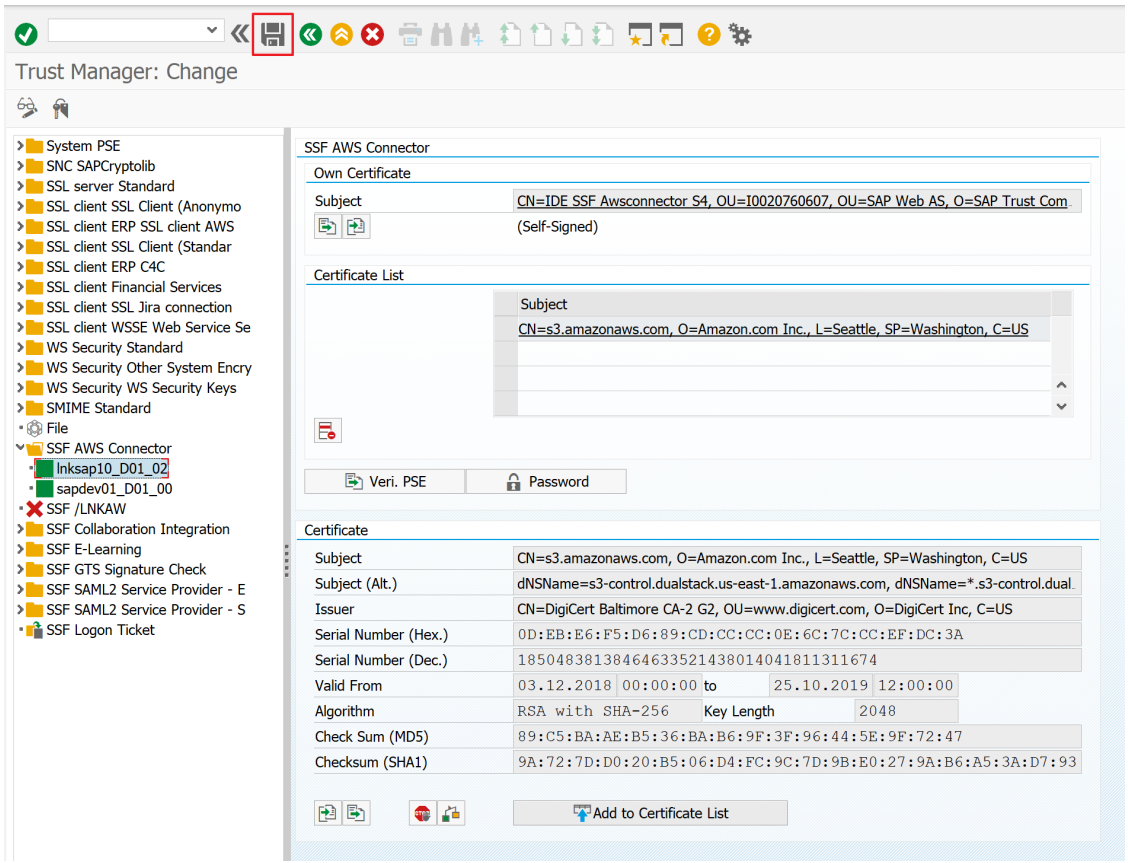
Accept



Press “Add to Certificate List”

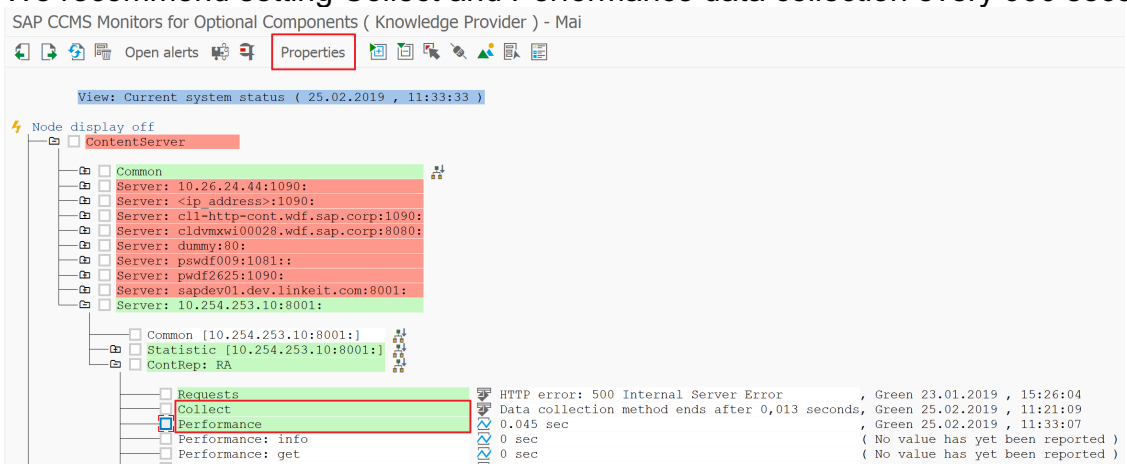


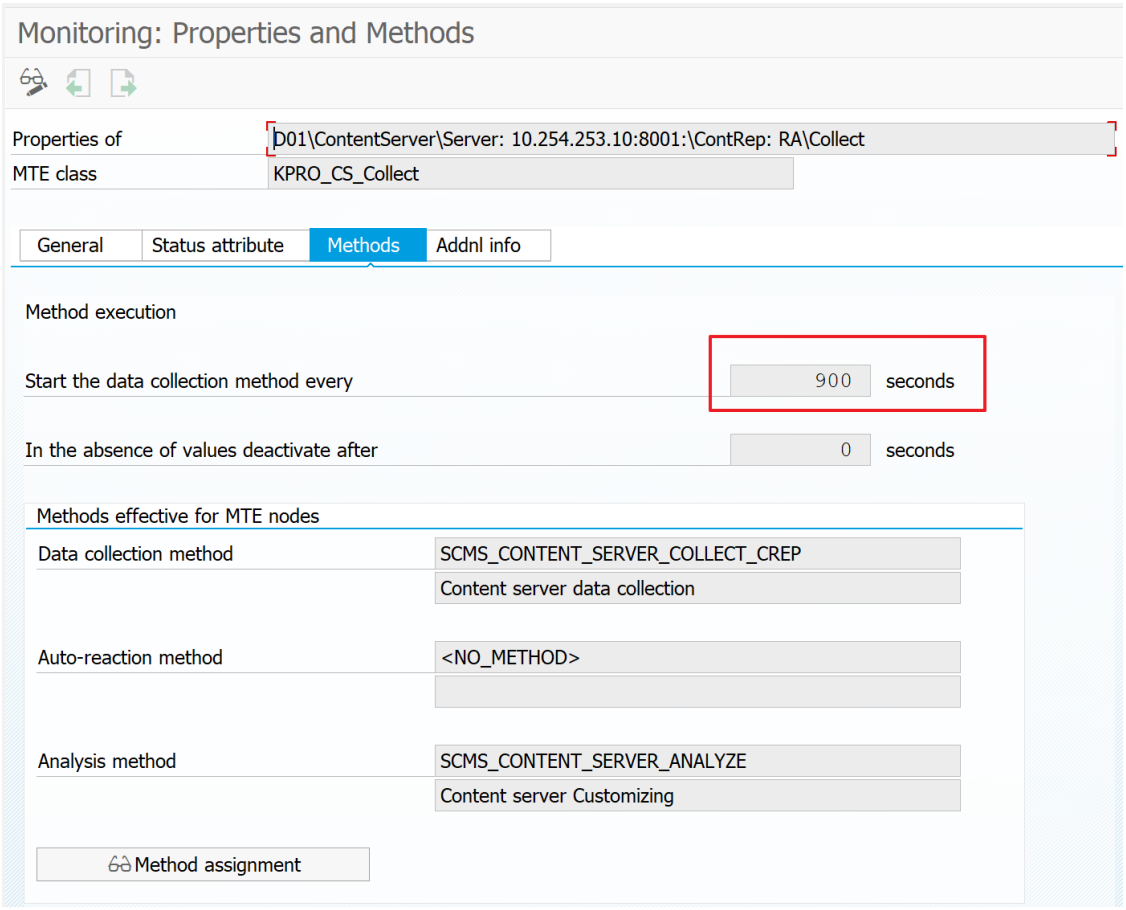
Press Save

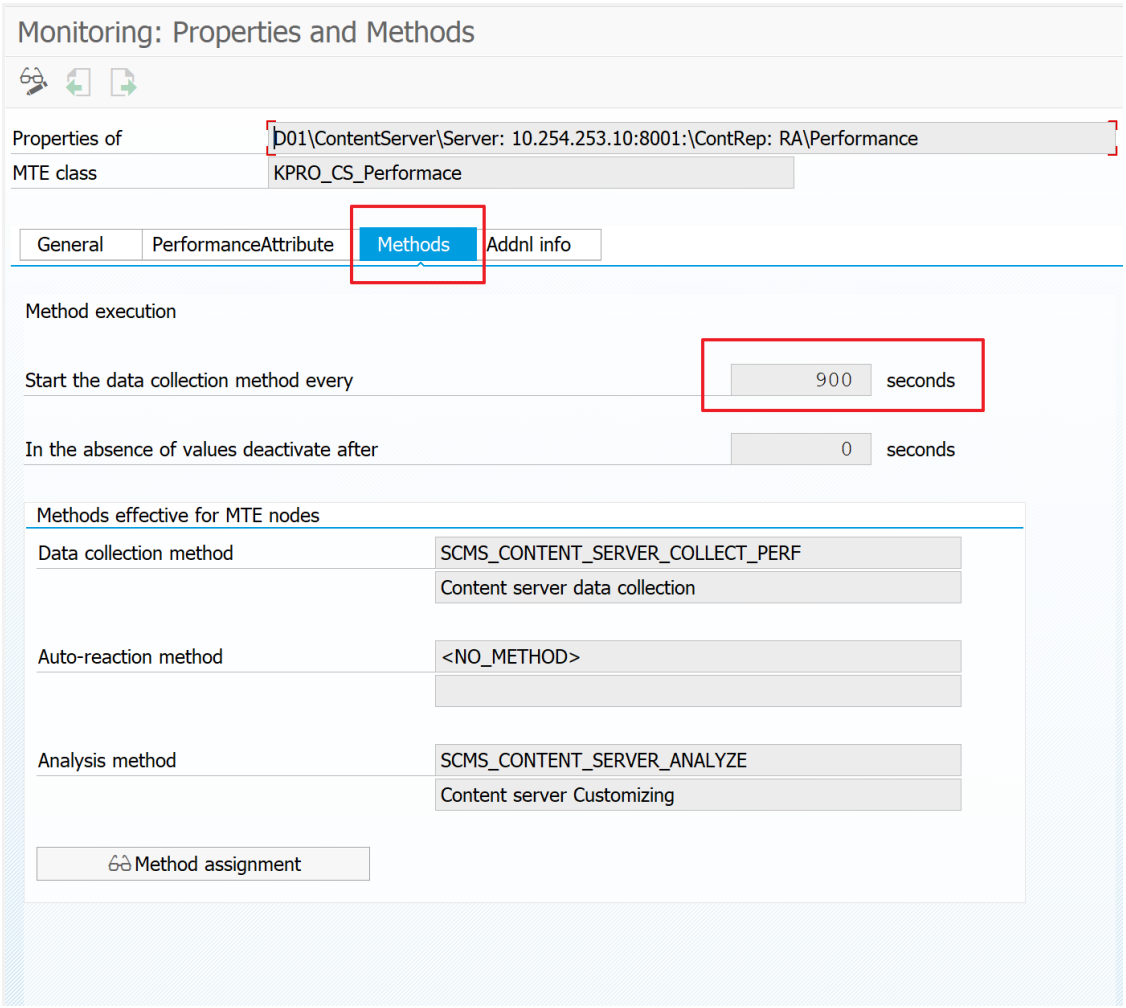

Trust Manager: Change
System PSE
SNC SAPCryptolib
SSL server Standard
SSL client SSL Client (Anonymo
SSL client ERP SSL client AWS
SSL client SSL Client (Standar
SSL client ERP C4C
SSL client Financial Services
SSL client SSL Jira connection
SSL client WSSE Web Service Se
WS Security Standard
WS Security Other System Encry
WS Security WS Security Keys
SMIME Standard
File
SSF AWS Connector
lnksap10_D01_02
sapdev01_D01_00
SSF /LNKAW
SSF Collaboration Integration
SSF E-Learning
SSF GTS Signature Check
SSF SAML2 Service Provider - E
SSF SAML2 Service Provider - S
SSF Logon Ticket
SSF AWS Connector
Own Certificate
Subject
CN=IDE SSF Awsconnector S4, OU=I0020760607, OU=SAP Web AS, O=SAP Trust Com
(Self-Signed)
Certificate List
Subject
CN=s3.amazonaws.com, O=Amazon.com Inc., L=Seattle, SP=Washington, C=US
Veri. PSE
Password
Certificate
Subject
CN=s3.amazonaws.com, O=Amazon.com Inc., L=Seattle, SP=Washington, C=US
Subject (Alt.)
dNSName=s3-control.dualstack.us-east-1.amazonaws.com, dNSName=*.s3-control.dual
Issuer
CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US
Serial Number (Hex.)
0D:EB:E6:F5:D6:89:CD:CC:CC:0E:6C:7C:CC:EF:DC:3A
Serial Number (Dec.)
18504838138464633521438014041811311674
Valid From
03.12.2018 00:00:00 to 25.10.2019 12:00:00
Algorithm
RSA with SHA-256
Key Length
2048
Check Sum (MD5)
89:C5:BA:AE:B5:36:BA:B6:9F:3F:96:44:5E:9F:72:47
Checksum (SHA1)
9A:72:7D:D0:20:B5:06:D4:FC:9C:7D:9B:E0:27:9A:B6:A5:3A:D7:93
Add to Certificate List

Monitoring settings (SCMSMO)

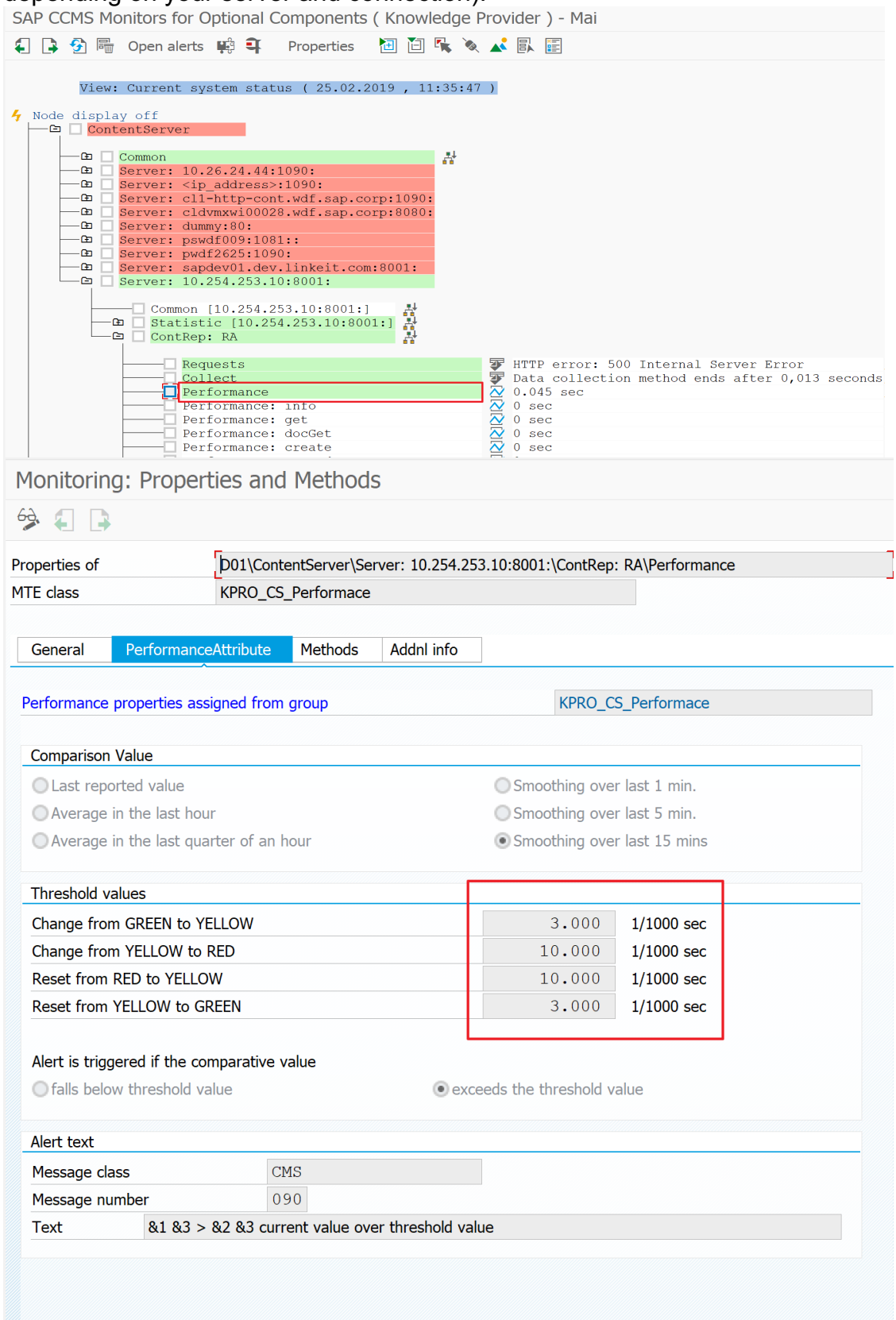
For each bucket you created, a Content Repository is created with name RX (Starting with RA … RZ … SA… SZ…).
In transaction **SCMSMO** you can access to monitoring.
We recommend setting Collect and Performance data collection every 900 seconds.




Monitoring: Properties and Methods
Properties of
D01\ContentServer\Server: 10.254.253.10:8001:\ContRep: RA\Collect
MTE class
KPRO_CS_Collect
General
Status attribute
Methods
Addnl info
Method execution
Start the data collection method every
900
seconds
In the absence of values deactivate after
0
seconds
Methods effective for MTE nodes
Data collection method
SCMS_CONTENT_SERVER_COLLECT_CREP
Content server data collection
Auto-reaction method
<NO_METHOD>
Analysis method
SCMS_CONTENT_SERVER_ANALYZE
Content server Customizing
Method assignment


Monitoring: Properties and Methods
Properties of
D01\ContentServer\Server: 10.254.253.10:8001:\ContRep: RA\Performance
MTE class
KPRO_CS_Performace
General
PerformanceAttribute
Methods
Addnl info
Method execution
Start the data collection method every
900
seconds
In the absence of values deactivate after
0
seconds
Methods effective for MTE nodes
Data collection method
SCMS_CONTENT_SERVER_COLLECT_PERF
Content server data collection
Auto-reaction method
<NO_METHOD>
Analysis method
SCMS_CONTENT_SERVER_ANALYZE
Content server Customizing
Method assignment

We also recommend Performance threshold values (you may need to adjust this depending on your server and connection):



Conclusion

At this point you have configured AWS Connector, which is ready to be used.
We hope you enjoy using AWS Connector.