aws

User Guide

AWS Systems Manager for SAP

AWS Systems Manager for SAP: User Guide

Table of Contents

What is AWS Systems Manager for SAP?

AWS Systems Manager for SAP is an automation capability to manage and operate your SAP applications on AWS. It provides a seamless integration between AWS services and SAP applications running on AWS. AWS Systems Manager for SAP is available to use with AWS APIs. For more information, see AWS Systems Manager for SAP API Reference Guide.

With AWS Systems Manager for SAP, you can backup and restore SAP HANA databases on Amazon EC2 with AWS Backup. For more information, see Get Started.

Topics

Features

AWS Systems Manager for SAP provides the following features for your SAP workloads running on Amazon EC2.

- Register and discover SAP applications
- List discovered SAP applications
- List configurations of discovered SAP applications
- Integration with AWS Backup – using https://console.aws.amazon.com/backup, enable automatic backup and restore operations of SAP HANA databases.

Supported Regions

AWS Systems Manager for SAP is available in all commercial AWS Regions. For more information, see AWS Systems Manager for SAP endpoints and quotas.

Related services

The following services are related to AWS Systems Manager for SAP on AWS.

- AWS Backup
- SAP HANA on AWS
- AWS Backint Agent for SAP HANA

Pricing

AWS Systems Manager for SAP is available to you at no additional cost. You only pay for the AWS resources that you provision to manage and operate your SAP environments.

Setting up

Topics

Sign up for AWS

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to an administrative user, and use only the root user to perform tasks that require root user access.

Create an IAM user

To create an administrator user, choose one of the following options.

Choose one way to manage your administrator	To	By	You can also
In IAM Identity Center (Recommended)	Use short-term credentials to access AWS. This aligns with the security best practices. For information about best practices, see Security best practices in IAM in the *IAM User Guide*.	Following the instructions in Getting started in the *AWS IAM Identity Center User Guide*.	Configure programmatic access by Configuring the AWS CLI to use AWS IAM Identity Center in the *AWS Command Line Interface User Guide*.
In IAM (Not recommended)	Use long-term credentials to access AWS.	Following the instructions in Creating your first IAM admin user and user group in the *IAM User Guide*.	Configure programmatic access by Managing access keys for IAM users in the *IAM User Guide*.

Get started with AWS Systems Manager for SAP

To get started with using AWS Systems Manager for SAP, ensure that you complete the following prerequisites for setup. You must run these steps on all Amazon EC2 instances in your setup.

Prerequisites

- Attach AWS Systems Manager for SAP permissions to Amazon EC2 instance running SAP HANA database
- Amazon EC2 tag
- Register SAP HANA database credentials in AWS Secrets Manager
- Verify AWS Systems Manager Agent (SSM Agent) is running
- Verify setup before registering your SAP HANA database
- Backup and restore – optional

Attach AWS Systems Manager for SAP permissions to Amazon EC2 instance running SAP HANA database

AWS Systems Manager for SAP communicates with the Amazon EC2 instance where your SAP HANA database running via policies. Attach the following IAM policies to the IAM role used by your Amazon EC2 instance.

- `AmazonSSMManagedInstanceCore` – this Amazon managed policy allows an instance to use Systems Manager service core functionality. For more information, see About policies for a Systems Manager instance profile.
- `AWSSystemsManagerForSAPFullAccess` – this Amazon managed policy grants full access to AWS Systems Manager for SAP. For more information, see AWS managed policy: `AWSSystemsManagerForSAPFullAccess`.

Amazon EC2 tag

`SSMForSAPManaged` – add this tag on your Amazon EC2 instance to enable AWS Systems Manager for SAP to access your Amazon EC2 instance.

Key	`SSMForSAPManaged`
Value	`True`

Register SAP HANA database credentials in AWS Secrets Manager

You must create a secret with the username and password of a database. A separate secret is required for each one of your databases running on an Amazon EC2 instance.

The following special characters are not allowed in a SAP HANA password:

- angle brackets (<>)
- backslashes (/)
- double quotes (")
- pipelines (|)
- question marks (?)
- semicolons (;)

Use the following steps to register your SAP HANA database credentials in AWS Secrets Manager.

1. Sign in to https://console.aws.amazon.com/secretsmanager/.
2. On the AWS Secrets Manager page, select **Store a new secret**.
3. For Secret type, select **Other type of secret** and create the following key value pairs.

Key	Value
username	*example_SAP_HANA_db_username*
password	*example_SAP_HANA_db_password*

4. Select **Next** and enter a Secret name. Note this Secret name for use while following the steps in the section called “Register SAP HANA database”.
5. In the **Resource permissions** container, choose **Edit permissions**, and paste the following policy with your Amazon Resource Name for the Amazon EC2 instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::AccountId:role/EC2RoleToAccessSecrets"
                ]
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*"
        }
    ]
}
```

This policy enables the IAM role used by your Amazon EC2 instance access to this secret. For more details, see Attach a permissions policy to an AWS Secrets Manager secret.

> **Note**
>
> You must attach this policy to each secret that you create for your SAP HANA database credentials.

6. Select **Next** and then, select **Store**.

Verify AWS Systems Manager Agent (SSM Agent) is running

Use the following command to verify the status of the SSM Agent on your instance.

```
sudo systemctl status amazon-ssm-agent
```

Your output should display *active (running)* as seen here.

```
amazon-ssm-agent.service - amazon-ssm-agent
     Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: disabled)
     Active: active (running) since Tue 2022-02-15 18:56:26 UTC; 12s ago
     ^^^^^^^^^^^^^^^^^^^^^^^^ You should expect to see "active (running)".
```

```
   Main PID: 16061 (amazon-ssm-agen)
      Tasks: 36
     CGroup: /system.slice/amazon-ssm-agent.service
             ##16061 /usr/sbin/amazon-ssm-agent
             ##16069 /usr/sbin/ssm-agent-worker
```

AWS Systems Manager Agent (SSM Agent) is pre-installed in several Amazon Machine Images (AMIs) provided by AWS. For more information, see Working with SSM Agent.

Verify setup before registering your SAP HANA database

- Ensure that you are running SAP HANA 2.x.
- Ensure that your Amazon EC2 instance has `/run` mount point mounted on `tmpfs`. Use the `df | grep tmpfs` command for verification.
- Ensure that your Amazon EC2 instance has Python 3.5 or higher version installed.
- Ensure that the `hdbcli` Python library is installed in the `/opt/aws/ssm-sap/` directory on your Amazon EC2 instance, if the revision of your SAP HANA 2.0 server is below 056.00.
- Ensure that the boto3 version is higher than 1.7.0 if boto3 is installed.

To register your database, see Register your SAP HANA database with AWS Systems Manager for SAP.

Backup and restore – *optional*

After registering your database, you can optionally choose to complete the prerequisites required to backup and restore your database. You must run these steps on all Amazon EC2 instances in your setup.

Topics

- Set up required permissions for Amazon EC2 instance for backup and restore of SAP HANA database
- Install AWS Backint Agent for SAP HANA with AWS Systems Manager Agent (SSM Agent) on your SAP application server

Set up required permissions for Amazon EC2 instance for backup and restore of SAP HANA database

To backup and restore your SAP HANA databases running on Amazon EC2 instance, attach the following IAM policies to the IAM role used by your Amazon EC2 instance.

- `AWSBackupDataTransferAccess` – this Amazon managed policy must be attached to the IAM role of Amazon EC2 instance where AWS Backint Agent for SAP HANA is located. AWS Backint Agent uses this IAM role to transfer data for backup and restore. For more information about the policy, see Managed policies for AWS Backup.
- `AWSBackupRestoreAccessforSAPHANA` – this Amazon managed policy enables access to restore your SAP HANA database using AWS Backup.
  - If you are going to use AWS Backup console for the restore process, attach this policy to the IAM role using the console.
  - If you are going to use AWS API for the restore process, attach this policy to the IAM role performing the API call.
  - Follow the recommended best practice of granting least privilege necessary for each role by attaching the `AWSBackupRestoreAccessforSAPHANA` policy only to the SAP HANA resource owner.
- `AWSBackupServiceRolePolicyForBackup` – this Amazon managed policy must be attached to the role that will passed to `StartBackupJob` or `DefaultRole`. For more information, see Service-linked role permissions for AWS Backup. The policy must contain the following trust relation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "backup.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Install AWS Backint Agent for SAP HANA with AWS Systems Manager Agent (SSM Agent) on your SAP application server

Follow along the steps described in AWS Backint Agent for SAP HANA documentation. For more information, see Install and configure AWS Backint Agent for SAP HANA.

Tutorials for AWS Systems Manager for SAP

This section provides tutorials to use AWS Systems Manager for SAP.

Topics

Register your SAP HANA databases with AWS Systems Manager for SAP

You can register a single node or a high availability setup with multiple nodes for SAP HANA database with AWS Systems Manager for SAP. Ensure that you have completed the setup perquisites described in Get started with AWS Systems Manager for SAP. Follow along these steps to register your database.

Steps

Step 1: Create a JSON for credentials

Create a JSON file to store the credentials you created in the section called “Register credentials in AWS Secrets Manager”.

```
[{
"DatabaseName": "<YOUR_SID>/<YOUR_DATABASE_NAME>",
"CredentialType": "ADMIN",
"SecretId": "<YOUR_SECRET_NAME>"
```

```
}, {
"DatabaseName": "<YOUR_SID>/<ANOTHER_ONE_OF_YOUR_DATABASE_NAME>",
"CredentialType": "ADMIN",
"SecretId": "<YOUR_SECRET_NAME>"
}]
```

- Enter a unique name for the JSON file. For example, `SsmForSapRegistrationCredentials.json`.
- For `DatabaseName`, ensure that you enter both, the system ID and the database name.
- For `SecretId`, use the Secret name created in Step 4 of the section called “Register credentials in AWS Secrets Manager”.

Step 2: Register database

Register your SAP HANA databases using the following command.

Pass the credentials using the JSON file created in Step 1.

```
// Command template
aws ssm-sap register-application \
--application-id <myApplication> \
--application-type HANA \
--instances <YOUR_EC2_INSTANCE_ID> \
--sap-instance-number <YOUR_HANA_SYSTEM_NUMBER> \
--sid <YOUR_HANA_SID> \
--region us-east-1 \
--credentials file://<PATH_TO_YOUR_CREDENTIALS_JSON_FILE>

// Example command with sample values
aws ssm-sap register-application \
--application-id <myApplication> \
--application-type HANA \
--instances i-0123456789abcdefg \
--sap-instance-number 00 \
--sid HDB \
--region us-east-1 \
--credentials file://SsmForSapRegistrationCredentials.json

// Example JSON response
{
    "Application": {
```

```
        "Id": "myApplication",
        "Type": "HANA",
        "Arn": "<APPLICATION_ARN>",
        "Status": "REGISTERING",
        "Components": [],
        "LastUpdated": "2022-08-19T10:58:48.521000-07:00"
    },
    "OperationId": "6bd44104-d63c-449d-8007-6c1b471e3e5e"
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
    // Take note of this operation ID. You'll need it in the next step.
}
```

Note the `OperationID` for the next step.

> **Note**
>
> To register a high availability SAP HANA database, you can input either the primary or the secondary instance ID with the `--instances` parameter. For example, for a high availability SAP HANA database residing on primary node `i-0123456789abcdefg` and secondary node `i-9876543210abcdefg`, you can specify database registration in any one of the following ways.
>
> - `--instances i-0123456789abcdefg`
> - `--instances i-9876543210abcdefg`

Step 3: Check registration status

The registration may take approximately five minutes to complete. Use the following command to check the status of the registration. Replace *<Your_Operation_ID>* with the `OperationID` from the previous step.

```
aws ssm-sap get-operation \
--operation-id <YOUR_OPERATION_ID> \
--region us-east-1
```

Step 4: Verify registration

Verify the registration with `GetApplication` API. You can also view the details of registered databases with `ListDatabases` and `GetDatabase` API.

```
// Command template
aws ssm-sap get-application \
--application-id <myApplication> \
--region us-east-1

// Example to get the summary of an application
aws ssm-sap get-application \
--application-id <myApplication> \
--region us-east-1

// Example output
{
    "Application": {
        "Id": "myApplication",
        "Type": "HANA",
        "Arn": "arn:aws:ssm-sap:us-east-1:123456789123:HANA/myApplication",
        "AppRegistryArn": "arn:aws:servicecatalog:us-east-1:123456789123:/applications/
myApplication",
        "Status": "ACTIVATED",
        "DiscoveryStatus": "SUCCESS",
        "Components": [
            "HDB-HDB00"
            ^^^^^^^^^^
            // Take note of this component ID. You'll need it in the next step.
        ],
        "LastUpdated": "2023-07-06T13:25:35.702000-07:00"
    },
    "Tags": {}
}
```

Step 5: View component summary

Get the component summary with GetComponent API.

```
// Command template
aws ssm-sap get-component \
--application-id <myApplication> \
--component-id <YOUR_COMPONENT_ID_FROM_LAST_STEP>
--region us-east-1
```

AWS Systems Manager for SAP provides two types of components for an SAP HANA application – parent and child.

- HANA – there is only one parent component representing the logical database.
- HANA_NODE – there are multiple child components representing database host entities.

See the following table for examples of single node and high availability SAP HANA database setup with AWS Systems Manager for SAP.

Single node

```
GetComponent API output for parent component
{
    "Component": {
        "ComponentId": "HDB-HDB00",
        "ChildComponents": [
            "HDB-HDB00-sapci"
        ],
        "ApplicationId": "myApplication",
        "ComponentType": "HANA",
        "Status": "RUNNING",
        "Databases": [
            "SYSTEMDB",
            "HDB"
        ],
        "Hosts": [
            {
                "HostName": "sapci",
                "HostIp": "172.31.31.70",
                "EC2InstanceId": "i-0123456789abcdefg",
                "InstanceId": "i-0123456789abcdefg",
                "HostRole": "LEADER",
                "OsVersion": "SUSE Linux Enterprise Server 15 SP4"
            }
        ],
        "PrimaryHost": "i-0123456789abcdefg",
        "LastUpdated": "2023-07-19T11:06:36.114000-07:00",
        "Arn": "arn:aws:ssm-sap:us-east-1:123456789123:HANA/myApplication/COMPONENT/
HDB-HDB00"
    },
    "Tags": {}
```

```
}
```

```
GetComponent API output for child component
{
    "Component": {
        "ComponentId": "HDB-HDB00-sapci",
        "ParentComponent": "HDB-HDB00",
        "ApplicationId": "myApplication",
        "ComponentType": "HANA_NODE",
        "Status": "RUNNING",
        "SapHostname": "sapci.local",
        "SapKernelVersion": "753, patch 1010, changelist 2124070",
        "HdbVersion": "",
        "Resilience": {
            "HsrTier": "",
            "HsrReplicationMode": "NONE",
            "HsrOperationMode": "NONE"
        },
        "AssociatedHost": {
            "Hostname": "sapci",
            "Ec2InstanceId": "i-04823df91c0934025",
            "OsVersion": "SUSE Linux Enterprise Server 15 SP4"
        },
        "LastUpdated": "2023-07-19T11:06:36.101000-07:00",
        "Arn": "arn:aws:ssm-sap:us-east-1:123456789101:HANA/myApplication/COMPONENT/
HDB-HDB00-sapci"
    },
    "Tags": {}
}
```

High availability

```
GetComponent API output for parent component
{
  “Component”: {
    “ComponentId”: “HDB-HDB00”,
    “ChildComponents”: [
      “HDB-HDB00-sapsecdb”,
      “HDB-HDB00-sappridb”
    ],
    “ApplicationId”: “myApplication”,
    “ComponentType”: “HANA”,
    “Status”: “RUNNING”,
```

```
    “Databases”: [
      “SYSTEMDB”,
      “HDB”
    ],
    "LastUpdated": "2023-06-28T22:57:24.053000-07:00",
    “Arn”: “arn:aws:ssm-sap:us-east-1:123456789123:HANA/myApplication/COMPONENT/HDB-
HDB00"
  },
  “Tags”: {}
}
```

```
GetComponent API output for child component (primary)
{
    "Component": {
        "ComponentId": "HDB-HDB00-sappridb",
        "ParentComponent": "HDB-HDB00",
        "ApplicationId": "myApplication",
        "ComponentType": "HANA_NODE",
        "Status": "RUNNING",
        "SapHostname": "sappridb.local",
        "SapKernelVersion": "753, patch 1010, changelist 2124070",
        "HdbVersion": "2.00.065.00.1665753120",
        "Resilience": {
            "HsrTier": "1",
            "HsrReplicationMode": "PRIMARY",
            "HsrOperationMode": "PRIMARY",
            "ClusterStatus": "ONLINE"
        },
        "AssociatedHost": {
            "Hostname": "sappridb",
            "Ec2InstanceId": "i-0123456789abcdefg",
            "OsVersion": "SUSE Linux Enterprise Server 15 SP4"
        },
        "LastUpdated": "2023-07-19T10:20:26.888000-07:00",
        "Arn": "arn:aws:ssm-sap:us-east-1:123456789123:HANA/myApplication/COMPONENT/
HDB-HDB00-sappridb"
    },
    "Tags": {}
}
```

```
GetComponent API output for child component (secondary)
{
    "Component": {
```

```
        "ComponentId": "HDB-HDB00-sapsecdb",
        "ParentComponent": "HDB-HDB00",
        "ApplicationId": "myApplication",
        "ComponentType": "HANA_NODE",
        "Status": "RUNNING",
        "SapHostname": "sapsecdb.local",
        "SapKernelVersion": "753, patch 1010, changelist 2124070",
        "HdbVersion": "2.00.065.00.1665753120",
        "Resilience": {
            "HsrTier": "2",
            "HsrReplicationMode": "SYNC",
            "HsrOperationMode": "LOGREPLAY",
            "ClusterStatus": "ONLINE"
        },
        "AssociatedHost": {
            "Hostname": "sapsecdb",
            "Ec2InstanceId": "i-0123456789abcdefg",
            "OsVersion": "SUSE Linux Enterprise Server 15 SP4"
        },
        "LastUpdated": "2023-07-19T10:20:26.639000-07:00",
        "Arn": "arn:aws:ssm-sap:us-east-1:123456789123:HANA/myApplication/COMPONENT/
HDB-HDB00-sapsecdb"
    },
    "Tags": {}
}
```


Backup your database – *optional*

Now the registration is complete, and you can begin data protection operations, including backup and restore of your SAP HANA databases. For more details, see AWS Backup documentation.

Register an application with AWS Systems Manager Application Manager

You can register an SAP HANA database as an application with AWS Systems Manager Application Manager using AWS Management Console. Follow along these steps to register your application.

1. Go to https://console.aws.amazon.com/systems-manager/ > **Application Management** > **Application Manager**.
2. Select **Create Application** > **Enterprise Workload**.

3. In **Application details**, enter a name and description for the application you want to register with Application Manager.
4. In **SAP HANA workload**, provide details of your workload.

    a. **Instance ID** – This is the Amazon EC2 instance ID where your workload is currently running. Choose **Browse instances**, and select the instance ID for your primary SAP HANA workload.

    b. **SAP System Identifier (SID)** – This is the SAP System Identifier (`sapsid`) of your SAP HANA instance.

    c. **SAP system number** – This is the system number of your SAP HANA instance.

    d. **Credentials** – These are the credentials of your database.

    > **Note**
    >
    > If you do not see the credentials for the application you want to register in the **Secret ID** drop-down list, ensure that you have registered your credentials with AWS Secrets Manager. For more information, see Register SAP HANA database credentials in AWS Secrets Manager.

    Optional Select **Add credentials** to add credentials for five databases.
5. *Optional* In **Application tags**, you can add 100 tags associated to resources.
6. Select **Create**.

Application

On registration completion, you can see your application in the list of applications. You can see the following tabs for each application.

Overview

For more information, see Viewing overview information about an application.

Resources

You can find the **Topology** of a AWS Systems Manager for SAP application in the **Resources** tab. It provides the details of your application components. The child components are embedded under parent components. Select each component to view its details.

For more information, see Viewing application resources.

Instances

For more information, see Working with your application instances.

Compliance

For more information, see Viewing compliance information.

Monitoring

> **Note**
>
> You must on-board your AWS Systems Manager for SAP application with Amazon CloudWatch Application Insights to view monitoring details in this tab.

Use the following steps to on-board your registered SAP HANA application with Application Insights.

1. Open https://console.aws.amazon.com/systems-manager/.
2. Go to **Application Manager**.
3. From the list of applications, find and select your SAP application. This opens your application details window.
4. Go to the **Monitoring** tab > **Application Insights** > **Add an application**.
5. You are now redirected to Amazon CloudWatch Application Insights console.
6. Follow the instructions described in Set up your SAP HANA database for monitoring.

   > **Note**
   >
   > Under **Select an application or resource group**, ensure to select your SAP HANA application registered with AWS Systems Manager for SAP.

7. Once you have completed onboarding your registered SAP HANA application with Amazon CloudWatch Application Insights, you can view monitoring details in the **Monitoring** tab.

For more information, see Viewing monitoring information.

OpsItems

For more information, see Viewing OpsItems for an application.

Logs

For more information, see Viewing log groups and log data.

Runbooks

For more information, see Working with runbooks in Application Manager.

Cost

You must enable AWS Cost Explorer Service to view details in the Cost tab. For more information, see Enabling Cost Explorer.

Register your SAP ABAP application with AWS Systems Manager for SAP

You can register a single node setup for SAP ABAP application with AWS Systems Manager for SAP. Ensure that you have completed the setup perquisites described in Get started with AWS Systems Manager for SAP. Follow along these steps to register your SAP ABAP application.

Steps

- Step 1: Register database
- Step 2: Register application
- Step 3: Check registration status
- Step 4: Verify registration
- Step 5: View component summary

Step 1: Register database

Register your SAP HANA database before registering your SAP ABAP application. For more information, see the section called “Register SAP HANA database”.

Note the `ApplicationId` of your registration.

Step 2: Register application

1. Use the `ApplicationId` noted in the previous step in the next command.
2. Use the following command to find the Amazon Resource Name (ARN) of the database.

```
% aws ssm-sap list-databases --application-id <mySAPHANAApplication>
{
    "Databases": [
        {
            "ApplicationId": "SAP_HANA_APPLICATION",
            "ComponentId": "HDB-HDB00",
            "DatabaseId": "SYSTEMDB",
            "DatabaseType": "SYSTEM",
            "Arn": "arn:aws:ssm-sap:us-east-1:123456789101:HANA/
SAP_HANA_APPLICATION/DB/SYSTEMDB",
            "Tags": {}
        },
        {
            "ApplicationId": "SAP_HANA_APPLICATION",
            "ComponentId": "HDB-HDB00",
            "DatabaseId": "HDB",
            "DatabaseType": "TENANT",
 ------>    "Arn": "arn:aws:ssm-sap:us-east-1:123456789101:HANA/
SAP_HANA_APPLICATION/DB/HDB",
            "Tags": {}
        }
    ]
}
```

3. Note the `database-arn` from the preceding step to register your SAP ABAP application with the following command.

```
// Command template
aws ssm-sap register-application \
--application-id <myApplication> \
--application-type SAP_ABAP \
--instances <YOUR_EC2_INSTANCE_ID> \
--sid <YOUR_HANA_SID> \
--region us-east-1
--database-arn <SAP HANA DATABASE ARN FROM REGISTERED APPLICATION>

// Example command with sample values
```

```
aws ssm-sap register-application
    –application-id "mySAPABAPApplication" \
    –application-type SAP_ABAP \
    –instances i-0307b3e5fbdc4bda1 \
    –sid ECD \
    –region us-east-1 \
    –database-arn "arn:aws:ssm-sap:us-east-1:123456789101:HANA/
SAP_HANA_APPLICATION/DB/HDB"

// Example JSON response
{
    "Application": {
        "Id": "mySAPABAPApplication",
        "Type": "SAP_ABAP",
        "Arn": "<APPLICATION_ARN>",
        "Status": "REGISTERING",
        "Components": [],
        "LastUpdated": "2022-08-19T10:58:48.521000-07:00"
    },
    "OperationId": "6bd44104-d63c-449d-8007-6c1b471e3e5e"
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
    // Take note of this operation ID. You'll need it in the next step.
}
```

Step 3: Check registration status

The registration may take a few minutes to complete. Use the following command to check the status of your registration. Use the `OperationId` generated when registering your SAP ABAP application in the preceding step.

```
aws ssm-sap get-operation \
--operation-id <YOUR_OPERATION_ID> \
--region us-east-1
```

Step 4: Verify registration

Verify the registration with `GetApplication` API. You can also view the details of registered databases with `ListDatabases` and `GetDatabase` API.

```
// Command template
aws ssm-sap get-application \
```

```
--application-id <myApplication> \
--region us-east-1

// Example to get the summary of an application
aws ssm-sap get-application \
--application-id mySAPABAPApplication \
--region us-east-1
{
  "Application": {
    "Id": "mySAPABAPApplication",
    "Type": "SAP_ABAP",
    "Arn": "arn:aws:ssm-sap:us-east-1:123456789101:SAP_ABAP/mySAPABAPApplication",
    "AppRegistryArn": "arn:aws:servicecatalog:us-east-1:123456789101:/
applications/0efeiejngum6atpd8ww2xklo",
    "Status": "ACTIVATED",
    "DiscoveryStatus": "SUCCESS",
    "Components": [
        "ECD-ABAP"
        ^^^^^^^^^^
        // Take note of this component ID. You'll need it in the next step.
    ],
    "LastUpdated": "2023-10-04T22:16:59.106000-07:00"
  },
  "Tags": {}
}
```

Step 5: View component summary

Get the component summary with [GetComponent](#) API.

```
// Command template aws ssm-sap get-component \
--application-id <myApplication> \
--component-id <YOUR_COMPONENT_ID_FROM_LAST_STEP>
--region us-east-1

//GetComponent API output for parent component
% aws ssm-sap get-component --component-id ECD-ABAP \
    --application-id mySAPABAPApplication \
    --region us-east-1

{
    "Component": {
        "ComponentId": "ECD-ABAP",
```

```
        "Sid": "ECD",
        "ChildComponents": [
            "ECD-ASCS10-sapci",
            "ECD-D12-sapci"
        ],
        "ApplicationId": "mySAPABAPApplication",
        "ComponentType": "ABAP",
        "Status": "RUNNING",
        "DatabaseConnection": {
            "DatabaseConnectionMethod": "DIRECT",
            "DatabaseArn": "arn:aws:ssm-sap:us-east-1:123456789101:HANA/
SAP_HANA_APPLICATION/DB/HDB",
            "ConnectionIp": "172.31.19.240"
        },
        "LastUpdated": "2023-10-04T22:16:59.089000-07:00",
        "Arn": "arn:aws:ssm-sap:us-east-1:123456789101:SAP_ABAP/mySAPABAPApplication/
COMPONENT/ECD-ABAP"
    },
    "Tags": {}
}

//GetComponent API output for child component
% aws ssm-sap get-component \
    --component-id ECD-ASCS10-sapci --application-id mySAPABAPApplication \
    --region us-east-1
{
    "Component": {
        "ComponentId": "ECD-ASCS10-sapci",
        "Sid": "ECD",
        "SystemNumber": "10",
        "ParentComponent": "ECD-ABAP",
        "ApplicationId": "mySAPABAPApplication",
        "ComponentType": "ASCS",
        "Status": "RUNNING",
        "SapFeature": "MESSAGESERVER|ENQUE",
        "SapHostname": "sapci",
        "SapKernelVersion": "785, patch 200, changelist 2150416",
        "Resilience": {
            "EnqueueReplication": false
        },
        "AssociatedHost": {
            "Hostname": "sapci",
            "Ec2InstanceId": "i-0307b3e5fbdc4bda1",
            "IpAddresses": [
```

```
                {
                    "IpAddress": "172.31.19.240",
                    "Primary": true,
                    "AllocationType": "VPC_SUBNET"
                }
            ],
            "OsVersion": "SUSE Linux Enterprise Server 15 SP4"
        },
        "LastUpdated": "2023-10-04T22:16:58.915000-07:00",
        "Arn": "arn:aws:ssm-sap:us-east-1:123456789101:SAP_ABAP/mySAPABAPApplication/
COMPONENT/ECD-ASCS10-sapci"
    },
    "Tags": {}
}
```

Supported versions for SAP deployments

The following section provides information about the versions of operating systems, databases, and applications supported by AWS Systems Manager for SAP.

Topics

Operating systems

The following table provides details of the operating systems supported by AWS Systems Manager for SAP.

Operating system	Versions
Red Hat Enterprise Linux	8.6, 8.4, 8.2, 8.1, 7.9, and 7.7
SUSE Linux Enterprise Server for SAP Applications	15, 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5, 12 SP4, and 12 SP5
SUSE Linux Enterprise Server	15, 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5, 12 SP4, and 12 SP5

Databases

The following table provides details of the database versions supported by AWS Systems Manager for SAP.

Database	Versions
SAP HANA (single node)	2.0
SAP HANA (high availability)	2.0

SAP applications

The following table provides details of SAP applications supported by AWS Systems Manager for SAP.

Applications	Versions
SAP HANA (single-node)	2.0
SAP HANA (high availability)	2.0
SAP NetWeaver on SAP ABAP	750 and higher

Security in AWS Systems Manager for SAP

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to AWS Systems Manager for SAP, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using AWS Systems Manager for SAP. The following topics show you how to configure AWS Systems Manager for SAP to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your AWS Systems Manager for SAP resources.

Topics

AWS managed policies for AWS Systems Manager for SAP

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ReadOnlyAccess** AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

AWS managed policy: AWSSystemsManagerForSAPFullAccess

Attach the `AWSSystemsManagerForSAPFullAccess` policy to your IAM identities.

The `AWSSystemsManagerForSAPFullAccess` policy grants full access to AWS Systems Manager for SAP service.

Permissions details

This policy includes the following permissions.

- `ssm-sap` – Allows principals full access to AWS Systems Manager for SAP.
- `iam` – Allows a service-linked role to be created, which is a requirement for using AWS Systems Manager for SAP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-sap:*"
            ],
            "Resource": "arn:*:ssm-sap:*:*:*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/ssm-sap.amazonaws.com/
AWSServiceRoleForAWSSSMForSAP"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "ssm-sap.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS managed policy: AWSSystemsManagerForSAPReadOnlyAccess

Attach the `AWSSystemsManagerForSAPReadOnlyAccess` policy to your IAM identities.

The `AWSSystemsManagerForSAPReadOnlyAccess` policy grants read only access to the AWS Systems Manager for SAP service.

Permissions details

This policy includes the following permissions.

- `ssm-sap` – Allows principals read only access to AWS Systems Manager for SAP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-sap:get*",
                "ssm-sap:list*"
            ],
            "Resource": "arn:*:ssm-sap:*:*:*"
```

```
        }
    ]
}
```

AWS Systems Manager for SAP updates to AWS managed policies

View details about updates to AWS managed policies for AWS Systems Manager for SAP since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Systems Manager for SAP Document history page.

Change	Description	Date
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	Added AWS Resource Group actions to the policy.	November 21, 2023
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	Added Systems Manager action to the policy.	November 17, 2023
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	Added Amazon EC2 and Systems Manager actions to the policy.	October 27, 2023
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	Added AWS Service Catalog and AWS Resource Group actions to the policy.	July 25, 2023
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	Added the `PutMetricData` Amazon CloudWatch action to the policy.	January 05, 2023
AWSSystemsManagerForSAPFullAccess – Updated policy	Updated the `"arn:aws:iam::*:role/aws-service-role/ssm-sap.amazonaws.com/AWSServiceRoleForAWSSSMForSAP"` resource in policy.	November 18, 2022

Change	Description	Date
AWSSystemsManagerForSAPFullAccess – New policy made available at launch	**AWSSystemsManagerForSAPFullAccess** grants an IAM user account full access to AWS Systems Manager for SAP service.	November 15, 2022
AWSSystemsManagerForSAPReadOnlyAccess – New policy made available at launch	**AWSSystemsManagerForSAPReadOnlyAccess** grants an IAM user account read only access to AWS Systems Manager for SAP service.	November 15, 2022
AWSSSMForSAPServiceLinkedRolePolicy – New policy made available at launch	The **AWSSSMForSAPServiceLinkedRolePolicy** service-linked role policy provides access to AWS Systems Manager for SAP.	November 15, 2022
AWS Systems Manager for SAP started tracking changes	AWS Systems Manager for SAP started tracking changes for its AWS managed policies.	November 15, 2022

Using service linked roles for AWS Systems Manager for SAP

AWS Systems Manager for SAP uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to AWS Systems Manager for SAP. Service-linked roles are predefined by AWS Systems Manager for SAP and include all of the permissions that the service requires to call other AWS services, including Amazon EC2, Systems Manager, IAM, Amazon CloudWatch, Amazon EventBridge, AWS Resource Groups, and AWS Service Catalog.

A service-linked role makes setting up AWS Systems Manager for SAP easier because you don't have to manually add the necessary permissions. AWS Systems Manager for SAP defines the permissions of its service-linked roles, and unless you make changes to the configuration, only AWS

Systems Manager for SAP can assume its roles. Configurable permissions include the trust policy and the permissions policy. You can't attach the permissions policy to any other IAM entity.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Follow the **Yes** link to view the service-linked role documentation for that service, if applicable.

Service-linked role permissions for AWS Systems Manager for SAP

AWS Systems Manager for SAP uses the service-linked role named **AWSServiceRoleForAWSSSMForSAP** and associates it with the **AWSSSMForSAPServiceLinkedRolePolicy** IAM policy – Provides AWS Systems Manager for SAP the permissions required to manage and integrate SAP applications on AWS.

The policy enables AWS Systems Manager for SAP to perform actions specified in the policy. These actions are from the following AWS services – Amazon EC2, Systems Manager, IAM, Amazon CloudWatch, Amazon EventBridge, AWS Resource Groups, and AWS Service Catalog.

Permissions details

This policy includes the following permissions.

- `cloudwatch` – Allows publication of AWS Systems Manager for SAP metric data to Amazon CloudWatch.
- `ec2` – Allows description of instances, and creation, deletion, and description of tags.
- `eventbridge` – Allows Amazon EventBridge to create, update, and delete rules, and add or remove targets to the rules.
- `iam` – Allows creation of roles and instance profiles.
- `resource-groups` – Allows AWS Resource Groups to create and delete groups.
- `servicecatalog` – Allows AWS Service Catalog to create, update, and delete applications, and attribute groups. The permission also enables association/disassociation of attribute groups to applications.
- `ssm` – Allows SSM to describe documents, run commands, and return command details.

The **AWSSSMForSAPServiceLinkedRolePolicy** service-linked role trusts the following services to assume the role:

- `ssm-sap.amazonaws.com`

The following is the full policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DescribeInstanceActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ssm:GetCommandInvocation",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DescribeInstanceStatus",
            "Effect": "Allow",
            "Action": "ec2:DescribeInstanceStatus",
            "Resource": "*"
        },
        {
            "Sid": "TargetRuleActions",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:PutTargets",
                "events:DescribeRule",
                "events:PutRule",
                "events:RemoveTargets"
            ],
            "Resource": [
                "arn:*:events:*:*:rule/SSMSAPManagedRule*",
                "arn:*:events:*:*:event-bus/default"
            ]
        },
        {
            "Sid": "DocumentActions",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:SendCommand"
            ],
            "Resource": [
```

```
                "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
                "arn:*:ssm:*:*:document/AWSSSMSAP*",
                "arn:*:ssm:*:*:document/AWSSAP*"
            ]
        },
        {
            "Sid": "CustomerSendCommand",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": "arn:*:ec2:*:*:instance/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "ssm:resourceTag/SSMForSAPManaged": "True"
                }
            }
        },
        {
            "Sid": "InstanceTagActions",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": "arn:*:ec2:*:*:instance/*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/awsApplication": "false"
                },
                "StringEqualsIgnoreCase": {
                    "ec2:ResourceTag/SSMForSAPManaged": "True"
                }
            }
        },
        {
            "Sid": "DescribeTag",
            "Effect": "Allow",
            "Action": "ec2:DescribeTags",
            "Resource": "*"
        },
        {
            "Sid": "GetApplication",
            "Effect": "Allow",
            "Action": "servicecatalog:GetApplication",
            "Resource": "arn:*:servicecatalog:*:*:*"
```

```
        },
        {
            "Sid": "DeleteOrUpdateApplication",
            "Effect": "Allow",
            "Action": [
                "servicecatalog:DeleteApplication",
                "servicecatalog:UpdateApplication"
            ],
            "Resource": "arn:*:servicecatalog:*:*:*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SSMForSAPCreated": "True"
                }
            }
        },
        {
            "Sid": "CreateApplication",
            "Effect": "Allow",
            "Action": [
                "servicecatalog:TagResource",
                "servicecatalog:CreateApplication"
            ],
            "Resource": "arn:*:servicecatalog:*:*:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/SSMForSAPCreated": "True"
                }
            }
        },
        {
            "Sid": "CreateServiceLinkedRole",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:*:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "servicecatalog-appregistry.amazonaws.com"
                }
            }
        },
        {
            "Sid": "PutMetricData",
            "Effect": "Allow",
```

```
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/Usage",
                        "AWS/SSMForSAP"
                    ]
                }
            }
        },
        {
            "Sid": "CreateAttributeGroup",
            "Effect": "Allow",
            "Action": "servicecatalog:CreateAttributeGroup",
            "Resource": "arn:*:servicecatalog:*:*:/attribute-groups/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/SSMForSAPCreated": "True"
                }
            }
        },
        {
            "Sid": "GetAttributeGroup",
            "Effect": "Allow",
            "Action": "servicecatalog:GetAttributeGroup",
            "Resource": "arn:*:servicecatalog:*:*:/attribute-groups/*"
        },
        {
            "Sid": "DeleteAttributeGroup",
            "Effect": "Allow",
            "Action": "servicecatalog:DeleteAttributeGroup",
            "Resource": "arn:*:servicecatalog:*:*:/attribute-groups/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SSMForSAPCreated": "True"
                }
            }
        },
        {
            "Sid": "AttributeGroupActions",
            "Effect": "Allow",
            "Action": [
                "servicecatalog:AssociateAttributeGroup",
```

```
                "servicecatalog:DisassociateAttributeGroup"
            ],
            "Resource": "arn:*:servicecatalog:*:*:*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SSMForSAPCreated": "True"
                }
            }
        },
        {
            "Sid": "ListAssociatedAttributeGroups",
            "Effect": "Allow",
            "Action": "servicecatalog:ListAssociatedAttributeGroups",
            "Resource": "arn:*:servicecatalog:*:*:*"
        },
        {
            "Sid": "CreateGroup",
            "Effect": "Allow",
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:Tag"
            ],
            "Resource": "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SSMForSAPCreated": "True"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "SSMForSAPCreated"
                    ]
                }
            }
        },
        {
            "Sid": "GetGroup",
            "Effect": "Allow",
            "Action": "resource-groups:GetGroup",
            "Resource": "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
        },
        {
            "Sid": "DeleteGroup",
            "Effect": "Allow",
            "Action": "resource-groups:DeleteGroup",
```

```
            "Resource": "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SSMForSAPCreated": "True"
                }
            }
        },
        {
            "Sid": "CreateAppTagResourceGroup",
            "Effect": "Allow",
            "Action": [
                "resource-groups:CreateGroup"
            ],
            "Resource": "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/EnableAWSServiceCatalogAppRegistry": "true"
                }
            }
        },
        {
            "Sid": "TagAppTagResourceGroup",
            "Effect": "Allow",
            "Action": [
                "resource-groups:Tag"
            ],
            "Resource": "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry": "true"
                }
            }
        },
        {
            "Sid": "GetAppTagResourceGroupConfig",
            "Effect": "Allow",
            "Action": [
                "resource-groups:GetGroupConfiguration"
            ],
            "Resource": [
                "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
            ]
        }
    ]
```

```
}
```

To view the update history of this policy, see AWS Systems Manager for SAP updates to AWS managed policies.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

Creating a service-linked role for AWS Systems Manager for SAP

AWS Systems Manager for SAP uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to AWS Systems Manager for SAP. Service-linked roles are predefined by AWS Systems Manager for SAP and include all of the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up AWS Systems Manager for SAP easier because you don't have to manually add the necessary permissions. AWS Systems Manager for SAP defines the permissions of its service-linked roles, and unless you make changes to the configuration, only AWS Systems Manager for SAP can assume its roles. Configurable permissions include the trust policy and the permissions policy. You can't attach the permissions policy to any other IAM entity.

If you delete this service-linked role, AWS Systems Manager for SAP automatically creates this service-linked role for you when you resume using AWS Systems Manager for SAP.

Editing a service-linked role for AWS Systems Manager for SAP

AWS Systems Manager for SAP does not allow you to edit the **AWSServiceRoleForAWSSSMForSAP** service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using the AWS Systems Manager for SAP console, CLI, or API.

Deleting a service-linked role for AWS Systems Manager for SAP

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the **AWSServiceRoleForAWSSSMForSAP** service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

When deleting AWS Systems Manager for SAP resources used by the **AWSServiceRoleForAWSSSMForSAP** SLR, you cannot have any running assessments (tasks for generating recommendations). No background assessments can be running, either. If assessments are running, the SLR deletion fails in the IAM console. If the SLR deletion fails, you can retry the deletion after all background tasks have completed. You don't need to clean up any created resources before you delete the SLR.

Supported Regions for AWS Systems Manager for SAP service-linked roles

AWS Systems Manager for SAP supports using service-linked roles in all of the regions where the service is available. For more information, see Service endpoints for AWS Systems Manager for SAP.

Monitoring

AWS Systems Manager for SAP works with other AWS tools to empower you to monitor its workloads. These tools include the following:

- Use **Amazon CloudWatch** and **Amazon EventBridge** to monitor AWS Systems Manager for SAP processes.
  - You can use CloudWatch to track metrics, create alarms, and view dashboards.
  - You can use EventBridge to view and monitor AWS Systems Manager for SAP events.
- Use **AWS CloudTrail** to monitor AWS Systems Manager for SAP API calls.

Topics

Monitoring AWS Systems Manager for SAP events using EventBridge

Topics

Monitor events using EventBridge

You can track the following AWS Systems Manager for SAP-related events in EventBridge.

Event type	Status	Event details
SSM for SAP Operation State Change	`InProgress` , `Success`, `Error`	operationId, type, applicationId, resourceId, resourceType, status, statusMessage

Use these sample JSON payloads if you would like to use these events programmatically.

Event state	JSON payload

SSM for SAP Operation: InProgress	{
	"version": "0",
	"id": "6b41eac1-3685-c064-12a3-f16b57f30114",
	"detail-type": "SSM for SAP Operation State Change",
	"source": "aws.ssm-sap",
	"account": "112233445566",
	"time": "2023-01-25T08:04:33Z",
	"region": "us-east-1",
	"resources": [],
	"detail": {
	"operationId": "dbfd5c7d-0f5a-4ad3-87bf-d04b65eba21e",
	"type": "REGISTER_APPLICATION",
	"applicationId": "HANA_TEST",
	"resourceId": "HDB",
	"resourceType": "APPLICATION",
	"status": "InProgress",
	"statusMessage": null
	}
	}

SSM for SAP Operation: Success	{
	"version": "0",
	"id": "05595cb1-ceac-1fb0-9040-045ca7865146",
	"detail-type": "SSM for SAP Operation State Change",
	"source": "aws.ssm-sap",
	"account": "112233445566",
	"time": "2023-01-26T04:45:43Z",
	"region": "us-east-1",
	"resources": [],
	"detail": {

Event state	JSON payload

	<pre>"operationId": "e5de5599
	-3b1e-4892-9201-835e71c6090a",
	"type": "REGISTER_APPLICAT
	ION",
	"applicationId": "HANA_TEST",
	"resourceId": "HDB",
	"resourceType": "APPLICAT
	ION",
	"status": "Success",
	"statusMessage": null
	}
	}</pre>

SSM for SAP Operation: Error	<pre>{
	"version": "0",
	"id": "fb715f90-e80c-1c7f-f179-e6
	646f4b97d9",
	"detail-type": "SSM for SAP
	Operation State Change",
	"source": "aws.ssm-sap",
	"account": "112233445566",
	"time": "2023-01-26T04:46:34Z",
	"region": "us-east-1",
	"resources": [],
	"detail": {
	"operationId": "77c8f0e6
	-6987-4e2b-9517-c5a44388992a",
	"type": "UPDATE_CREDENTIALS",
	"applicationId": "HANA",
	"resourceId": "HDB",
	"resourceType": "APPLICAT
	ION",
	"status": "Error",
	"statusMessage": null
	}
	}</pre>

Example

The following is an event pattern example of Operation State Change event from AWS Systems Manager for SAP using the `RegisterApplication` API.

```
{
  "source": ["aws.ssm-sap"],
  "detail-type": ["SSM for SAP Operation State Change"],
  "detail": {
    "type": ["REGISTER_APPLICATION"]
  }
}
```

AWS Systems Manager for SAP metrics with Amazon CloudWatch

You can view CloudTrail metrics for AWS Systems Manager for SAP via AWS Management Console or AWS CLI.

AWS Management Console

Metrics are grouped first by the service namespace, and then by the various dimension combination within each namespace. Use the following steps to view the metrics in AWS Management Console.

1. Open https://console.aws.amazon.com/cloudwatch/.
2. In the left navigation pane, select **Metrics**.
3. In namespace, select **AWS/SSMForSAP**.

AWS Command Line Interface

Use the following command to view the metrics via AWS CLI.

```
aws cloudwatch list-metrics --namespace "AWS/SSMForSAP"
```

The following are all the metrics available to you.

Metric	Dimensions	Units	Description
OperationStarted	OperationType	Count	An operation is started.
OperationSucceeded	OperationType	Count	An operation is succeeded.
OperationFailed	OperationType	Count	An operation is failed.

Usage Metrics

AWS Systems Manager for SAP provides resource usage metrics in the **AWS/Usage** namespace. For more information, see AWS usage metrics.

Logging AWS Systems Manager for SAP API calls with CloudTrail

AWS Systems Manager for SAP is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Systems Manager for SAP. CloudTrail captures all API calls for AWS Systems Manager for SAP as events. The calls captured include calls from the AWS Systems Manager for SAP console and code calls to the AWS Systems Manager for SAP API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Systems Manager for SAP. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to AWS Systems Manager for SAP, the IP address from which the request was made, who made the request, when it was made, and additional details. To learn more about CloudTrail, see the AWS CloudTrail User Guide.

Quotas for AWS Systems Manager for SAP

Your AWS account has default quotas, formerly referred to as limits, for each AWS service. Unless otherwise noted, each quota is Region-specific. You can request increases for some quotas, and other quotas cannot be increased.

To view a list of the quotas for AWS Systems Manager for SAP, see AWS Systems Manager for SAP service quotas.

To view the quotas for AWS Systems Manager for SAP, open the Service Quotas console. In the navigation pane, choose **AWS services** and select **AWS Systems Manager for SAP**.

To request a quota increase, see Requesting a Quota Increase in the *Service Quotas User Guide*. If the quota is not yet available in Service Quotas, use the limit increase form.

Troubleshooting AWS Systems Manager for SAP

Topics

Database registration failure

Problem – `Registration of SAP HANA database on AWS Systems Manager for SAP fails with an error`

Resolution – Use the following steps to resolve this error.

1. Deregister the database with the following command.

```
aws ssm-sap deregister-application \
--application-id <YOUR_APPLICATION_ID> \
--region us-east-1
```

   <YOUR_APPLICATION_ID> must be the same as the one used during registration.

2. Re-register the database.

```
aws ssm-sap register-application \
--application-id <YOUR_APPLICATION_ID> \
```

```
--region us-east-1
```

Problem – `Application DiscoveryStatus: REGISTRATION_FAILED; StatusMessage: The database ARN specified in registration input does not match discovered database connection.`

Resolution – The specified `--database-arn` does not match the database connection discovered on the SAP_ABAP instance. De-register the failed SAP ABAP application registration, and re-register with the correct `--database-arn`. For more information, see Register your SAP ABAP application with AWS Systems Manager for SAP.

InvalidInstanceIdException

Problem – `Error executing SSM document - InvalidInstanceIdException Instances [[<EC2_INSTANCE_ID>]] not in a valid state for account <ACCOUNT_ID> (Service: Ssm, Status Code: 400, Request ID: <REQUEST_ID>)`

Resolution – Ensure that your Amazon EC2 instance is active, and that the SSM Agent has been installed. For more information, see Verify AWS Systems Manager (SSM Agent) is running. After verification, deregister, and then re-register your application.

AccessDeniedException

Problem – `Discovered 1 SAP instances. {HDB: Unable to decrypt credentials <SECRET_NAME>: An error occurred (AccessDeniedException) when calling the GetSecretValue operation: User: arn:aws:sts::<ACCOUNT_ID>:assumed-role/<EC2_IAM_ROLE>/<INSTANCE_ID> is not authorized to perform: secretsmanager:GetSecretValue on resource: <SECRET_NAME> because no identity-based policy allows the secretsmanager:GetSecretValue action}, {HDB: Failed to discover HANA database ports. Exception type: <class 'IndexError'>}, REGISTER_APPLICATION`

Resolution – Ensure that your Amazon EC2 instance is setup correctly. For more information, see Set up required permissions for Amazon EC2 instance running SAP HANA database.
The IAM role attached to your Amazon EC2 instance must have the permission to perform `secretsmanager:GetSecretValue` action. After verification, deregister, and then re-register your application.

ResourceNotFoundException

Problem – `ERROR Discovered 1 SAP instances. {HDB: Unable to decrypt credentials <SECRET_NAME>: An error occurred (ResourceNotFoundException) when calling the GetSecretValue operation: Secrets Manager can't find the specified secret.},{HDB: Failed to discover HANA database ports. Exception type: <class 'IndexError'>}, REGISTER_APPLICATION`

Resolution – Verify and ensure that you are using the correct `SECRET_NAME`. For more information, see Register SAP HANA database credentials in AWS Secrets Manager. After verification, deregister, and then re-register your application.

Problem – `An error occurred (ResourceNotFoundException) when calling the RegisterApplication operation: Resource cannot be found`

Resolution – The `--database-arn` provided in the registration input parameter does not exist. Ensure that the connected SAP HANA database has been registered as an application with AWS Systems Manager for SAP. The database must be registered before registering the SAP ABAP application. For more information, see Register database.

Invalid control character

Problem – `Invalid control character at: line 2 column 32 (char 34)`

Resolution – Ensure that the `JSON` file that contains your SAP HANA database credentials is formatted correctly as a `JSON` file. Some characters may be pasted incorrectly after copying them from this file. Edit the file to remove line spaces, double quotes, spaces, and tabs. Add the formatted file content to your machine, terminal, and in your file editor. Save the changes to the file and retry registering your database.

Expecting ',' delimiter

Problem – `Expecting ',' delimiter: line 1 column 36 (char 35)`

Resolution- – Ensure that the `JSON` file that contains your SAP HANA database credentials is formatted correctly as a `JSON` file. Some characters may be pasted incorrectly after copying them from this file. Edit the file to remove line spaces, double quotes, spaces, and tabs. Add the

formatted file content to your machine, terminal, and in your file editor. Save the changes to the file and retry registering your database.

Maximum limit of resources

Problem – `The number of registered resources under your account <ACCOUNTID> has reached max limit`

Resolution – With AWS Systems Manager for SAP, you can register up to 10 applications per AWS account. You can add up to 20 SAP HANA databases on each application. For more information, see Quotas for AWS Systems Manager for SAP.

Unauthorized user

Problem – `Error executing SSM document - SsmException User: arn:aws:sts::<ACCOUNT_ID>:assumed-role/AWSServiceRoleForAWSSSMForSAP/ssm-sap is not authorized to perform: ssm:SendCommand on resource: arn:aws:ec2:us-east-1:<ACCOUNT_ID>:instance/<INSTANCE_ID> because no identity-based policy allows the ssm:SendCommand action (Service: Ssm, Status Code: 400, Request ID: 25ec41f5-1fa8-4a1a-80ac-6b7e85088d74)`

Resolution – Ensure that your Amazon EC2 instance has the `SSMForSAPManaged` tag with the value `True`. For more information, see Set up required permissions for Amazon EC2 instance running SAP HANA database.

REFRESH_FAILED; Database connection mismatch

Problem – `Application DiscoveryStatus: REFRESH_FAILED; StatusMessage: The database ARN specified in registration input does not match discovered database connection.`

Resolution – The specified `--database-arn` does not match the database connection discovered on the SAP_ABAP instance. Use the `UpdateApplicationSettings` API to provide the correct `--database-arn` of your SAP HANA database along with the `--application-id` of the SAP ABAP application.

```
aws ssm-sap update-application-settings --application-id --database-arn
```

Unsupported setup

Problem – `SSM-SAP only supports single-node SAP_ABAP deployment.`

Resolution – AWS Systems Manager for SAP currently only supports single-node SAP ABAP deployment registration. Your SAP ABAP application must be connected to a single-node SAP HANA instance that resides in the same Amazon EC2 instance. All components belonging to the SAP ABAP application (ASCS, dialog instances, etc.) must also reside on the same Amazon EC2 instance.

Input parameter errors

Problem – `An error occurred (ValidationException) when calling the RegisterApplication operation: Credentials and/or instance number is not expected for SAP applications with type SAP_ABAP.`

Resolution – `--credentials` and `--sap-instance-number` are inapplicable parameters for registering Systems Manager application of type SAP_ABAP. Remove both the parameters from the `RegisterApplication` call.

Problem – `An error occurred (ValidationException) when calling the RegisterApplication operation: The SID and database ARN of ASCS or Application Server must be specified for SAP applications with type SAP_ABAP.`

Resolution – The SID and ARN of ASCS of the connected SAP HANA database are required input parameters for registering SAP ABAP application. Ensure that the connected SAP HANA database has been registered as a Systems Manager application before registering SAP ABAP with AWS Systems Manager for SAP. For more information, see Register your SAP ABAP application with AWS Systems Manager for SAP.

Application status: FAILED

Problem – `System configuration change detected. To continue using this application as a standalone, for operations like backup/restore through AWS Backup, deregister this application and register again.`

Resolution – AWS Systems Manager for SAP does not support moving a highly available (2 nodes) application to a single node system. You must re-register your primary application with the same

application ID to ensure that the primary database is associated with the application, and that backup continuity is maintained. Use the following steps.

1. De-register the database with the following command.

```
aws ssm-sap deregister-application \
--application-id <YOUR_APPLICATION_ID> \
--region <REGION>
```

> **Note**
>
> Use the same *APPLICATION_ID* as the one used during registration.

2. Use the following command to re-register the database with the same *APPLICATION_ID*.

```
aws ssm-sap register-application \
--application-id <YOUR_APPLICATION_ID> \
--region <REGION>
```

Document history

The following table describes the documentation releases for AWS Systems Manager for SAP.

Change	Description	Date
New feature	AWS Backup support for SAP HANA high availability deployments.	December 22, 2023
Policy update	Updated the AWSSSMForSAPServiceLinkedRolePolicy policy.	November 21, 2023
Policy update	Updated the AWSSSMForSAPServiceLinkedRolePolicy policy.	November 17, 2023
New content	Added details for Application tabs to the tutorial.	November 17, 2023
Policy update	Updated the AWSSSMForSAPServiceLinkedRolePolicy policy.	October 31, 2023
New feature	Register SAP ABAP application with AWS Systems Manager for SAP.	October 31, 2023
Policy update	Updated the AWSSSMForSAPServiceLinkedRolePolicy policy.	July 26, 2023
New feature	Register SAP HANA database with AWS Systems Manager for SAP in a high availability setup.	July 26, 2023

Updates	Updated the Get started section of the guide.	March 9, 2023
New content	Added Supported Regions section to the guide.	February 22, 2023
New content	Added Supported versions section to the guide.	February 21, 2023
New content	Added Tutorials section to the guide.	February 15, 2023
Initial release	Initial release of AWS Systems Manager for SAP User Guide.	January 30, 2023
Policy update	Updated the AWSSSMForSAPServiceLinkedRolePolicy policy.	January 5, 2023
Policy update	Updated the AWSSystemsManagerForSAPFullAccess policy.	November 18, 2022
Public preview	Public preview of AWS Systems Manager for SAP.	November 15, 2022