User Guide

AWS Systems Manager for SAP

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Systems Manager for SAP: User Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

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. Systems Manager for SAP is available to use with AWS APIs. For more information, see Systems Manager for SAP API Reference Guide.

With 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.
- Run configuration checks on your registered SAP applications to validate their setup and identify configuration issues.
- Integration with AWS EventBridge Scheduler – using AWS EventBridge Scheduler, schedule SAP management operations such as start, stop, and configuration check operations.

Supported Regions

For more information on currently supported regions for AWS Systems Manager for SAP, see Systems Manager for SAP endpoints and quotas.

> **Note**
>
> Supported services by AWS Region contains the currently supported Regions where SAP HANA database backups on Amazon EC2 instances are available with AWS Backup.

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
- AWS EventBridge Scheduler

Pricing

AWS Systems Manager for SAP follows a simple pricing model where you pay only for the features you use. There are no upfront commitments or minimum fees

Free Features

- SAP application registration and management
- Application-aware start and stop operations
- Basic application monitoring and insights

Usage-Based Features

SAP HANA Database Backup with AWS Backup integration

- No additional charge for backup orchestration through Systems Manager for SAP

- Pay only for AWS Backup storage
- For AWS Backup pricing details, visit AWS Backup pricing

SAP Configuration Management

- $0.25 USD per configuration check run per application in all AWS regions
- Run checks on-demand or on schedule
- Configuration check results are retained for 30 days

Example Pricing Scenario for Configuration Management

If you run three configuration checks weekly on two SAP HANA applications, your monthly cost would be $6.00 USD. This is calculated based on three checks per week, running on two applications, over four weeks, at $0.25 per check (3 checks × 2 applications × 4 weeks × $0.25 = $6.00).

Additional Information

- No charge for registering SAP applications
- No minimum fees or upfront commitments required

Setting up Systems Manager for SAP

If you are new to AWS, begin with the following topics. When you sign up for AWS, your AWS account is automatically signed up for all services in AWS, including Systems Manager for SAP.

Topics

Sign up for AWS

To sign up for an AWS account

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

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

   Part of the sign-up procedure involves email verification and either receiving a phone call or SMS to enter a verification code.

   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 a 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 Create an IAM user for emergency access in the *IAM User Guide*.	Configure programmatic access by Manage 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.

Topics

Attach 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`

Identify or create SAP HANA user

The SAP HANA database user credentials that you provide to AWS Systems Manager for SAP must have specific privileges based on the operations you intend to perform.

You must provide credentials for the SYSTEM_DB user, which requires SAP HANA system privileges. The following table shows the required privileges for different operations:

Operation	Required Privileges
Application registration and discovery	CATALOG READ
Backup operations with AWS Backup	BACKUP ADMIN, INFILE ADMIN

You can use an existing SYSTEM_DB user with the required privileges, or create a new dedicated user for AWS Systems Manager for SAP operations. Optionally, you can also provide credentials for individual tenant database users.

When creating or identifying the SAP HANA user, ensure that the password does not contain the following special characters:

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

Register SAP HANA database credentials in AWS Secrets Manager

You must create a secret with the username and password of the SAP HANA users identified or created in the previous section. A separate secret is required for each user of your databases running on an Amazon EC2 instance.

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 Register your SAP HANA databases with Systems Manager for SAP.
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::123456789012: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 EC2 instance has Python 3.5 or later installed. SSM-SAP automatically uses the latest Python version available on your system. For custom-built or compiled Python installations, ensure that the _lzma module is included in the build and available within your Python environment.
- 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

You can manage your SAP deployments with Systems Manager for SAP using AWS CLI or AWS Management Console. This section provides tutorials to perform these tasks.

See the following topics for detailed tutorials.

Topics

AWS CLI

Using AWS CLI, you can register SAP HANA or SAP ABAP applications, start, stop, refresh, and deregister SAP applications with Systems Manager for SAP.

Topics

Register your SAP HANA databases with Systems Manager for SAP

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

Topics

- Step 2: Register database
- Step 3: Check registration status
- Step 4: Verify registration
- Step 5: View component summary
- Backup your database – optional

Step 1: Create a JSON for credentials

Create a JSON file to store the credentials you created in Register SAP HANA database 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 Register SAP HANA database credentials in AWS Secrets Manager.

The following is an example JSON file.

```
[
    {
        "DatabaseName": "HDB/SYSTEMDB",
        "CredentialType": "ADMIN",
        "SecretId": "HANABackup"
```

```
    },
    {
        "DatabaseName": "HDB/HDB",
        "CredentialType": "ADMIN",
        "SecretId": "HANABackup"
    }
]
```

Step 2: Register database

Register your SAP HANA databases using the following command.

Make sure to use the correct SAP HANA database instance number and SAP HANA database name (SID). These are different than the SAP instance number and SAP System Identifier.

Command Template

```
aws ssm-sap register-application --application-id <APPLICATION_ID> --
application-type HANA --instances <YOUR_EC2_INSTANCE_ID> --sap-instance-number
 <YOUR_HANA_DATABASE_SYSTEM_NUMBER> --sid <YOUR_HANA_DATABASE_SID> --region <REGION> --
credentials file://<PATH_TO_YOUR_CREDENTIALS_JSON_FILE>
```

Example command with sample values

```
aws ssm-sap register-application \
--application-id myHanaApplication \
--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": "myHanaApplication",
        "Type": "HANA",
        "Arn": "<APPLICATION_ARN>",
        "Status": "REGISTERING",
```

```
        "Components": [],
        "LastUpdated": "2022-08-19T10:58:48.521000-07:00"
    },
    "OperationId": "6bd44104-d63c-449d-8007-6c1b471e3e5e" //(1)
}
```

1. Take note of this operation ID. You'll need it in the next step.

In the preceding example, the instance number is 00 and SID is HDB. This can be verified with `/usr/sap/<SID>/HDB<instance number>`. For example, the path will be `/usr/sap/HDB/HDB00`.

> **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 a few 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 <REGION>
```

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 <APPLICATON_ID> --region <REGION>
```

Example to get the summary of an application

```
aws ssm-sap get-application \
--application-id myHanaApplication \
--region us-east-1
```

Example output

```
{
    "Application": {
        "Id": "myHanaApplication",
        "Type": "HANA",
        "Arn": "arn:aws:ssm-sap:us-east-1:123456789123:HANA/myHanaApplication",
        "Status": "ACTIVATED",
        "DiscoveryStatus": "SUCCESS",
        "Components": [
            "HDB-HDB00" //(1)
        ],
        "LastUpdated": "2023-07-06T13:25:35.702000-07:00"
    },
    "Tags": {}
}
```

1. Take note of this component ID. You'll need it in the next step.

Step 5: View component summary

Get the component summary with GetComponent API.

```
aws ssm-sap get-component --application-id <APPLICATION_ID> --component-id
 <YOUR_COMPONENT_ID_FROM_LAST_STEP> --region <REGION>
```

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 Systems Manager for SAP.

Example

Single node

GetComponent API output for parent component


```
{
    "Component": {
        "ComponentId": "HDB-HDB00",
        "ChildComponents": [
            "HDB-HDB00-sapci"
        ],
        "ApplicationId": "myHanaApplication",
        "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/myHanaApplication/
COMPONENT/HDB-HDB00"
    },
    "Tags": {}
}
```


GetComponent API output for child component


```
{
```

```
    "Component": {
        "ComponentId": "HDB-HDB00-sapci",
        "ParentComponent": "HDB-HDB00",
        "ApplicationId": "myHanaApplication",
        "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/myHanaApplication/
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": "myHanaApplication",
        "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/myHanaApplication/
COMPONENT/HDB-HDB00"
    },
    "Tags": {}
}
```

GetComponent API output for child component (primary)

```
{
    "Component": {
        "ComponentId": "HDB-HDB00-sappridb",
        "ParentComponent": "HDB-HDB00",
        "ApplicationId": "myHanaApplication",
        "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/myHanaApplication/
COMPONENT/HDB-HDB00-sappridb"
    },
    "Tags": {}
}
```

GetComponent API output for child component (secondary)

```
{
    "Component": {
        "ComponentId": "HDB-HDB00-sapsecdb",
        "ParentComponent": "HDB-HDB00",
```

```
        "ApplicationId": "myHanaApplication",
        "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/myHanaApplication/
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 your SAP ABAP application with AWS Systems Manager for SAP

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

Topics

- 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 Register your SAP HANA databases with Systems Manager for SAP.

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 <APPLICATION_ID>
```

```
{
    "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", //(Note)
            "Tags": {}
        }
    ]
}
```

Note the `database-arn` for use in the next step.

3. Register your SAP ABAP application with the following command.

Command template

```
aws ssm-sap register-application \
--application-id <APPLICATION_ID> \
--application-type SAP_ABAP \
--instances <YOUR_EC2_INSTANCE_ID> \
--sid <YOUR_HANA_SID> \
--region <REGION>
--database-arn <SAP HANA DATABASE ARN FROM REGISTERED APPLICATION>
--component-info '[
    {
      "ComponentType": "WD",
      "Sid": "<YOUR_WEB_DISPATCHER_SID>",
      "Ec2InstanceId": "<YOUR_YOUR_WEB_DISPATCHER_EC2_INSTANCE_ID>"
    }
  ]'
```

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"
    --component-info '[{"ComponentType": "WD", "Sid":"WD1",
 "Ec2InstanceId":"i-07837dbacc572b5f2"}]'
```

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" //(Note)
}
```

Note 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 <REGION>
```

Step 4: Verify registration

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

1. Run Commands to Verify Registration

   Command template

   ```
   aws ssm-sap get-application --application-id <APPLICATION_ID> --region <REGION>
   ```

   Example to get the summary of an application

   ```
   aws ssm-sap get-application --application-id mySAPABAPApplication --region us-east-1
   ```

   Example JSON Response

   ```
   {
     "Application": {
       "Id": "mySAPABAPApplication",
       "Type": "SAP_ABAP",
       "Arn": "arn:aws:ssm-sap:us-east-1:123456789101:SAP_ABAP/mySAPABAPApplication",
       "Status": "ACTIVATED",
   ```

```
    "DiscoveryStatus": "SUCCESS",
    "Components": [
        "ECD-ABAP"
        "WD1-WD14"  //(Note)
    ]
    "LastUpdated": "2023-10-04T22:16:59.106000-07:00"
  },
  "Tags": {}
}
```

Note Take note of this component ID. You'll need it in the next step.

Step 5: View component summary

Get the component summary with GetComponent API.

1. Command template

```
aws ssm-sap get-component --application-id <APPLICATION_ID> --component-id
 <YOUR_COMPONENT_ID_FROM_LAST_STEP> --region <REGION>
```

2. GetComponent API output for parent component ECD-ABAP

```
aws ssm-sap get-component \
   --application-id mySAPABAPApplication \
   --component-id ECD-ABAP \
   --region us-east-1
```

Sample JSON Output

```
{
    "Component": {
        "ComponentId": "ECD-ABAP",
        "Sid": "ECD",
        "ChildComponents": [
            "ECD-ASCS10-sapci",
            "ECD-D12-sapci"
            "ECD-D00-sapappser1",
            "ECD-D00-sapappser2"
        ],
        "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": {}
}
```

3. GetComponent API output for parent component WD1-W14

```
aws ssm-sap get-component --component-id WD1-W14\
    --application-id mySAPABAPApplication \
    --region us-east-1
```

Sample JSON Output

```
{
    "Component": {
        "ComponentId": "WD1-W14",
        "Sid": "WD1",
        "ChildComponents": [
            "WD1-W14-sapwd"
        ],
        "ApplicationId": "mySAPABAPApplication",
        "ComponentType": "WEBDISP",
        "Status": "RUNNING",
        "LastUpdated": "2024-10-04T22:16:59.089000-07:00",

        "Arn": "arn:aws:ssm-sap:us-east-1:123456789101:SAP_ABAP/mySAPABAPApplication/
COMPONENT/WD1-W14"
    },
    "Tags": {}
}
```

4. GetComponent API output for child component ECD-ASCS10-sapci

```
aws ssm-sap get-component \
    --component-id ECD-ASCS10-sapci --application-id mySAPABAPApplication \
    --region us-east-1
```

Sample Output

```
{
    "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": {}
}
```

5. GetComponent API for Child Component WD1-W14-sapwd

```
aws ssm-sap get-component \
   --component-id WD1-W14-sapwd --application-id mySAPABAPApplication \
   --region us-east-1
```

Sample Output

```
{
    "Component": {
        "ComponentId": "WD1-W14-sapwd",
        "Sid": "WD1",
        "SystemNumber": "14",
        "ParentComponent": "WD1-W14",
        "ApplicationId": "mySAPABAPApplication",
        "ComponentType": "WD",
        "Status": "RUNNING",
        "SapFeature": "WEBDISP",
        "SapHostname": "sapci",
        "SapKernelVersion": "785, patch 200, changelist 2150416",
        "Resilience": {
            "EnqueueReplication": false
        },
        "AssociatedHost": {
            "Hostname": "sapwd",
            "Ec2InstanceId": "i-12345abcde678f9g0",
            "IpAddresses": [
                {
                    "IpAddress": "172.31.32.187",
                    "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/WD1-W14-sapwd"
    },
    "Tags": {}
}
```

Start SAP application

You can perform a start operation on a single node or HA (high availability) SAP HANA application or on a single node or distributed setup of an SAP ABAP application which is registered with AWS Systems Manager for SAP.

When starting an SAP HANA application, the Amazon EC2 instance(s) on which the SAP HANA application will run is started first (if it is not already running), before the application is started. When starting a single node setup of an SAP ABAP application, the HANA database and/or the Amazon EC2 instance on which the SAP ABAP application will run is started first (if it is not already running).

Before you initiate a start operation, complete the setup prerequisites described in Get started with AWS Systems Manager for SAP and register your SAP application, if you have not already done so.

You can start Systems Manager for SAP application using AWS CLI or AWS Management Console. The following procedure is for starting an SAP application using AWS CLI.

Topics

Step 1: Register SAP Application

Register your SAP application, if you have not already done so. For more information, see Register SAP HANA database or Register SAP ABAP application.

In your records, note the `ApplicationId` of your registration.

Step 2: Start SAP Application

You can use the following AWS CLI command to start your SAP application:

```
aws ssm-sap start-application \
--application-id <APPLICATION_ID> \
--region <REGION_ID>
```

The parameter `application-id` is required. As the value, use the ApplicationID generated from registration in Step 1.

Command template

```
aws ssm-sap start-application --application-id <APPLICATION_ID> --region <REGION_ID>
```

Command example

```
aws ssm-sap start-application \
--application-id myHanaApplication \
--region us-east-1
```

Return example

```
{
    "OperationId": "a7h4j3k6-8463-836h-018h-7sh377h6hhd6" //(Note)
}
```

Note the OperationId for use in the next step

Step 3: Check Start Operation status

The start operation can take up to five minutes to complete. During that time, you can use the following command to check the status of the operation. Use the `OperationId` that was generated in Step 2.

Command template

```
aws ssm-sap get-operation --operation-id <OPERATION_ID> --region <REGION_ID>
```

Step 4: Monitor and verify Start operation

Verify the start operation on the application through the event using the ListOperationEvents API.

Command template

```
aws ssm-sap list-operation-events --operation-id <OPERATION_ID> --region <REGION_ID>
```

Command example

```
aws ssm-sap list-operation-events \
--operation-id b2bc3266-9369-4163-b935-6a586c80e76b \
--region us-east-1
```

Json output

```
{
    "OperationEvents": [
        {
            "Description": "Start the SAP component ECD-ABAP",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-ABAP",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:53:59.846000+00:00"
        },
        {
            "Description": "Start the SAP component ECD-D12-sapci",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-D12-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:52:59.846000+00:00"
        },
        {
            "Description": "Start the SAP component ECD-D12-sapci",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-D12-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:51:59.846000+00:00"
        },
        {
            "Description": "Start the SAP component ECD-ASCS10-sapci",
```

```
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-ASCS10-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:50:59.846000+00:00"
        },
        {
            "Description": "Start the SAP component ECD-ASCS10-sapci",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-ASCS10-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:49:59.846000+00:00"
        },
        {
            "Description": "Start the SAP component ECD-ABAP",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-ABAP",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:48:59.846000+00:00"
        },
        {
            "Description": "Start the SAP component HDB-HDB00",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:HANA/
hanaStartStop/COMPONENT/HDB-HDB00",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:47:59.856000+00:00"
        },
        {
            "Description": "Start the SAP component HDB-HDB00-sapci",
```

```
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:HANA/
hanaStartStop/COMPONENT/HDB-HDB00-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:47:59.846000+00:00"
        },
        {
            "Description": "Start the SAP component HDB-HDB00-sapci",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:HANA/
hanaStartStop/COMPONENT/HDB-HDB00-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:46:59.846000+00:00"
        },
        {
            "Description": "Start the SAP component HDB-HDB00",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:HANA/
hanaStartStop/COMPONENT/HDB-HDB00",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:46:59.836000+00:00"
        },
        {
            "Description": "Start the EC2 instance i-abcdefgh987654321",
            "Resource": {
                "ResourceArn": "arn:aws:ec2:us-east-1:111111111111:instance/i-
abcdefgh987654321",
                "ResourceType": "AWS::EC2::Instance"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:45:59.846000+00:00"
        },
        {
            "Description": "Start the EC2 instance i-abcdefgh987654321",
```

```
            "Resource": {
                "ResourceArn": "arn:aws:ec2:us-east-1:111111111111:instance/i-
abcdefgh987654321",
                "ResourceType": "AWS::EC2::Instance"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:44:59.846000+00:00"
        }
    ]
}
```

Stop SAP application

You can perform a stop operation on a single node or HA (high availability) SAP HANA application or on a single node or distrubuted setup of SAP ABAP application that has been registered with AWS Systems Manager for SAP.

While performing the stop operation on an SAP HANA application, you can optionally also stop the Amazon EC2 instance(s) on which the SAP HANA application is running. While performing a stop operation on a single node setup of SAP ABAP application, you can optionally also stop the HANA database application and the Amazon EC2 instance on which the SAP ABAP application is running.

Before you initiate a stop operation, complete the setup prerequisites described in Get started with AWS Systems Manager for SAP and register your SAP application, if you have not already done so.

You can stop Systems Manager for SAP application using AWS CLI or AWS Management Console. The following procedure is for stopping an SAP application using AWS CLI.

Topics

Step 1: Register SAP Application

Register your SAP application, if you have not already done so. For more information, see Register SAP HANA database or Register SAP ABAP application.

Step 2: Stop SAP Application

You can use the following AWS CLI command to stop your SAP application:

```
aws ssm-sap stop-application \
--application-id <APPLICATION_ID> \
--stop-connected-entity <ENTITY> \
--include-ec2-instance-shutdown \
--region <REGION_ID>
```

The parameter `application-id` is required. As the value, use the ApplicationID generated from registration in Step 1.

The following parameters are optional:

- Use the `stop-connected-entity` parameter with a value of DBMS (Database Management System) to also stop the corresponding database application when you stop a single node setup of an SAP ABAP application.
- Use the Boolean parameter `include-ec2-instance-shutdown` to shut down the Amazon EC2 instance on which the SAP HANA or single node set up of an SAP ABAP application is running

The following are examples of the stop operation on a single node SAP ABAP setup and an SAP HANA setup with AWS Systems Manager for SAP:

Example

SAP ABAP

Command template

```
aws ssm-sap stop-application --application-id <APPLICATION_ID> --stop-connected-
entity <ENTITY> --include-ec2-instance-shutdown --region <REGION_ID>
```

Command example

```
aws ssm-sap stop-application \
--application-id myABAPApplication \
--stop-connected-entity DBMS \
--include-ec2-instance-shutdown \
```

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

Return example

```
{
    "OperationId": "a7h4j3k6-8463-836h-018h-7sh377h6hhd6"
}
```

SAP HANA

Command template

```
aws ssm-sap stop-application --application-id <APPLICATION_ID> --include-ec2-
instance-shutdown --region <REGION_ID>
```

Command example

```
aws ssm-sap stop-application \
--application-id myABAPApplication \
--include-ec2-instance-shutdown \
--region us-east-1
```

Return Example

```
{
    "OperationId": "j3h5j4k5-8323-192j-102n-18h7hhh27h27"
}
```

Step 3: Check Stop Operation status

The stop operation can take up to five minutes to complete. During that time, you can use the following command to check the status of the operation. Use the `OperationId` that was generated in Step 2.

Command template

```
aws ssm-sap get-operation --operation-id <OPERATION_ID> --region <REGION_ID>
```

Command example

```
aws ssm-sap get-operation \
--operation-id b2bc3266-9369-4163-b935-6a586c80e76b \
--region us-east-1
```

Step 4: Monitor and verify stop operation

Verify the stop operation on the application through the event using the ListOperationEvents API.

Command template

```
aws ssm-sap list-operation-events --operation-id <OPERATION_ID> --region <REGION_ID>
```

Command example

```
aws ssm-sap list-operation-events \
--operation-id a1bc2345-6789-0123-d456-7e890f12g34h
```

Return example

```
{
    "OperationEvents": [
        {
            "Description": "Stop the EC2 instance i-abcdefgh987654321",
            "Resource": {
                "ResourceArn": "arn:aws:ec2:us-east-1:111111111111:instance/i-
abcdefgh987654321",
                "ResourceType": "AWS::EC2::Instance"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:55:59.846000+00:00"
        },
        {
            "Description": "Stop the EC2 instance i-abcdefgh987654321",
            "Resource": {
                "ResourceArn": "arn:aws:ec2:us-east-1:111111111111:instance/i-
abcdefgh987654321",
                "ResourceType": "AWS::EC2::Instance"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:54:59.846000+00:00"
```

```
        },
        {
            "Description": "Stop the SAP component HDB-HDB00",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:HANA/
hanaStartStop/COMPONENT/HDB-HDB00",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:53:59.846000+00:00"
        },
        {
            "Description": "Stop the SAP component HDB-HDB00-sapci",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:HANA/
hanaStartStop/COMPONENT/HDB-HDB00-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:52:59.846000+00:00"
        },
        {
            "Description": "Stop the SAP component HDB-HDB00-sapci",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:HANA/
hanaStartStop/COMPONENT/HDB-HDB00-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:51:59.846000+00:00"
        },
        {
            "Description": "Stop the SAP component HDB-HDB00",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:HANA/
hanaStartStop/COMPONENT/HDB-HDB00",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:50:59.846000+00:00"
```

```
        },
        {
            "Description": "Stop the SAP component ECD-ABAP",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-ABAP",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:49:59.846000+00:00"
        },
        {
            "Description": "Stop the SAP component ECD-ASCS10-sapci",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-ASCS10-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:48:59.846000+00:00"
        },
        {
            "Description": "Stop the SAP component ECD-ASCS10-sapci",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-ASCS10-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:47:59.846000+00:00"
        },
        {
            "Description": "Stop the SAP component ECD-D12-sapci",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-D12-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "COMPLETED",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:46:59.846000+00:00"
```

```
        },
        {
            "Description": "Stop the SAP component ECD-D12-sapci",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-D12-sapci",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:45:59.846000+00:00"
        },
        {
            "Description": "Stop the SAP component ECD-ABAP",
            "Resource": {
                "ResourceArn": "arn:aws:ssm-sap:us-east-1:111111111111:SAP_ABAP/
nwStartStop/COMPONENT/ECD-ABAP",
                "ResourceType": "AWS::SystemsManagerSAP::Component"
            },
            "Status": "IN_PROGRESS",
            "StatusMessage": "",
            "Timestamp": "2024-01-03T04:44:59.846000+00:00"
        }
    ]
}
```

Refresh SAP application

The following steps will guide you through a refresh of your SAP HANA application or of your single node setup of SAP ABAP application. This refresh updates the application metadata in the AWS Systems Manager for SAP.

Before you refresh an application, complete the setup prerequisites described in Get started with AWS Systems Manager for SAP and register your SAP application if you have not already done so.

Step 1: Register SAP Application

Register your SAP application, if you have not already done so. For more information, see Register SAP HANA database or Register SAP ABAP application.

In your records, note the `ApplicationId` of your registration.

Step 2: Refresh SAP Application

You can use the following AWS CLI command to refresh your SAP application:

```
aws ssm-sap start-application-refresh \
--application-id <APPLICATION_ID> \
--region <REGION_ID>
```

The parameter `application-id` is required. As the value, use the ApplicationID generated from registration in Step 1.

Step 3: Check Refresh Operation status

The refresh operation can take up to five minutes to complete. During that time, you can use the following command to check the status of the operation. Use the `OperationId` generated in Step 2.

Command template

```
aws ssm-sap get-operation \
--operation-id <OPERATION_ID> \
--region <REGION_ID>
```

Step 4: Verify application status

Use the command get-application (GetApplication API) to verify the application status. You can also view the details of registered databases with `ListDatabases` and `GetDatabase` API.

Command template

```
aws ssm-sap get-application --application-id <APPLICATION_ID> --region <REGION_ID>
```

Example to get the summary of an application

```
aws ssm-sap get-application \
--application-id mySAPABAPApplication \
--region us-east-1
```

Response example

```
{
"Application": {
"Id": "mySAPABAPApplication",
    "Type": "SAP_ABAP",
    "Arn": "arn:aws:ssm-sap:us-east-1:123456789101:SAP_ABAP/mySAPABAPApplication",
    "Status": "ACTIVATED",
    "DiscoveryStatus": "SUCCESS",
    "Components": [
        "ECD-ABAP"
    ],
    "LastUpdated": "2023-10-04T22:16:59.106000-07:00"
  },
  "Tags": {}
}
```

Deregister SAP application

The following steps will guide you through deregistration your SAP HANA application or of your single node setup of SAP ABAP application registered with Systems Manager for SAP.

If a database has not been previously registered with AWS Systems Manager, the deregistration process will result in a `ValidationException`.

Step 1: Get ApplicationId of your SAP application

Command template

```
aws ssm-sap list-applications --region <REGION_ID>
```

Note the `ApplicationId` of your registration.

Step 2: Deregister SAP application

You can use the AWS CLI command deregister-application (API DeregisterApplication) to deregister your SAP application.

Command template

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

The parameter `application-id` is required. As the value, use the ApplicationID retrieved in Step 1.

Step 3: Verify deregistration

Run the command list-applications (ListApplications API) to verify your application is not present.

Run Configuration Checks with Systems Manager for SAP

You can run configuration checks on your registered SAP applications to validate their setup and ensure they follow best practices. Configuration checks are organized to help you execute checks and understand their results:

- **Configuration Check** - The top level at which checks are executed. Each check comprehensively answers a question such as "Have I chosen the right instance?" or "Is my storage configured correctly?"
- **SubCheck** - A logical grouping used to organize and view results. SubChecks group related information based on how it is gathered or defined. For example, all package status checks or parameters for a specific resource might be grouped into one subcheck.
- **Results** - Individual findings that evaluate a single parameter or configuration point in the system. Results can apply to a resource or be evaluated against the application. For example, "This package is installed on the primary HANA instance" or "Timezone is consistent across both the primary and secondary instances".

You start configuration checks at the check level, while subchecks and results provide structured ways to view and understand the findings.

Topics

Run Configuration Checks

Step 1: View Available Checks

View the list of available configuration checks to determine which checks you wish to evaluate for your SAP application.

Command template

```
aws ssm-sap list-configuration-check-definitions --region <REGION_ID>
```

Example command with sample values

```
aws ssm-sap list-configuration-check-definitions --region us-east-1
```

Example JSON response

```
{
    "ConfigurationChecks": [
        {
            "Id": "SAP_CHECK_01",
            "Name": "SAP EC2 Instance Type Selection",
            "Description": "Checks any EC2 Instances Associated with this HANA
 Application, and evaluates whether the Instance Type complies with SAP Certification
 requirements and that necessary hardware settings are in place.",
            "ApplicableApplicationTypes": [
                "HANA"
            ]
        },
        {
            "Id": "SAP_CHECK_02",
            "Name": "SAP HANA EBS Storage Configuration",
            "Description": "Application SAP HANA EBS Storage Configuration on Amazon
 EC2 Instances",
            "ApplicableApplicationTypes": [
                "HANA"
            ]
        },
        {
            "Id": "SAP_CHECK_03",
            "Name": "SAP HANA Pacemaker Configuration",
            "Description": "Application SAP HANA Resilience - Pacemaker Cluster
 Configuration",
            "ApplicableApplicationTypes": [
                "HANA"
            ]
        }
    ]
}
```

1. Use the check IDs (such as SAP_CHECK_01) when you want to start specific checks rather than running all available checks.

Step 2: Start Configuration Checks

Start the configuration checks for your application. You can run all available checks specify individual check ids. If no configuration-check-ids are specified, all checks will be run.

Command template

```
aws ssm-sap start-configuration-checks \
--application-id <APPLICATION_ID> \
--configuration-check-ids <CHECK_ID> \
--region <REGION_ID>
```

Example command with sample values

```
aws ssm-sap start-configuration-checks \
--application-id myHanaApplication \
--configuration-check-ids SAP_CHECK_03 \
--region us-east-1
```

Example JSON response

```
{
    "ConfigurationCheckOperations": [
        {
            "Id": "af3142c1-f178-49e7-a390-ad047e2d518d", //(1)
            "ApplicationId": "myHanaApplication",
            "ConfigurationCheckId": "SAP_CHECK_03",
            "ConfigurationCheckName": "SAP HANA Pacemaker Configuration",
            "ConfigurationCheckDescription": "Application SAP HANA Resilience -
 Pacemaker Cluster Configuration"
        }
    ]
}
```

1. Take note of this operation ID. You'll need it to check the status and view results.

Step 3: Monitor Check Status

The configuration checks may take several minutes to complete. Use the following command to check the status.

Command template

```
aws ssm-sap get-configuration-check-operation --operation-id <OPERATION_ID> --region
 <REGION_ID>
```

Example command with sample values

```
aws ssm-sap get-configuration-check-operation \
--operation-id 6bd44104-d63c-449d-8007-6c1b471e3e5e \
--region us-east-1
```

Example JSON response in progress

```
{
    "ConfigurationCheckOperation": {
        "Id": "12345678-abcd-efab-cdef-123456789abc",
        "ApplicationId": "HANA_H4H",
        "Status": "INPROGRESS",
        "ConfigurationCheckId": "SAP_CHECK_03",
        "ConfigurationCheckName": "SAP HANA Pacemaker Configuration",
        "ConfigurationCheckDescription": "Application SAP HANA Resilience - Pacemaker
 Cluster Configuration",
        "StartTime": "2025-08-25T14:11:39.080000+10:00"
    }
}
```

Example JSON response successful

```
{
    "ConfigurationCheckOperation": {
        "Id": "12345678-abcd-efab-cdef-123456789abc",
        "ApplicationId": "HANA_H4H",
        "Status": "SUCCESS",
        "StatusMessage": "Configuration Check operation completed successfully",
        "ConfigurationCheckId": "SAP_CHECK_03",
        "ConfigurationCheckName": "SAP HANA Pacemaker Configuration",
```

```
        "ConfigurationCheckDescription": "Application SAP HANA Resilience - Pacemaker
 Cluster Configuration",
        "StartTime": "2025-08-25T14:11:39.080000+10:00",
        "EndTime": "2025-08-25T14:14:32.262000+10:00",
        "RuleStatusCounts": {
            "Failed": 6,
            "Warning": 5,
            "Info": 10,
            "Passed": 144,
            "Unknown": 0
        }
    }
}
```

Reviewing Configuration Check Results

Configuration check results are organized hierarchically. Start by identifying the check operation you want to review, then drill down through subchecks to view individual rule results.

Step 1: List Check Operations

View the history of configuration check operations. Each operation represents a complete execution of one or more configuration checks. You can list all operations or just the latest operation for each check type.

Command template

```
aws ssm-sap list-configuration-check-operations \
--application-id <APPLICATION_ID> \
--region <REGION_ID> \
--list-mode <LIST_MODE>
```

The `--list-mode` parameter accepts two values:

- `ALL_OPERATIONS` (default) - Lists all configuration check operations
- `LATEST_PER_CHECK` - Lists only the most recent operation for each check type

Example command with sample values

```
aws ssm-sap list-configuration-check-operations \
--application-id myHanaApplication \
```

```
--region us-east-1 \
--list-mode LATEST_PER_CHECK
```

Example JSON response

```
{
    "ConfigurationCheckOperations": [
        {
            "Id": "12345678-abcd-efab-cdef-123456789abc",
            "ApplicationId": "HANA_H4H",
            "Status": "SUCCESS",
            "StatusMessage": "Configuration Check operation completed successfully",
            "ConfigurationCheckId": "SAP_CHECK_03",
            "ConfigurationCheckName": "SAP HANA Pacemaker Configuration",
            "ConfigurationCheckDescription": "Application SAP HANA Resilience -
 Pacemaker Cluster Configuration",
            "StartTime": "2025-08-25T14:11:39.080000+10:00",
            "EndTime": "2025-08-25T14:14:32.262000+10:00",
            "RuleStatusCounts": {
                "Failed": 6,
                "Warning": 5,
                "Info": 10,
                "Passed": 144,
                "Unknown": 0
            }
        },
        {
            "Id": "98765432-dcba-abcd-efab-987654321def",
            "ApplicationId": "HANA_H4H",
            "Status": "SUCCESS",
            "StatusMessage": "Configuration Check operation completed successfully",
            "ConfigurationCheckId": "SAP_CHECK_02",
            "ConfigurationCheckName": "SAP HANA EBS Storage Configuration",
            "ConfigurationCheckDescription": "Application SAP HANA EBS Storage
 Configuration on Amazon EC2 Instances",
            "StartTime": "2025-08-25T14:11:38.961000+10:00",
            "EndTime": "2025-08-25T14:12:35.030000+10:00",
            "RuleStatusCounts": {
                "Failed": 7,
                "Warning": 20,
                "Info": 43,
                "Passed": 40,
                "Unknown": 0
```

```
            }
        },
        {
            "Id": "11223344-aabb-ccdd-eeff-112233445566",
            "ApplicationId": "HANA_H4H",
            "Status": "SUCCESS",
            "StatusMessage": "Configuration Check operation completed successfully",
            "ConfigurationCheckId": "SAP_CHECK_01",
            "ConfigurationCheckName": "SAP EC2 Instance Type Selection",
            "ConfigurationCheckDescription": "Checks any EC2 Instances Associated
 with this HANA Application, and evaluates whether the Instance Type complies with SAP
 Certification requirements and that necessary hardware settings are in place",
            "StartTime": "2025-08-25T14:11:38.807000+10:00",
            "EndTime": "2025-08-25T14:12:25.237000+10:00",
            "RuleStatusCounts": {
                "Failed": 0,
                "Warning": 2,
                "Info": 8,
                "Passed": 36,
                "Unknown": 0
            }
        }
    ]
}
```


Step 2: View Sub-Check Results

Each configuration check is divided into subchecks that group related rules together. For example, a subcheck might focus on package status checks or parameters for a specific resource. list-sub-check-results provides the subcheck-ids which allow you to view the detailed reuslts.

Command template

```
aws ssm-sap list-sub-check-results --operation-id <OPERATION_ID> --region <REGION_ID>
```

Example command with sample values

```
aws ssm-sap list-sub-check-results \
--operation-id 6bd44104-d63c-449d-8007-6c1b471e3e5e \
--region us-east-1
```

Example JSON response

```
{
    "SubCheckResults": [
        {
            "Id": "55667788-1122-3344-5566-778899aabbcc",
            "Name": "Operating System Package Prerequisites",
            "Description": "Validates required Operating System packages for SAP HANA
 High Availability are installed and aligned between cluster nodes. Requirements are
 based on known restrictions for Operating System, Version and SAP HANA Revision",
            "References": [
                "[SAP on AWS Hana High Availability Configuration / Red Hat /
 Prerequisites / Operating System Requirements / Packages](https://docs.aws.amazon.com/
sap/latest/sap-hana/sap-hana-pacemaker-rhel-os-settings.html#packages)",
                "[SAP on AWS Hana High Availability Configuration / SUSE /
 Prerequisites / Operating System Requirements / Packages](https://docs.aws.amazon.com/
sap/latest/sap-hana/sap-hana-pacemaker-sles-os-settings.html#packages)"
            ]
        },
        {
            "Id": "abcdef12-3456-7890-abcd-ef1234567890",
            "Name": "Linux Systemd Service Configuration",
            "Description": "Validates systemd service status and enablement for
 required High Availability services including Corosync and Pacemaker",
            "References": [
                "[SAP on AWS Hana High Availability Configuration / Red Hat /
 Prerequisites / Operating System Requirements](https://docs.aws.amazon.com/sap/latest/
sap-hana/sap-hana-pacemaker-rhel-os-settings.html)",
                "[SAP on AWS Hana High Availability Configuration / SUSE /
 Prerequisites / Operating System Requirements](https://docs.aws.amazon.com/sap/latest/
sap-hana/sap-hana-pacemaker-sles-os-settings.html)"
            ]
        },
        // additional subchecks
    ]

}
```

Note Take note of the sub-check result IDs. You'll need them to view detailed rule results.

Step 3: View Rule Results

View the detailed results for each rule within a sub-check.

Command template

```
aws ssm-sap list-sub-check-rule-results --sub-check-result-id <SUB_CHECK_RESULT_ID> --
region <REGION_ID>
```

Example command with sample values

```
aws ssm-sap list-sub-check-rule-results \
--sub-check-result-id 197fad22-aa0a-4fbf-a26a-1d2f034ffa46 \
--region us-east-1
```

Example JSON response

```
{
    "RuleResults": [
        {
            "Id": "52df02e1-511d-4023-ba61-617a71c5f0c9",
            "Description": "Pacemaker cluster property 'stonith-enabled' matches SAP
 HANA cluster recommendations",
            "Status": "PASSED",
            "Message": "STONITH is enabled for cluster fencing",
            "Metadata": {
                "ActualValue": "true",
                "ClusterParameter": "stonith-enabled",
                "Component": "H4H-HDB00",
                "ExpectedValue": "true"
            }
        },
        {
            "Id": "d3501b51-c675-467c-8fd6-76741fafe32a",
            "Description": "Pacemaker cluster property 'stonith-action' matches SAP
 HANA cluster recommendations",
            "Status": "PASSED",
            "Message": "STONITH action configured for controlled node recovery",
            "Metadata": {
                "ActualValue": "off",
                "ClusterParameter": "stonith-action",
                "Component": "H4H-HDB00",
                "ExpectedValue": "off"
            }
        },
        {
            "Id": "281bbdf3-65c8-4b44-bdef-109190ee6201",
```

```
            "Description": "Pacemaker cluster property 'stonith-timeout' matches SAP
 HANA cluster recommendations",
            "Status": "PASSED",
            "Message": "STONITH timeout configured to allow sufficient time for fencing
 operations",
            "Metadata": {
                "ActualValue": "600",
                "ClusterParameter": "stonith-timeout",
                "Component": "H4H-HDB00",
                "ExpectedValue": "600"
            }
        },
        // additional rules
    ]
}
```

AWS Management Console

Using AWS Management Console, you can register SAP HANA and SAP ABAP applications, and start or stop SAP applications with Systems Manager for SAP.

Topics

- Register SAP HANA database with AWS Systems Manager for SAP
- Register SAP ABAP application with AWS Systems Manager for SAP
- Start SAP application
- Stop SAP application
- Run Configuration Checks

Register SAP HANA database with AWS Systems Manager for SAP

Follow along these steps to register SAP HANA database as a Systems Manager for SAP application.

1. Go to https://console.aws.amazon.com/systems-manager/ > **Application Tools** > **Application Manager**.
2. Select **Create Application** > **Enterprise Workload**.
3. For Application type, select **SAP HANA**.
4. In **Application details**, enter a name for the application you want to register with Application Manager.

5. 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.
6. *Optional* In **Application tags**, you can add 100 tags associated to resources.
7. Select **Create**.

Application tabs

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

Example

Overview

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

Resources

You can find the **Topology** of a 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 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.

   Under **Select an application or resource group**, make sure to select the SAP HANA application registered with Systems Manager for SAP.

   > **Note**
   >
   > You can create only one CloudWatch Application Insights application on a single-node SAP ABAP application. You can onboard either the SAP ABAP application or the connected SAP HANA application.

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.

The cost of the single-node SAP ABAP application is an aggregate of the cost of SAP ABAP and SAP HANA applications on the same EC2 instance.

Register SAP ABAP application with AWS Systems Manager for SAP

Important

You must register the SAP HANA database you want to connect to the SAP ABAP application before registering the SAP ABAP application.

Follow along these steps to register either a single node or a multi node (distributed or high availability) SAP ABAP as a Systems Manager for SAP application.

1. Go to https://console.aws.amazon.com/systems-manager/ > **Application Tools** > **Application Manager**.
2. Select **Create Application** > **Enterprise Workload**.
3. For Application type, select **SAP ABAP**.
4. In **Application details**, enter a name for the application you want to register with Application Manager.
5. Provide the following 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 ABAP workload.

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

c. **SAP HANA database Amazon Resource Name (ARN)** – This is the Amazon Resource Name (ARN) of the SAP HANA database you want to connect to your SAP ABAP application.

- Select **Browse databases** to choose the database.
- Select **Register a new application** to register an SAP HANA database to connect to the SAP ABAP application. You can refresh the database list on successful completion of the SAP HANA application.

6. (*Optional*). In **Connected Web Dispatcher components** you can provide the following details of up to 5 of your SAP Web Dispatcher resources that your application is using. SAP Web Dispatcher resources are only discoverable by Systems Manager for SAP after you input these details:

a. **SAP System Identifier (SID)** is the SAP System Identifier (`sapsid`) of your SAP Web Dispatcher resource.

b. **Instance ID** is the Amazon EC2 instance ID on which your SAP Web Dispatcher is currently running. Select **Browse instances** to find the instance ID.

7. (*Optional*). In **Application tags**, you can add 100 tags associated to resources.

8. Select **Create**.

Application tabs

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

Example

Overview

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

Resources

You can find the **Topology** of a 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 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.

   Under **Select an application or resource group**, make sure to select the SAP HANA application registered with Systems Manager for SAP.

   > **Note**
   >
   > You can create only one CloudWatch Application Insights application on a single-node SAP ABAP application. You can onboard either the SAP ABAP application or the connected SAP HANA application.

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.

The cost of the single-node SAP ABAP application is an aggregate of the cost of SAP ABAP and SAP HANA applications on the same EC2 instance.

Start SAP application

Follow along these steps to start Systems Manager for SAP application using AWS Management Console.

1. Go to https://console.aws.amazon.com/systems-manager/ > **Application Tools** > **Application Manager**.
2. From the list of registered applications, choose the application you want to start.
3. Select **Actions** > **Start application**.
4. Select **Start**.

You can monitor the task status using the *operation ID* provided in the flash banner or by selecting **Actions** > **View operations**.

Stop SAP application

Follow along these steps to stop Systems Manager for SAP application using AWS Management Console.

1. Go to https://console.aws.amazon.com/systems-manager/ > **Application Tools** > **Application Manager**.

2. From the list of registered applications, choose the application you want to stop.
3. Select **Actions** > **Stop application**.
   a. When sttopping an SAP HANA application, you can also stop the associated EC2 instance where the SAP HANA application is running.
   b. When stopping an SAP ABAP application, you can also stop the connected SAP HANA application, and/or stop the associated EC2 instance where the SAP ABAP and SAP HANA applications are running.

   > **Note**
   >
   > You can stop the EC2 instance only if you have selected the option to stop the connected SAP HANA application.

4. Select **Stop**.

You can monitor the task status using the *operation ID* provided in the flash banner or by selecting **Actions** > **View operations**.

Run Configuration Checks

Use the following steps to evaluate the SAP configuration of a Systems Manager for SAP application, which is either of type SAP HANA or SAP ABAP.

See also support restrictions for Systems Manager for SAP.

Topics

To access configuration checks

1. Open the AWS Systems Manager console at https://console.aws.amazon.com/systems-manager/
2. In the navigation pane, choose **Application Tools**, then choose **Application Manager**

3. From the list of registered applications, choose the SAP application you want to evaluate
4. Choose **Actions**, then choose **SAP Configuration Checks**

To evaluate configuration checks

1. Select one or more checks you want to evaluate
2. Choose **Run**
3. Monitor the task status using either the operation ID provided in the notification banner or by choosing **Actions** > **View operations**

To view and analyze check results

1. Select a single check to view its details
2. Expand individual subchecks to see detailed rules
3. Sort subchecks by Rule Status, Description, or Component
4. Filter results by rule status using the status totals or the filter box
5. Clear filters by selecting the cancel indicator
6. View previous results by selecting a different evaluation date from the dropdown list
7. Access additional information through the provided Documentation links

Schedule Configuration Checks using AWS EventBridge Scheduler console

1. Sign in to the AWS Management Console, then choose the following link to open the EventBridge Scheduler section of the EventBridge console: https://console.aws.amazon.com/scheduler/home . You can switch your AWS Region by using the AWS Management Console's Region selector.
2. On the **Schedules** page, choose **Create schedule**.
3. On the **Specify schedule detail** page, in the **Schedule name and description** section, do the following:
   a. For **Schedule name**, enter a name for your schedule. For example, `SAPConfigurationChecksSchedule`
   b. For **Description - optional**, enter a description for your schedule.

c. For **Schedule group**, choose a schedule group from the drop down options. If you haven't previously made any schedule groups, you can choose the `default` group for your schedule. To create a new schedule group, choose the **create your own schedule** link in the console description. You use schedule groups to add tags to groups of schedules.

4. In the **Schedule pattern** section, do the following:

   a. For **Occurrence**, choose one of the following pattern options. The configuration options change depending on which pattern that you select.

      i. **One-time schedule** – A one-time schedule invokes a target only once at the date and time that you specify. For **Date and time**, enter a valid date in `YYYY/MM/DD` format. Then, specify a timestamp in 24-hour `hh:mm` format. Finally, choose a timezone from the drop down options.

      ii. **Recurring schedule** – A recurring schedule invokes a target at a rate that you specify using a **cron** expression or rate expression. Choose **Cron-based schedule** to configure a schedule by using a **cron** expression. To use a rate expression, choose **Rate-based schedule** and enter a positive number for **Value**, then choose a **Unit** from the drop down options.

      For more information on using cron and rate expressions, see Schedule types in EventBridge Scheduler.

   b. For **Flexible time window**, choose **Off** to turn off the option, or choose one of the pre-defined time windows from the drop down list. For example, if you choose **15 minutes** and you set a recurring schedule to invoke its target once every hour, the schedule runs within 15 minutes after the start of every hour.

5. If you chose **Recurring schedule** in the previous step, in the **Timeframe** section, specify a timezone, and optionally set a start date and time, and an end date and time for the schedule. A recurring schedule without a start date will begin as soon as it is created and available. A recurring schedules without an end date will continue to invoke it's target indefinitely.

6. Choose **Next**.

7. On the **Select target** page, do the following:

   a. Select **All APIs** option, and Find service "Systems Manager for SAP" from the search box.

   b. Find the **Target** action "StartConfigurationChecks" and provide the json payload based on the StartConfigurationChecks API action (ApplicationId string input, and optionally, ConfigurationCheckIds array string)

8. Choose **Next**, then on the **Settings - optional** page, follow the steps described in EventBridge console Getting Started guide (Step 9 onwards), to change the default settings of the desired schedule.
9. In the Permissions section, in order for the Scheduler to execute the StartConfigurationCheck operation successfully, an IAM role needs to be created with the AWSSystemsManagerForSAPFullAccess managed policy, using the steps below:
   a. In the AWS IAM Console, Create a new role, using a “Custom trust Policy“, and the following trust relationship:

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

   b. On the Next page, Add Permissions by searching for and selecting the AWSSystemsManagerForSAPFullAccess managed policy
   c. Next, provide the Role name and Description, (and tags if any), before creating the role for the scheduler.
   d. Select this new Role in the Permissions section of the schedule on the AWS EventBridge Console, while creating the schedule
10. Choose **Create schedule** to finish creating your new schedule. You can view a list of your new and existing schedules on the **Schedules** page. Under the **Status** column, verify that your new schedule is **Enabled**.
11. To verify that your schedule invokes the Systems Manager for SAP service’s StartConfigurationChecks target, follow the steps listed at the section called “To view and analyze check results”.

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	Supported Versions
Red Hat Enterprise Linux (RHEL)	• 9.6, 9.4, 9.2, 9.0 • 8.10, 8.8, 8.6
SUSE Linux Enterprise Server for SAP Applications (SLES for SAP)	• 15 SP7, 15 SP6, 15 SP5, 15 SP4, 15 SP3 • 12 SP5
SUSE Linux Enterprise Server (SLES)	• 15 SP7, 15 SP6, 15 SP5, 15 SP4, 15 SP3 • 12 SP5

Databases

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

Database	Versions
SAP HANA Scale-Up (single node)	2.0

Database	Versions
SAP HANA Scale-Up (high availability)	2.0

SAP applications

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

Applications	Versions	Supported Database
SAP ABAP Systems (including NetWeaver and S/4HANA) - Single Instance	750 and higher	SAP HANA
SAP ABAP Systems (including NetWeaver and S/4HANA) - Distributed and Highly Available Architectures	750 and higher	SAP HANA

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 Systems Manager for SAP. The following topics show you how to configure 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 Systems Manager for SAP resources.

Topics

- AWS managed policies for AWS Systems Manager for SAP
- Using service linked roles for AWS Systems Manager for SAP
- AWS PrivateLink for AWS Systems Manager for SAP

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 Systems Manager for SAP service.

Permissions details

This policy includes the following permissions.

- `ssm-sap` – Allows principals full access to Systems Manager for SAP.
- `iam` – Allows a service-linked role to be created, which is a requirement for using Systems Manager for SAP.
- `ec2` – Allows Systems Manager for SAP to start or stop an Amazon EC2 instance, if that instance is tagged with the key value pair `SSMForSAPManaged=True`.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AwsSsmForSapPermissions",
            "Effect": "Allow",
            "Action": [
```

```
                "ssm-sap:*"
            ],
            "Resource": "arn:*:ssm-sap:*:*:*"
        },
        {
            "Sid": "AwsSsmForSapServiceRoleCreationPermission",
            "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"
                }
            }
        },
        {
            "Sid": "Ec2StartStopPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "ec2:resourceTag/SSMForSAPManaged": "True"
                }
            }
        }
    ]
}
```

AWS managed policy: AWSSystemsManagerForSAPReadOnlyAccess

Attach the `AWSSystemsManagerForSAPReadOnlyAccess` policy to your IAM identities.

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

Permissions details

This policy includes the following permissions.

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

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

Systems Manager for SAP updates to AWS managed policies

View details about updates to AWS managed policies for 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 Systems Manager for SAP Document history page.

Change	Description	Date
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	The following permissions have been added to the policy for SAP Configuration Checks which validate the IP address used in a Pacemaker HA Setup: • `ec2:DescribeVpcs`	August 1, 2025
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	The following permissions have been added to the policy:	July 8, 2025

Change	Description	Date
	• `ce:ListCostAllocationTags` • `ce:UpdateCostAllocationTagsStatus` • `ce:ListCostAllocationTagBackfillHistory` • `ce:StartCostAllocationTagBackfill`	
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	Removed `TagKeys` and `ArnLike` condition for `awsApplication` tag.	May 23, 2025

Change	Description	Date
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	The following permissions have been added to `DescribeInstanceActions` within this policy: • `ec2:DescribeRouteTables` • `ec2:DescribeInstanceTypes` • `ec2:DescribeVolumes` • `ec2:DescribeInstanceAttribute` • `ec2:DescribeSnapshots` These permissions are required to support new functionality that allows users to run discovery on workloads.	July 8, 2025
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	Activate and backfill cost allocation tags created for SAP applications.	December 20, 2024
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	Updated policy for managing application tags on Amazon EBS volumes.	September 05, 2024

Change	Description	Date
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	Added `ec2:CreateTags` , `ec2:DeleteTags` , `resource-groups:Tag` , and `resource-groups:CreateGroup` actions to the policy. These permissions enable you to create and delete tags on EC2 instances and volumes. These permissions also enable you to create, tag, and delete Systems Manager for SAP resource groups.	August 05, 2024
AWSSystemsManagerForSAPFullAccess – Updated policy	Added `ec2:StartInstances` and `ec2:StopInstances` actions to the policy. These permissions enable you to start or stop an SAP application registered with Systems Manager for SAP.	July 10, 2024
AWSSSMForSAPServiceLinkedRolePolicy – Updated policy	Added `ec2:StartInstances` and `ec2:StopInstances` actions to the policy. These permissions enable you to start or stop an SAP application registered with Systems Manager for SAP.	April 26, 2024

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
AWSSystemsManagerForSAPFullAccess – New policy made available at launch	**AWSSystemsManagerForSAPFullAccess** grants an IAM user account full access to Systems Manager for SAP service.	November 15, 2022

Change	Description	Date
AWSSystemsManagerForSAPReadOnlyAccess – New policy made available at launch	**AWSSystemsManagerForSAPReadOnlyAccess** grants an IAM user account read only access to Systems Manager for SAP service.	November 15, 2022
AWSSSMForSAPServiceLinkedRolePolicy – New policy made available at launch	The **AWSSSMForSAPServiceLinkedRolePolicy** service-linked role policy provides access to Systems Manager for SAP.	November 15, 2022
Systems Manager for SAP started tracking changes	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 Systems Manager for SAP. Service-linked roles are predefined by 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 Systems Manager for SAP easier because you don't have to manually add the necessary permissions. Systems Manager for SAP defines the permissions of its service-linked roles, and unless you make changes to the configuration, only 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 Systems Manager for SAP

Systems Manager for SAP uses the service-linked role named AWSSSMForSAPServiceLinkedRolePolicy 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 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 Systems Manager for SAP metric data to Amazon CloudWatch.
- `ec2` – Allows
  - Description, start and stop of instances
  - Creation, deletion, and description of tags on EC2 instances that are with `SSMForSAPManaged:True`.
  - Creation and deletion of tags on EBS volumes attached to the EC2 instances tagged with `SSMForSAPManaged:True`.
  - Description of VPCs
- `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.
- `ce` - Allows AWS Cost Explorer to list and update cost allocation tags, start cost allocation backfill, and list cost allocation backfill history.

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

- `ssm-sap.amazonaws.com`

To view the update history of this policy, see 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 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 Systems Manager for SAP. Service-linked roles are predefined by 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 Systems Manager for SAP easier because you don't have to manually add the necessary permissions. Systems Manager for SAP defines the permissions of its service-linked roles, and unless you make changes to the configuration, only 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, Systems Manager for SAP automatically creates this service-linked role for you when you resume using Systems Manager for SAP.

Editing a service-linked role for Systems Manager for SAP

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 Systems Manager for SAP console, CLI, or API.

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

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 Systems Manager for SAP.

AWS PrivateLink for AWS Systems Manager for SAP

You can use AWS PrivateLink to establish a private connection between your VPC and AWS Systems Manager for SAP by creating an interface VPC endpoint. With interface endpoints, you can privately access Systems Manager for SAP APIs without needing an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Traffic between your VPC and Systems Manager for SAP stays within the AWS network. Amazon EC2 instances in your VPC don't require public IP addresses to use Systems Manager for SAP APIs.

Create a VPC endpoint for Systems Manager for SAP

Use the following procedure to create a VPC endpoint for AWS Systems Manager for SAP.

To create a VPC endpoint:

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Endpoints**.
3. Choose **Create endpoint**.
4. For **Service category**, choose **AWS services**.
5. For **Service Name**, search for and select `com.amazonaws.[region].ssm-sap`. There should only be 1 entry.

6. For **VPC**, select the VPC where you want to create the endpoint.
7. For **Subnets**, select the subnets (Availability Zones) where you want to create the endpoint network interfaces.
8. For **Security group**, select one or more security groups to associate with the endpoint network interfaces.
   - Ensure the security group allows inbound HTTPS traffic (port 443) from the resources in your VPC that need to communicate with Systems Manager for SAP.
9. (Optional) Under **Policy**, you can keep the default setting **Full access** or customize the policy to restrict access.
10. Choose **Create endpoint**.

Note - VPC endpoints for AWS Systems Manager for SAP are dual-stack by default, supporting both IPv4 and IPv6 communication.

Creating FIPS-compliant VPC endpoints

For customers who need to meet FIPS (Federal Information Processing Standard) compliance requirements, Systems Manager for SAP offers FIPS-compliant endpoints.

To create a FIPS-capable VPC endpoint:

1. Follow steps 1-4 from the standard VPC endpoint creation process above.
2. For **Service Name**, search for and select `com.amazonaws.[region].ssm-sap-fips`.
3. Continue with the remaining standard process steps.

> **Note**
>
> FIPS endpoints are available only in specific AWS regions. Consult the Systems Manager for SAP documentation or AWS regional services list for availability information.

Verify the endpoint connection

After creating the endpoint, verify its status:

1. In the VPC console, choose **Endpoints**.

2. Look for your newly created endpoint and check that its **Status** is **Available**.
3. Note the **Endpoint ID** for reference in case you need to troubleshoot connectivity issues.

Important Notes About Service Dependencies

When using Systems Manager for SAP with VPC endpoints, be aware that you are responsible for creating VPC endpoints for other AWS services that Systems Manager for SAP depends on, such as:

- ssm
- ssm-messages
- ec2-messages

For more information on how to setup these endpoints, refer to the guide at AWS Systems Manager VPC endpoints.

If these dependent service endpoints are not configured, or if your VPC doesn't have internet access through an internet gateway or NAT gateway, operations involving these services will fail. Review your security group and network ACL configurations to ensure they allow traffic to these dependent service endpoints.

Considerations

- VPC endpoint policies support all Systems Manager for SAP API operations
- AWS PrivateLink charges apply when using interface VPC endpoints. For more information, refer to Pricing in the AWS PrivateLink guide
- For information about endpoint quotas, see AWS PrivateLink quotas

Additional Resources

- For more information about enabling Systems Manager for SAP service dependency on VPC endpoints, see AWS Systems Manager VPC endpoints
- For more information about AWS PrivateLink and VPC endpoints, see AWS PrivateLink Guide

Monitoring Systems Manager for SAP

AWS Systems Manager for SAP works with other AWS tools to enable you to monitor SAP 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.

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	`{`

Event state	JSON payload

	"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
	}
	}

Event state	JSON payload

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": {
	"operationId": "e5de5599-3b1e-4892-9201-835e71c6090a",
	"type": "REGISTER_APPLICATION",
	"applicationId": "HANA_TEST",
	"resourceId": "HDB",
	"resourceType": "APPLICATION",
	"status": "Success",
	"statusMessage": null
	}
	}

Event state	JSON payload

SSM for SAP Operation: Error	{
	"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
	}
	}

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.

Example

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 using 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. CloudTrail captures API calls for AWS Systems Manager for SAP as events. The calls captured include calls from the AWS Management Console and code calls to the AWS Systems Manager for SAP API operations. 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, when it was made, and additional details.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root user or user credentials.
- Whether the request was made on behalf of an IAM Identity Center user.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

CloudTrail is active in your AWS account when you create the account and you automatically have access to the CloudTrail **Event history**. The CloudTrail **Event history** provides a viewable, searchable, downloadable, and immutable record of the past 90 days of recorded management events in an AWS Region. For more information, see Working with CloudTrail Event history in the *AWS CloudTrail User Guide*. There are no CloudTrail charges for viewing the **Event history**.

For an ongoing record of events in your AWS account past 90 days, create a trail or a CloudTrail Lake event data store.

CloudTrail trails

A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. All trails created using the AWS Management Console are multi-Region. You can create a single-Region or a multi-Region trail by using the AWS CLI. Creating a multi-Region trail is recommended because you capture activity in all AWS Regions in your account. If you create a single-Region trail, you can view only the events

logged in the trail's AWS Region. For more information about trails, see Creating a trail for your AWS account and Creating a trail for an organization in the *AWS CloudTrail User Guide*.

You can deliver one copy of your ongoing management events to your Amazon S3 bucket at no charge from CloudTrail by creating a trail, however, there are Amazon S3 storage charges. For more information about CloudTrail pricing, see AWS CloudTrail Pricing. For information about Amazon S3 pricing, see Amazon S3 Pricing.

CloudTrail Lake event data stores

CloudTrail Lake lets you run SQL-based queries on your events. CloudTrail Lake converts existing events in row-based JSON format to Apache ORC format. ORC is a columnar storage format that is optimized for fast retrieval of data. Events are aggregated into *event data stores*, which are immutable collections of events based on criteria that you select by applying advanced event selectors. The selectors that you apply to an event data store control which events persist and are available for you to query. For more information about CloudTrail Lake, see Working with AWS CloudTrail Lake in the *AWS CloudTrail User Guide*.

CloudTrail Lake event data stores and queries incur costs. When you create an event data store, you choose the pricing option you want to use for the event data store. The pricing option determines the cost for ingesting and storing events, and the default and maximum retention period for the event data store. For more information about CloudTrail pricing, see AWS CloudTrail Pricing.

For information about CloudTrail record contents, see CloudTrail record contents in 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 Systems Manager for SAP, see Systems Manager for SAP service quotas.

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

- ListSubcheckRuleResults SubCheck Result ValidationException
- ListSubcheckRuleResults - Unknown Rules

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 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 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 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 <ApplicationId> --database-arn
 <DatabaseArn>
```

Unsupported setup

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

Resolution – 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 Systems Manager for SAP. For more information, see Register your SAP ABAP application with 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 – 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>
```

StartApplication AccessDeniedException

Problem – `An error occurred (AccessDeniedException) when calling the StartApplication operation: User: arn:aws:sts::<account_id> :assumed-role/<role_name> is not authorized to perform: ssm-sap:StartApplication on resource: arn:aws:ssm-sap:<region>: <account_id>:HANA/<hana_application_id>`

Possible cause – When the `StartApplication` operation is performed on an SAP ABAP application and the procedure includes starting its connected HANA application, you must have the necessary IAM permissions to run `ssm-sap:StartApplication` on the connected application. Without those permissions, the error message will occur.

Resolution – Add the permission `ssm-sap:StartApplication` against the HANA application to the role of the user calling `StartApplication`.

StartApplication ConflictException

Problem – `Start Application can not be run on an already running application. Run ssm-sap start-application-refresh --application-id <ApplicationId> to ensure that the ssm-sap status reflects the current application state.`

Possible cause – The application you attempted to start is already running.

Resolution – Refresh SAP application to ensure the `ssm-sap` status reflects the current application state.

StartApplication ValidationException

Problem – `An error occurred (ValidationException) when calling the StartApplication operation: Caller lacks permissions to start Amazon EC2 instances`

Possible cause – When the `StartApplication` operation includes starting the Amazon EC2 instances running the SAP application, you must have the necessary IAM permissions to run

`ec2:StartInstances` on the corresponding Amazon EC2 instances. Without those permissions, the error message will occur.

Resolution – Add the permission `ec2:StartInstances` permission against the Amazon EC2 hosts of the SAP application to the role of the user calling `StartApplication`.

StopApplication AccessDeniedException

Problem – `An error occurred (AccessDeniedException) when calling the StopApplication operation: User: arn:aws:sts::<account_id>:assumed-role/<role_name> is not authorized to perform: ssm-sap:StopApplication on resource:arn:aws:ssm-sap:<region>:<account_id>:HANA/<hana_application_id>`

Possible cause – When the `StopApplication` operation is performed on an SAP ABAP application and the procedure includes starting its connected HANA application, you must have the necessary IAM permissions to run `ssm-sap:StopApplication` on the connected application. Without those permissions, the error message will occur.

Resolution – Add the permission `ssm-sap:StopApplication` against the HANA application to the role of the user calling `StopApplication`.

StopApplication ConflictException

Problem – `An error occurred (ConflictException) when calling the StopApplication operation: The specified component is already stopped.` or `An error occurred (ConflictException) when calling the StopApplication operation: The specified component is not in a state that can be started or stopped.`

Possible cause – If your application status or status of the components are stale, the StopApplication operation can result in these or similar `ConflictExceptions`.

Resolution –

1. Refresh SAP application.
2. Then, retry Stop SAP application.

Possible cause – If the `SSMForSAPManaged:True` tag has not been applied to the EC2 instance.

Resolution – Apply the `SSMForSAPManaged:True` tag to the EC2 instance.

StopApplication ValidationException

Problem – `An error occurred (ValidationException) when calling the StopApplication operation: Caller lacks permissions to stop Amazon EC2 instances`

Possible cause – When the `StopApplication` operation includes stopping the Amazon EC2 instances running the SAP application, you must have the necessary IAM permissions to run `ec2:StopInstances` on the corresponding EC2 instances. Without those permissions, the error message will occur.

Resolution – Add the permission `ec2:StopInstances` permission against the Amazon EC2 hosts of the SAP application to the role of the user calling `StopApplication`.

Unsupported `sslenforce` setup

Problem – `HANA error code: 4321. HANA error message: connection failed: only secure connections are allowed`

Resolution – Set `sslenforce` to flase in the `global.ini` file.

StartConfigurationChecks AccessDeniedException

Problem – `An error occurred (AccessDeniedException) when calling the StartConfigurationChecks operation: User: arn:aws:sts::<account_id>:assumed-role/<role_name> is not authorized to perform: ssm-sap:StartConfigurationChecks on resource: arn:aws:ssm-sap:<region>:<account_id>:HANA/<hana_application_id>`

Possible cause – When the StartConfigurationChecks operation is performed, you must have the necessary IAM permissions to execute configuration checks on the application.

Resolution – Add the permission `ssm-sap:StartConfigurationChecks` against the application to the role of the user calling `StartConfigurationChecks`.

Component Status ValidationException

Problem – `An error occurred (ValidationException): "<applicationId> has <componentIds> component(s) not RUNNING. Start all components to run Configuration Checks."`

Possible cause – All components must be in RUNNING state before starting configuration checks. The checks cannot proceed if any component is stopped, failed, or still starting up.

Resolution – Start all non-running components and wait for them to reach RUNNING state before retrying configuration checks.

Single Node Compatibility ValidationException

Problem – `An error occurred (ValidationException): "Application <applicationId> has 1 running HANA_NODE Component. The Configuration Check 'SAP_CHECK_03' is not applicable for Single Node HANA applications."`

Possible cause – SAP_CHECK_03 is being executed on a single-node HANA deployment, but this check is only applicable for HA deployments.

Resolution – Remove SAP_CHECK_03 from configuration checks for single-node deployments. Use only SAP_CHECK_01 and SAP_CHECK_02.

Check Type Compatibility ValidationException

Problem – `An error occurred (ValidationException): "The Configuration Check(s) '<checkIds>' are not applicable for the <applicationType> application <applicationId>"`

Possible cause – The requested configuration checks are not compatible with the application type.

Resolution – Use only supported configuration checks:

- For a list of supported configuration checks, use the ListConfigurationCheckDefinitions API
- You can use this API to get details about which checks are available for your specific deployment type

Concurrent Checks ValidationException

Problem – `An error occurred (ValidationException): "Unable to start new configuration checks for <applicationId>. The following checks are currently in progress: <checkIds>"`

Possible cause – Configuration checks of the same type are already running for this application.

Resolution – Wait for currently running checks to complete before starting new ones.

ListConfigurationCheckOperations ResourceNotFoundException

Problem – `An error occurred (ResourceNotFoundException): "Application <applicationId> doesn’t exist."`

Possible cause – The specified application ID cannot be found in the application store for the given account ID.

Resolution – Verify the application ID is correct and properly registered in your AWS account.

ListSubcheckResults Operation ValidationException

Problem – `An error occurred (ValidationException): "Operation Not Found: <operationId>"`

Possible cause – The specified operation ID is invalid or no longer exists in the system.

Resolution – Verify the operation ID is correct and still active.

ListSubcheckRuleResults SubCheck Result ValidationException

Problem – `An error occurred (ValidationException): "SubCheckResult Not Found: <subCheckResultId>"`

Possible cause – The specified subcheck result ID cannot be found in the system.

Resolution – Verify the subcheck result ID is correct and associated with the specified operation.

ListSubcheckRuleResults - Unknown Rules

Problem – Unknown rules are encountered during configuration checks.

Possible cause – This occurs when there is a mismatch between your environment's configuration and the supported rule definitions in Systems Manager for SAP.

Resolution – Contact AWS Support with the operation ID, timestamp, AWS Region, and rule name. AWS Support will investigate the configuration mismatch and provide guidance for your environment.

Document history of Systems Manager for SAP User Guide

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

Change	Description	Date
Policy update	Updated AWSSSMFor SAPServiceLinkedRolePolicy.	August 1, 2025
Minor Changes	Systems Manager for SAP now supports SLES for SAP 15 SP6. Other minor documentation corrections.	July 24, 2025
Policy update	Updated AWSSSMFor SAPServiceLinkedRolePolicy.	July 8, 2025
Policy update	Updated AWSSSMFor SAPServiceLinkedRolePolicy.	May 23, 2025
Supported version update	Systems Manager for SAP now offers support of SAP NetWeaver of SAP ABAP single node and multi mode for versions 750 and later. For more information, see Supported versions.	December 20, 2024
Policy update	Updated AWSSSMFor SAPServiceLinkedRolePolicy.	December 20, 2024
Policy update	Updated AWSSSMFor SAPServiceLinkedRolePolicy.	September 5, 2024
New feature	Start and stop Systems Manager for SAP applicati	August 22, 2024

	on using AWS Management Console.	
New feature	Register SAP ABAP application with Systems Manager for SAP.	August 22, 2024
Policy update	Updated AWSSSMForSAPServiceLinkedRolePolicy.	August 5, 2024
Policy update	Updated the AWSSystemsManagerForSAPFullAccess policy.	July 10, 2024
Support update	Systems Manager for SAP now supports Red Hat Enterprise Linux versions 9.0 and 9.2.	May 10, 2024
Policy update	Updated AWSSSMForSAPServiceLinkedRolePolicy.	May 10, 2024
New feature	Users can now stop and start SAP HANA applications and single node SAP ABAP applications.	May 10, 2024
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 Systems Manager for SAP.	October 31, 2023
Policy update	Updated the AWSSSMForSAPServiceLinkedRolePolicy policy.	July 26, 2023
New feature	Register SAP HANA database with 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