



Sol4Cloud AlinkServer documentation

Version: 0.1.2

Date: July 7th, 2026

Table of content

AlinkServer Introduction.....2

Installation.....3

Configuration.....4

Administration.....5

ALinkServer Introduction

We have dreamed of a world in which you could just start using a solution with no upfront purchase

- simply pay-as-you-go fully managed by Amazon AWS. No hassle with sales men and procurement
- simply start using the solution and consume it off your AWS commitment.

Our first solution: ALinkServer - Archive your SAP system data and documents directly to AWS S3 by deploying a cloud-native pay-as-you-go ALinkServer implementing SAP ArchiveLink 4.6 interface specification

ALinkServer is SAP ArchiveLink 4.6 implementation of SAP ArchiveLink repository that stores all SAP archived content directly in as objects in AWS S3 buckets. ALinkServer configuration enables the admin to configure a dedicated S3 bucket per SAP ArchiveLink repository.

One ALinkServer server configuration supports identical SAP repository IDs across multiple SAP landscapes by specifying a “Runtime environment” parameter in the configuration that is also present in the SAP ArchiveLink repository URL in SAP configuration. See chapter Configuration for more details.

ALinkServer can be easily launched as service on AWS Elastic Container Service. First launch of the ALinkServer application will walk admin user through basic server setup. ALinkServer stores all content related metadata directly as S3 object metadata instead of a traditional relational database. Small amount of ALinkServer configuration data (server configuration and ArchiveLink repositories configurations) is stored in AWS DynamoDB. Admin user names and passwords are stored in AWS Secrets Manager. See chapter Installation for more details.

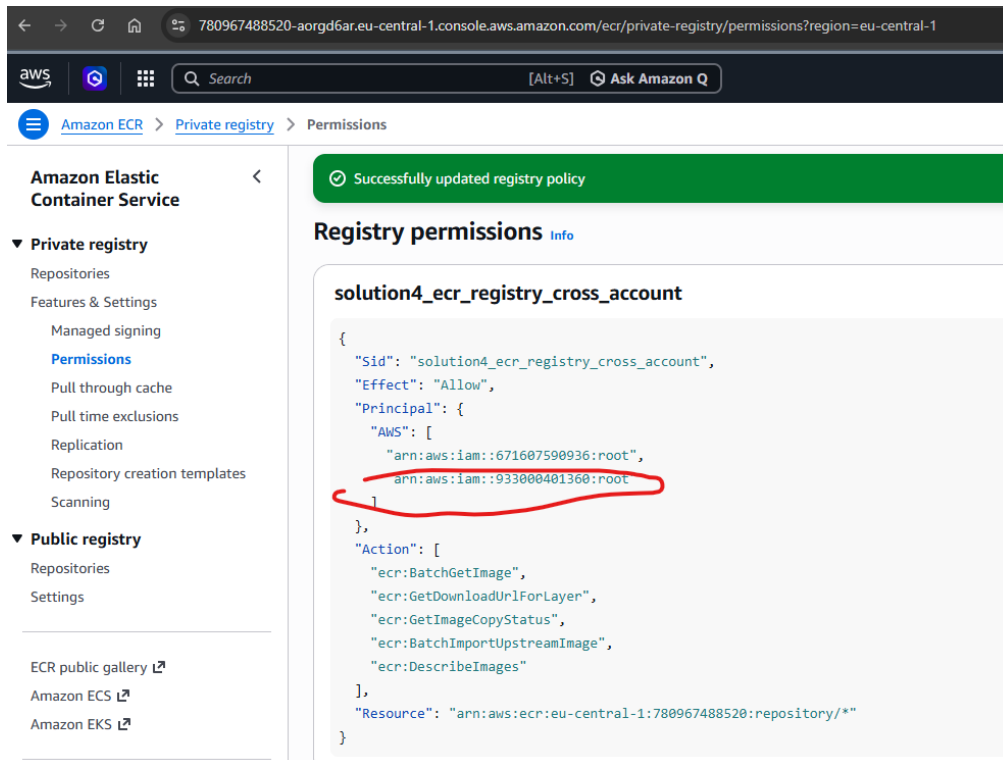
Each ALinkServer container is configured to start two web applications:

1. Main ALinkServer that implements the ArchiveLink functionality and its URLs will be configured in SAP transaction OAC0
2. ALinkServerAdmin process that is used for configuration and administration of the ALinkServer e.g. to create new content repositories, create new admin users etc.
ALinkServerAdmin process is also responsible for reporting server container usage to AWS.

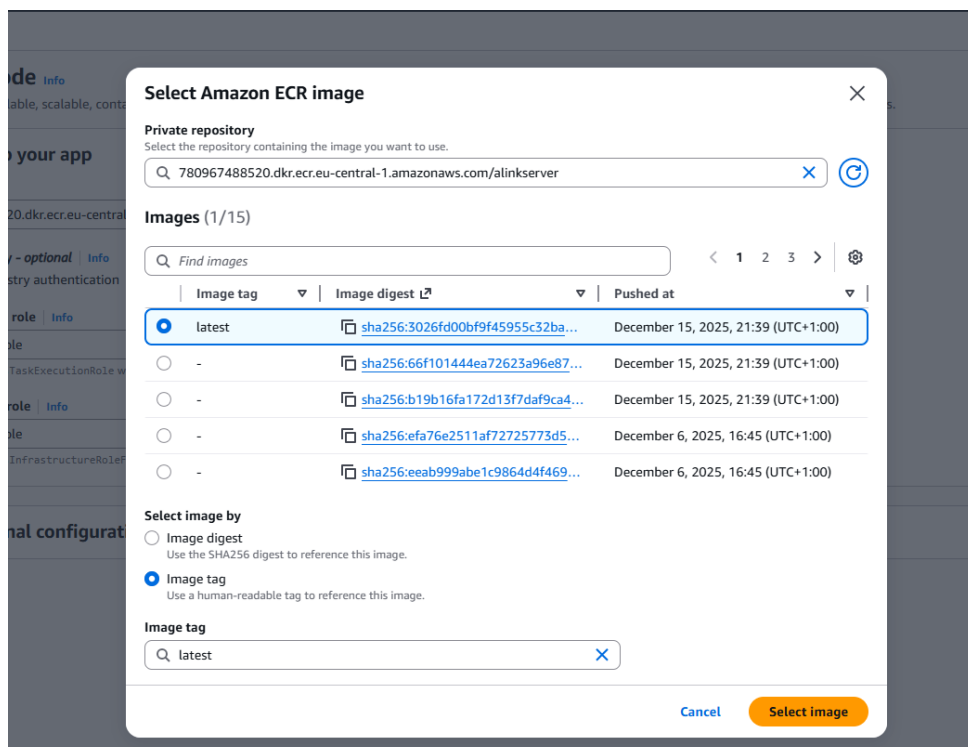
For more details about ALinkServer administration and monitoring see chapter Administration.

Installation

1) (Optional?) In Sol4Cloud account allow ECR registry access by third party service and account by adding account id to the list of allowed permissions:



2) Test in „customer“ account that the repository can be accessed:



3) Create task definition in Elastic Container Service.

- Launch type: AWS Fargate
- OS Linux/x86
- CPU 2, RAM 4GB
- Container: 780967488520.dkr.ecr.eu-central-1.amazonaws.com/alinkserver:latest
- Container ports:
8000 – TCP – alinkserver – HTTP
8001 – TCP – alinkadminserver – HTTP

4) Configure Task Role for Task definition. Create new role in IAM/Roles:

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access Management, Access reports, etc. The main content area displays the details for the role 'ALinkServerECSContainerTaskRole'. The 'Summary' tab is active, showing the creation date (March 31, 2026, 17:49 UTC+02:00) and last activity. The 'Permissions' tab is also visible, showing three attached policies: AmazonDynamoDBFullAccess, AmazonS3FullAccess, and SecretsManagerReadWrite, all of which are AWS managed. The 'Permissions boundary' is currently not set.

Attach the role to Task definition above.

The screenshot shows the AWS ECS console interface. The 'Task roles - conditional' section is expanded, showing the 'Task role' dropdown set to 'ALinkServerECSContainerTaskRole' and the 'Task execution role' dropdown set to 'ecsTaskExecutionRole'. Both dropdowns have a 'Create new role' button next to them. Below these, there are sections for 'Task placement - optional' and 'Fault injection - optional'.

5) Change the SecurityGroup configuration in the network configuration of the Service to allow inbound ports 8000 and 8001:

sg-020d298f346aee151 - default

Details

Security group name

default

Security group ID

sg-020d298f346aee151

Description

default VPC security group

VPC ID

vpc-0ada4aa52eb46e8f8

Owner

671607590936

Inbound rules count

3 Permission entries

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Sharing

VPC associations

Related resources - new

Tags

Inbound rules (3)

Q Search

☐	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	D
☐	-	sgr-02052cf03fc8c906d	IPv4	Custom TCP	TCP	8001	0.0.0.0/0	-
☐	-	sgr-0641838d708ceac3a	-	All traffic	All	All	sg-020d298f346aee151...	-
☐	-	sgr-01585d8f6db153187	IPv4	Custom TCP	TCP	8000	0.0.0.0/0	-

Configuration

Service Connect:

Create new Namespace in AWS Cloud Map

Add CloudWatch permissions to ecsTaskExecutionRole

ecsTaskExecutionRole [Info](#)

Summary

Creation date
March 31, 2026, 14:45 (UTC+02:00)

Last activity
 8 minutes ago

ARN
 arn:aws:iam::6716075909

Maximum session duration
1 hour

Permissions

Trust relationships

Tags

Last Accessed

Revoke sessions

Permissions policies (2) [Info](#)

You can attach up to 10 managed policies.

Filter by Type
All types

☐	Policy name ↗	Type
☐	AmazonECSTaskExecutionRolePolicy	AWS managed
☐	AWSAppSyncPushToCloudWatchLogs	AWS managed

► **Permissions boundary** (not set)

Administration