AWS Blueprints

Implementation Guide

April 2021

Content

About this guide

This implementation guide discusses the steps and the solution components involved in deploying the Amazon Web Services (AWS) Blueprints. AWS Blueprints provides pre-configured solutions that are deployed into a secure and multi-account structure to accelerate and transform their cloud adoption. It includes links to an AWS CloudFormation template that launches and configures the AWS services required to deploy this solution using the AWS best practices for security and availability.

The guide is intended for AWS Distributors, AWS Solution Providers, and technical teams, such as IT infrastructure architects, administrators, and DevOps professionals who have practical experience architecting in the AWS Cloud. To deploy, customize, and extend AWS Blueprints, we recommend having a fundamental understanding of core AWS technologies including Amazon Virtual Private Cloud (Amazon VPC), Amazon Elastic Compute Cloud (Amazon EC2), AWS CloudFormation, AWS Service Catalog, AWS Identity and Access Management (IAM), security groups, network access control lists, subnetting and routing, and multi-account structures.

Overview

AWS Blueprints consists of portfolios of tested and validated AWS services and third-party applications that AWS Distributors (which include managed service providers (MSPs) and value-added resellers (VARs)) and AWS Solution Providers can use to deploy, manage, and monitor solutions for their small and medium business (SMB) customers in the AWS Cloud. As shown in Figure 1, this solution deploys repeatable, scalable portfolios using AWS Service Catalog, which includes a mix of AWS services and third-party applications. Additionally, AWS Distributors and AWS Solution Providers can extend this solution by integrating their own value-added capabilities.

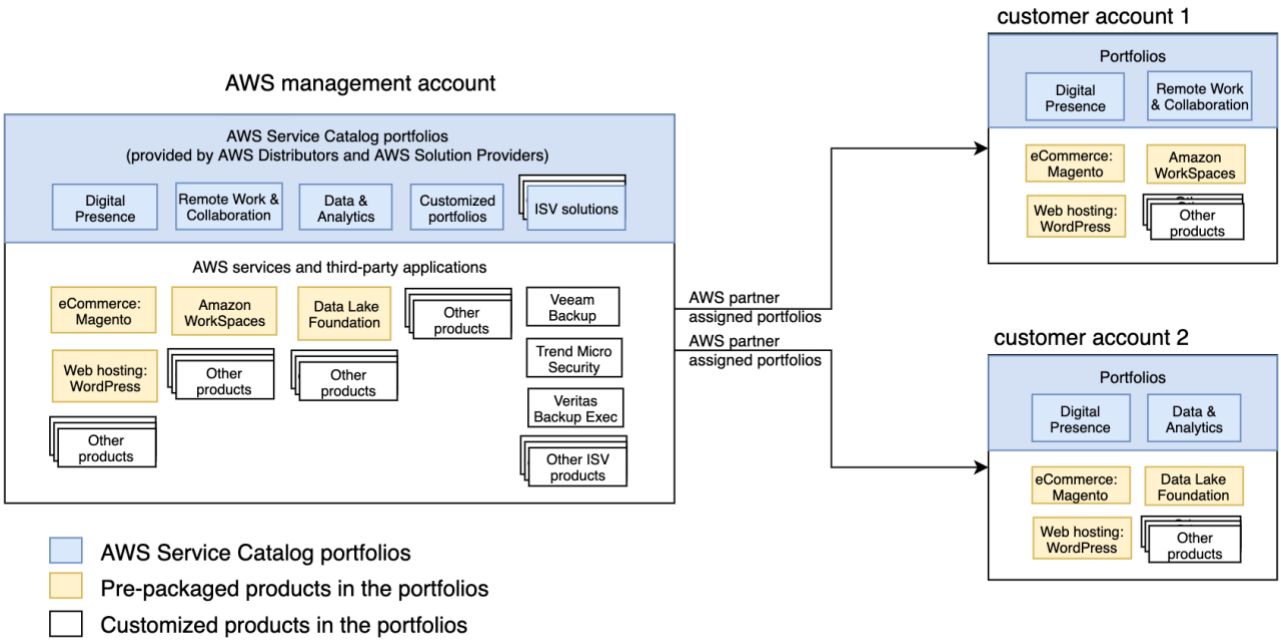

Figure 1: AWS Blueprints reference framework

This solution offers the following features:

- **Customizable and extensible pre-packaged portfolios:** As shown in Figure 1, AWS Distributors and AWS Solution Providers can use this solution as a reference implementation to customize the catalog of services that will meet the unique demands of SMB customers. AWS Distributors and AWS Solution Providers can develop and add their own products to the portfolio and also add products directly from AWS Marketplace. This solution deploys AWS services and applications organized into portfolios, including Digital Presence, Data & Analytics, and Remote Work & Collaboration.

Additionally, Independent Software Vendor (ISV) products from AWS Marketplace can be created in custom portfolios. Three examples are shown in Figure 1, including Veeam Backup for AWS Free Edition, Veritas Backup Exec™ for AWS, and Trend Micro Deep Security.

- **SMB focused solutions:** This solution deploys AWS services and third-party applications using AWS Service Catalog that are SMB-focused.
- **Automated solution deployment:** AWS Distributors and AWS Solution Providers can deploy multiple configurations of the AWS services and third-party applications in the AWS Service Catalog portfolio using an automated process. The portfolio can be shared across AWS accounts or within AWS Organizations for a customer account.

Additionally, this solution offers flexible deployment and delivery models to AWS Distributors and AWS Solution Providers when deploying to customer-managed AWS accounts. For information about these flexible models, refer to the Deployment models and Delivery model sections in this guide.

Cost

You are responsible for the cost of the AWS services used while running this solution. As of April 2021, there is **no cost** for running this solution with the default settings in the US East (N. Virginia) Region and with the number of API calls made by your AWS account to AWS Service Catalog kept to 1,000 or less, including the free tier. Refer to the AWS Service Catalog pricing page for additional information.

Note that we highly recommend using AWS Control Tower to support the deployment of this solution. As of April 2021, the cost for running this solution with AWS Control Tower and default settings in the US East (N. Virginia) AWS Region is approximately **$3.75 to $60.625 per month**. This range in cost is due to the variable configuration parameters, which you customize to fit your specifications and requirements. Refer to the AWS Control Tower pricing page for pricing information to set up AWS Control Tower and the different usage profiles available to you. For information to deploy AWS Control Tower, refer to Deploying with AWS Control Tower in the Implementation consideration section.

Costs for AWS services are applied when you deploy either the pre-packaged portfolios or your customized portfolios in AWS Service Catalog to your customers. Note that each AWS service in the portfolios has its own cost, which varies depending on the service and the number of customers in the deployment. To calculate the cost to deploy a portfolio containing AWS services, refer to the pricing page for each AWS service that is part of the deployment.

Refer to the following AWS pricing pages for the services included in the pre-packaged portfolios:

- Digital Presence: Magento, WordPress

- Data & Analytics: Data Lake Foundation on AWS (refer to the **Cost and licenses** tab for information).
- Remote Work & Collaboration: Simple Active Directory (AD), Amazon WorkSpaces

Refer to the following use cases for example costs for deploying AWS services in portfolios.

> **Note:** After deploying this solution, activate the AWS Cost and Usage Report to deliver billing metrics to an Amazon Simple Storage Service (Amazon S3) bucket in your account. This report provides cost estimates based on usage throughout each month and aggregates the data at the end of the month.
>
> Note that this report is always activated for distribution accounts. The distributor activates and configures this report before a distribution seller can access the account. Additionally, the distribution seller usually does not have access to this report.
>
> For more information about the report, refer to What are AWS Cost and Usage Reports in the *Cost and Usage Report User Guide*.

You are responsible for the cost of the AWS services and any third-party licenses used while running Quick Start reference deployments. There is no additional cost for using a Quick Start.

Prices are subject to change. For cost estimates related to third-party applications included with this solution, refer to the Software licenses section.

Use case example: deploy the Remote Work & Collaboration portfolio

The end-user computing portfolio includes Amazon WorkSpaces and Simple Active Directory.

For Amazon WorkSpaces pricing information, refer to the Amazon WorkSpaces pricing page.

For Simple AD costs, refer to the following table, which provides an example of monthly cost for deploying this service. You do not incur any charges for the first 30 days for Simple AD.

Table 1: Cost for Simple AD

AWS service	Dimensions	Cost per month
Simple Active Directory	Small directory (after 30 days or 1,500 free-trial hours)	$36.00

The cost for Simple AD breaks down as follows:

- 24 hours x 30 days = 720 hours per domain controller
- 2 domain controllers per managed directory (required setup)
- 720 hours x 2 total domain controllers = 1,440 total domain controller hours
- 1,440 billable hours * $0.025 per domain controller hour = $36.00 / month

> **Note:** Your AWS bill for Simple AD does not break down costs by individual domain controllers. Your bill shows a single line item for Simple AD for $36.00.

Use case example #2: cost impacts when adding ISV and/or AWS Marketplace products

ISV and AWS Marketplace product costs are not included in the cost estimate for this solution. If you choose to create products from ISVs and/or AWS Marketplace, you need to factor in these costs. For example:

- Backup and Recovery products: Veeam Backup for AWS Free Edition, Veritas Backup Exec™ for AWS
- Security products: Trend Micro Deep Security

Software licenses

AWS Blueprints includes third-party applications in the Digital Presence AWS Service Catalog portfolio, including:

- Magento
- Word Press

When deploying AWS Blueprints, there are no license costs for the applications in the portfolios. Note that if a product has licensing costs, those costs are incurred when the solution is either deployed or launched to an account. For additional information regarding usage of these applications, refer to the respective third-party pricing pages.

> **Note:** AWS Distributors and AWS Solution Providers are responsible for developing the operational policies for their SMB customers. Additionally, AWS Distributors, AWS Solution Providers, and SMB customers are responsible for the maintenance, patching, and security updates of third-party applications deployed in the AWS Cloud as part of the Shared Responsibility Model. We recommend using AWS Systems Manager to manage your AWS infrastructure.

For cost estimates related to third party software that you add to this solution, refer to the pricing pages for each third-party vendor that you use. If you are consuming products from AWS Marketplace, you need to factor in the cost impacts of the products that you are adding to this solution. For example:

- Veeam Backup for AWS Free Edition
- Veritas Backup Exec™ for AWS
- Trend Micro Deep Security

Architecture overview

Deploying this solution with the default parameters builds the following environment in the AWS Cloud.

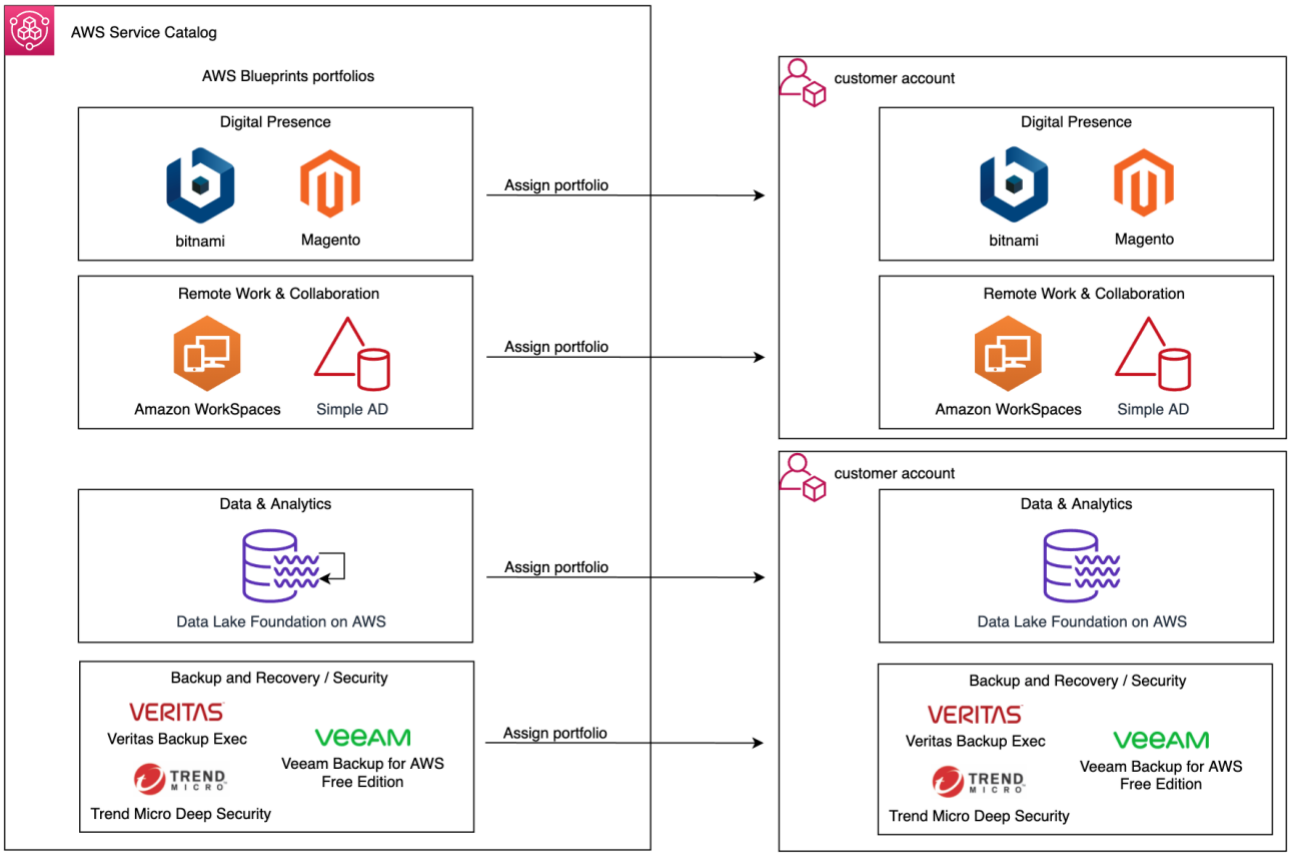

Figure 2: AWS Blueprints architecture on AWS

The AWS CloudFormation template deploys AWS Service Catalog and pre-packaged portfolios in your AWS management account. AWS Service Catalog allows you to package

AWS services and third-party applications into portfolios, which can then be managed and deployed to your customers.

AWS Service Catalog is deployed with the following portfolios:

- Digital Presence, which includes Magento and WordPress.
- Data & Analytics, which includes Data Lake Foundation on AWS.
- Remote Work & Collaboration, which includes: Simple Active Directory (AD) and Amazon WorkSpaces

Independent Software Vendor (ISV) products from AWS Marketplace can be created in custom portfolios. For example:

- Backup and Recovery portfolio, with products such as: Veeam Backup for AWS Free Edition and Veritas Backup Exec™ for AWS.
- Security portfolio, with products such as: Trend Micro Deep Security.

Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This Shared Responsibility Model helps reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. For more information about security on AWS, visit AWS Cloud Security.

IAM users and roles

The AWS Identity and Access Management (IAM) users and roles created in this solution are designed as a starting point to provide full administrative access into the environment. **It is not recommended that these IAM users and roles are used in an operational or production environment**. We recommend you develop and deploy IAM roles as applicable for your mission needs.

Security groups

The security groups created in this solution are designed to control and isolate network traffic between the applications deployed into the AWS accounts, and also with external users and clients. We recommend that you review the security groups and further restrict access as needed once the deployment is up and running.

AWS Key Management Service customer master keys (CMKs)

AWS Key Management Service (AWS KMS) customer master keys (CMKs) can be configured to encrypt resources such as Amazon S3 buckets and AWS CloudTrail trails. The keys are also used for other data-at-rest encryption needs, such as the encryption of Amazon Elastic Block Store volumes. Rotation of these CMKs is the responsibility of the customer. For more information, refer to AWS KMS concepts in the *AWS KMS Developer Guide*.

Security for AWS Blueprints deployment options

AWS Control Tower

If you deploy this solution using AWS Control Tower, refer to Security in AWS Control Tower in the *AWS Control Tower User Guide* to help you understand how to apply the shared responsibility model when using this AWS service. For deployment guidance, refer to Deploying with AWS Control Tower in the Implementation considerations section of this guide.

AWS Organizations

If you deploy this solution using AWS Organizations, refer to Security in AWS Organizations in the *AWS Organizations User Guide* to help you understand how to apply the shared responsibility model when using this AWS service. For deployment guidance, refer to Deploying with AWS Organizations in the Implementation considerations section of this guide.

> **Important:** AWS Distributors and AWS Solution Providers are responsible for providing the operational policies for their SMB customers and all users are responsible for ensuring that third-party applications are properly patched and secured in their AWS account. For additional information, refer to the AWS Systems Manager section of this guide.

Implementation considerations

Deployment options

Prior to deploying AWS Blueprints, you need to choose a method to centralize the management of the AWS Service Catalog portfolios provided by this solution. You can use either AWS Control Tower or AWS Organizations for the management capabilities.

(Recommended) Deploying with AWS Control Tower

AWS highly recommends that you set up AWS Control Tower in your AWS management account before deploying AWS Blueprints. AWS Control Tower can be leveraged as the centralized foundation for account management, account security and manage customer accounts at scale. AWS Control Tower with AWS Service Catalog provides the following capabilities and features for AWS Blueprints:

- A well-architected landing zone, a multi-account structure using AWS Organizations that incorporates best practices for security and compliance.
- Provisioning and account management using Account Factory containing the appropriate user group permissions; provisioners can specify standardized baselines and network configurations for all accounts in your organization.
- Identity management using AWS Single Sign-On (AWS SSO) default directory.
- Federated access to accounts using AWS SSO.
- Centralized logging from AWS CloudTrail, and AWS Config stored in Amazon Simple Storage Service (Amazon S3)
- Cross-account security audits using AWS IAM and AWS SSO.
- A solutions implementation, Customizations for AWS Control Tower, that combines AWS Control Tower and other highly-available, trusted AWS services to help customers set up a secure, multi-account AWS environment using AWS best practices.
- Standardization for the administration and management of approved templates, standardized across the organization.
- Self-service for locating the products they are authorized to use.
- Fine grain access control – portfolio access managed by IAM.
- Extensibility and version control - updating a product to a new version propagates the update to all products in every portfolio that references it.

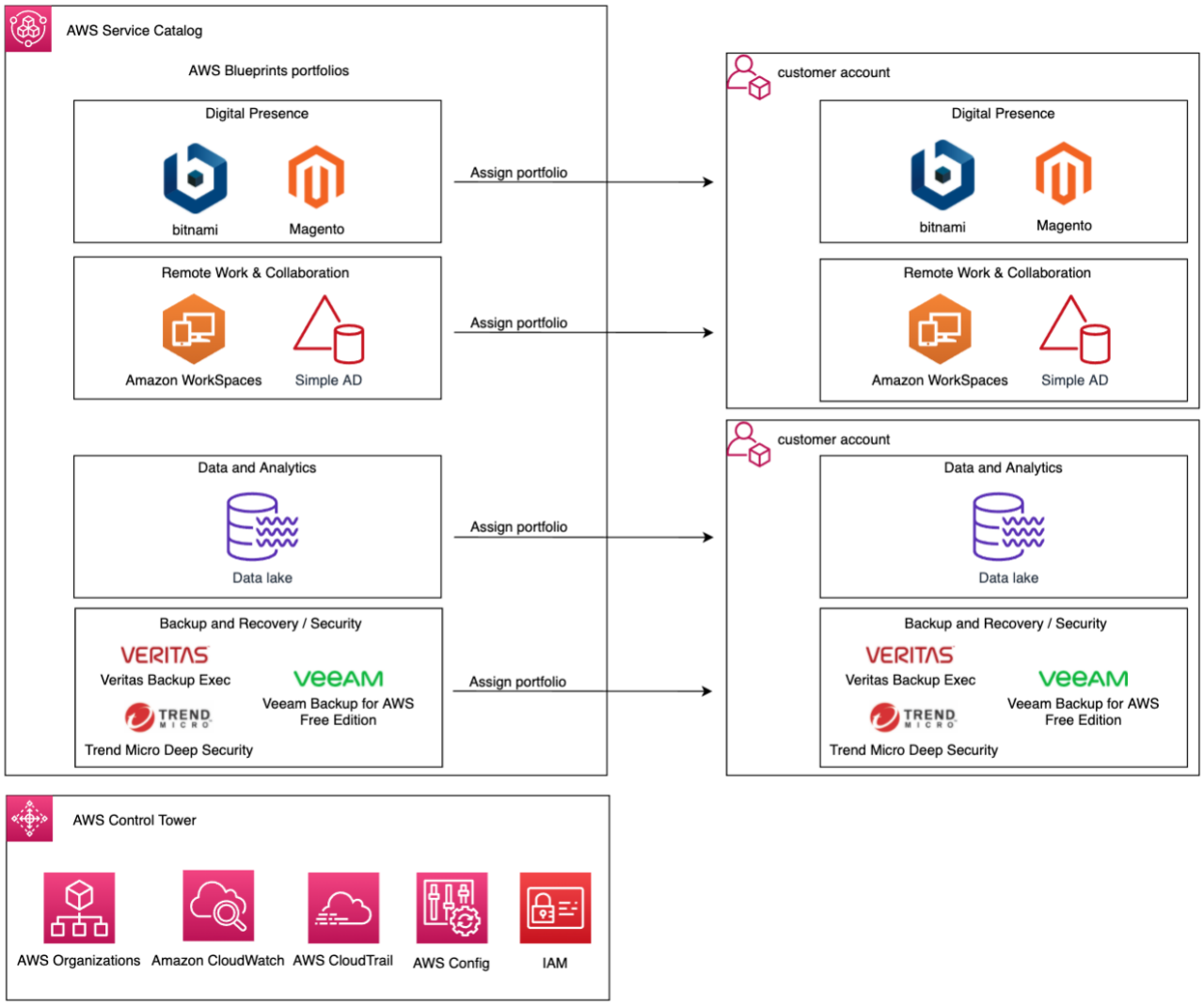

Figure 3: AWS Blueprints architecture using AWS Control Tower

If you are deploying in an AWS Control Tower account, you need IAM administrator access to the AWS management account.

If you do not have AWS Control Tower deployed in your AWS management account, refer to Getting Started with AWS Control Tower in the *AWS Control Tower User Guide*.

When setting up AWS Control Tower, deploy the following resources:

- Two organizational units (OUs), one for your shared accounts and one for accounts that will be provisioned by your customers.
- Three shared accounts, which are the management account and isolated accounts for archive logging and security audits.
- A native cloud directory with preconfigured groups and single sign-on (SSO) access.

- 20 preventive guardrails to enforce policies and two detective guardrails to detect configuration violations.

> **NOTE:** AWS Control Tower is not currently available in all AWS Regions. Therefore, if you use this service, you must launch this solution in an AWS Region where AWS Control Tower is available. For the most current availability by Region, refer to the AWS Regional Services List.

(Optional) Deploying with AWS Organizations

If you decide not to use AWS Control Tower, your alternative is to use AWS Organizations. You can use your existing AWS Organizations account to deploy AWS Blueprints. When using AWS Organizations, you need to provision and manage the account creation process using security policies, including enabling AWS CloudTrail, service control policies, IAM, and network baselines, such as an Amazon VPC and subnets before deploying the template.

AWS Organizations with AWS Service Catalog provides the following capabilities and features for AWS Blueprints:

- Standardization for the administration and management of approved templates, standardized across the organization.
- Self-service for locating the products they are authorized to use.
- Fine grain access control – portfolio access managed by IAM.
- Extensibility and version control – updating a product to a new version propagates the update to all products in every portfolio that references it.

If you do not have AWS Organizations set up in your AWS management account, refer to Getting Started with AWS Organizations in the *AWS Organizations User Guide*.

AWS CloudFormation Template

This solution uses AWS CloudFormation to automate the deployment of the AWS Blueprints solution in the AWS Cloud. It includes the following CloudFormation template, which you can download before deployment:

View template

aws-blueprints.template: Use this template to launch the solution and all associated components. The default configuration deploys AWS Service Catalog and a set of prepackaged portfolios that contains a mix of AWS services and resources including Amazon WorkSpaces, Simple Active Directory, and Data Lakes Foundation on AWS Quick Start. You can also customize the template based on your specific needs.

Automated Deployment

Before you launch the automated deployment, review the cost, architecture, security, and other considerations discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy into your account.

Time to deploy: Approximately 10 minutes.

Prerequisites

Before you can deploy this solution, AWS highly recommend that you have AWS Control Tower set up in your AWS management account. Additionally, your AWS management account must have IAM administrator privileges. AWS Blueprints must be deployed from one of these AWS services.

If you use AWS Control Tower, ensure that a multi-account structure is set up. You can use your existing set up to deploy AWS Blueprints.

> **Note:** Optionally, you can have AWS Organizations set up in your AWS management account before deploying this solution.

For information about your deployment options, refer to Deployment options in the Implementation considerations section of this guide.

Deployment Overview

Use the following steps to deploy this solution on AWS. For detailed instructions, follow the links for each step.

Step 1. Launch the stack

- Launch the AWS CloudFormation template into your AWS account.
- Enter the required parameters: **Distributor** and **Owner**.
- Review the other template parameters, and adjust if necessary.

Step 2. Share your AWS Service Catalog portfolios

Step 3. Launch the AWS Service Catalog portfolio of products

(Optional) Add products to the AWS Service Catalog portfolio

Step 1. Launch the stack

This automated AWS CloudFormation template deploys AWS Blueprints.

Note: You are responsible for the cost of the AWS services used while running this solution. For more details, visit the Cost section in this guide, and refer to the pricing webpage for each AWS service used in this solution.

1. Sign in to the AWS Management Console and select the button to launch the `aws-blueprints` AWS CloudFormation template. Alternatively, you can download the template as a starting point for your own implementation.

2. The template launches in the US East (N. Virginia) Region by default. To launch the solution in a different AWS Region, use the Region selector in the console navigation bar.
3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box and choose **Next**.
4. On the **Specify stack details** page, assign a name to your solution stack. For information about naming character limitations, refer to IAM and STS Limits in the *AWS Identity and Access Management User Guide*.
5. Under **Parameters**, review the parameters for this solution template and modify them as necessary. This solution uses the following default values.

Parameter	Default	Description
Distributor	<Optional input>	Specify a name that identifies either the AWS Solution Provider or the AWS Distributor responsible for sharing AWS Service Catalog portfolios in customer accounts.
Owner	*<Requires input>*	Specify a name that identifies the group or organization that supports the products in the AWS Service Catalog portfolios. This may be the same name as the **Distributor**. For example, IT or an AWS partner maybe entered.
SupportDescription	<Optional input>	Enter a description of the AWS Distributors or AWS Support Partners supporting this solution.
SupportEmail	<Optional input>	Enter the email address for the person or group that is supporting the AWS services and third-party applications deployed in the AWS Service Catalog portfolios. For example, this email address can be for the administrators representing the AWS Distributors or AWS Solution Providers or the account team for AWS Service Catalog.
SupportUrl	<Optional input>	Enter the website that customers can access to contact your support team, helpdesk, or ticketing system.

6. Choose **Next**.
7. On the **Configure stack options** page, choose **Next**.
8. On the **Review** page, review and confirm the settings. Check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.

9. Choose **Create stack** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation Console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately 10 minutes.

> **Note:** In addition to the primary AWS Lambda functions, this solution includes the `solution-helper` Lambda function, which runs only during initial configuration or when resources are updated or deleted.
>
> When you run this solution, you will notice all Lambda functions in the AWS console but `solution-helper` will not be active unless you are creating, updating, or deleting the solution's stack. You must not delete the `solution-helper` function, as it is necessary to manage associated resources.

Step 2. Share your AWS Service Catalog portfolios

Once the AWS Service Catalog portfolios are deployed into your management account, they can be shared and assigned to your customers. Use the following steps to share your AWS Service Catalog portfolios with your customers.

1. Navigate to AWS Service Catalog and in the left menu pane, select **Portfolios**.
2. In the Portfolios page, select a portfolio (**Digital Presence, Remote Work & Collaboration, Data & Analytics**).

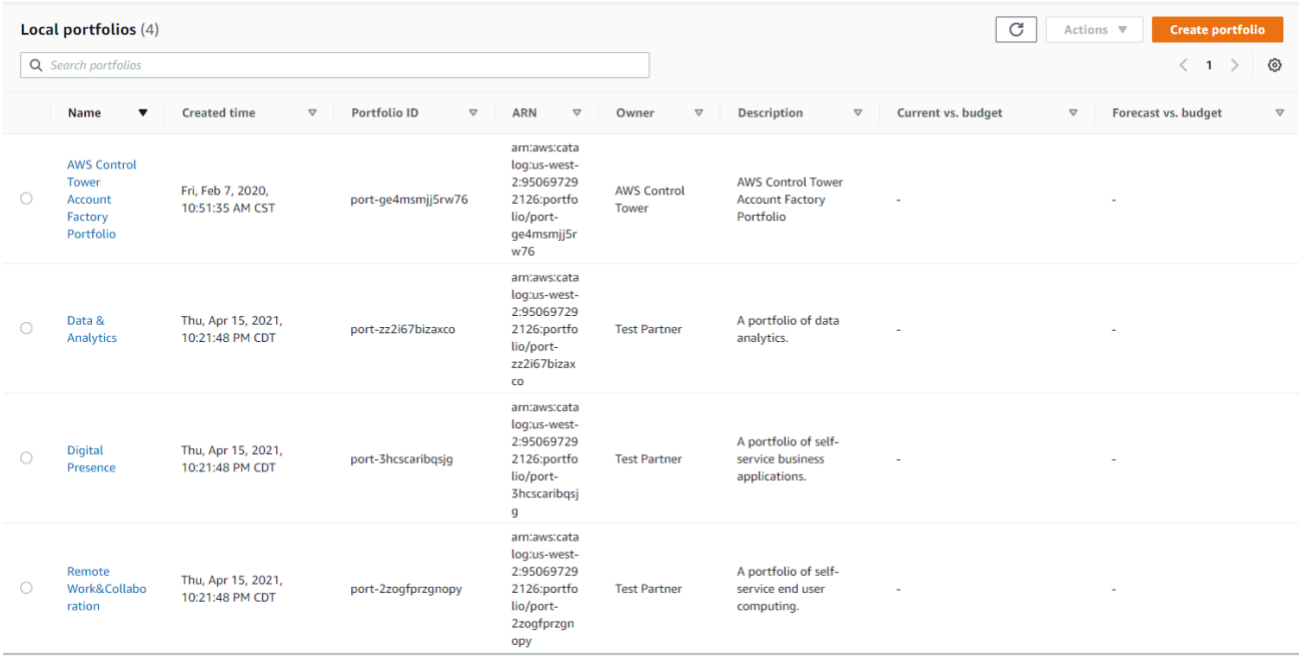

Figure 4: AWS Service Catalog showing the AWS Blueprints portfolios

3. On the portfolio page, select the **Share** tab.
4. In the **Share** tab, choose **Share**.
5. In the **Create Share** page, choose either the **AWS Account** or **Organization** and enter the corresponding account information.
6. Choose **Share**.

Import a portfolio into a customer's AWS account

After you have shared the portfolio, the customer can import it into their AWS account.

1. Sign in to the AWS Service Catalog console.
2. From the left navigation pane, select **Portfolios**.
3. From the **Portfolios** page, select the **Imported** tab.
4. Choose **Actions** and, from the drop-down menu, select **Import portfolio**.
5. In the **Import Portfolio** dialog box, enter the **Portfolio ID**.

> **Note:** The AWS Support Partner or AWS Distributor must share the Portfolio ID with their customers.

6. Choose **Import**.

You are returned to the Portfolio page where a confirmation message displays indicating a successful import.

7. Select the name of the portfolio you just imported.
8. Select the **Groups, roles and users** tab.
9. Choose **Add groups, roles, users**.
10. In the **Add groups, roles, and users** page, select the groups, roles, or users that should have access to this portfolio.
11. Choose **Add access**.

On the **Portfolios** page, the newly added members are displayed.

Step 3. Launch an AWS service or third-party application from the AWS Service Catalog portfolio in the customer's AWS account

After you have shared the necessary AWS Service Catalog portfolio(s) into your customer's AWS account, they will be able to launch the AWS services and third-party applications in the portfolio from the AWS Service Catalog console. When launching an AWS service or third-party application, you create a provisioned product, which is usually an instance of the product in an AWS CloudFormation stack.

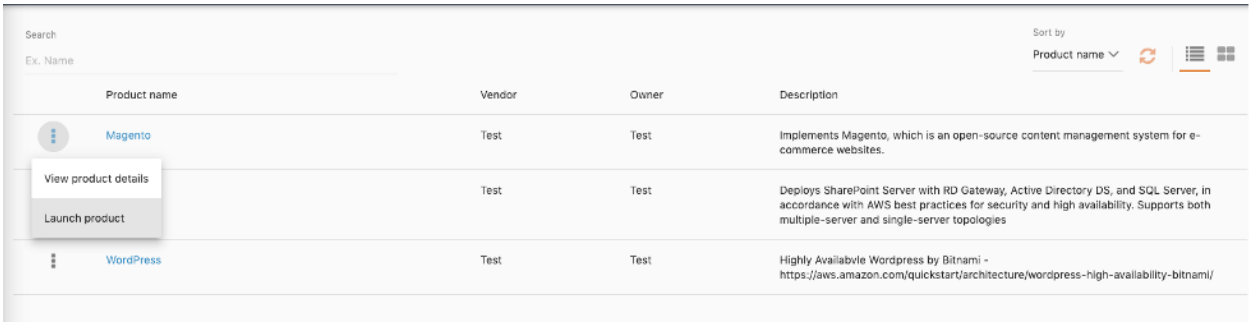

Figure 5: Example launch of a business application

Your customers can launch an AWS service or third-party application using the following steps. Additional information about the set up of the different AWS services and third-party applications follows these steps.

1. Sign in to the AWS Service Catalog console.
2. From the left navigation pane, select **Products**.
3. From the **Products** page, select the product name to launch, then choose **Launch product**.
4. On the **Launch** page for your selected product, enter the requested information and necessary parameters.
5. Choose **Launch product**.

You can view the status of the launched product from the **Provisioned product details** page. Alternatively, you can access the AWS CloudFormation console and select the **Events** tab to view the status of the deployment.

Since each AWS service and third-party application needs different set up information and parameter requirements, refer to the following product you are launching for additional guidance:

- Launch the third-party business applications
- Launch Simple AD

- Launch Amazon WorkSpaces

Launch the third-party business applications

To launch the third-party business applications, we recommend that you refer to the following AWS Quick Starts. These guides provide the implementation details you'll need when launching these applications from AWS Service Catalog.

- Magento on AWS Quick Start
- WordPress High Availability by Bitnami on AWS Quick Start

Launch Simple AD

Before you can launch Simple AD, you must import the end-user computing portfolio into the customer's AWS account. For the import steps, refer to Import a portfolio into a customer's AWS account in the Automated deployment section of this guide. Then use the following steps to set up and launch Simple AD.

1. Sign in to the AWS Service Catalog console.
2. From the left navigation pane, select **Products**.
3. On the **Products** page, select **Simple AD**.
4. On the **Simple AD** page, choose **Launch product**.
5. On the **Launch** page, under **Provisioned product name**, enter a unique product name or have the solution auto-generate one by selecting **Generate name**.
6. Under **Parameters**, take the following actions:
    - For **Create Alias**, keep the default option (either true or false). This parameter is only required for applications needing a URL to connect to the directory.
    - For **DomainName**, enter a fully qualified domain name. Note that you can use the Provisioned product name as an option.
    - For **EnableSingleSignOn**, select either true or false. Set this parameter to `true` if you want to allow AWS Directory Service to provide your users access to Amazon WorkDocs from a computer connected to the directory without the need to enter their credentials separately. Set to `false` if you do not want to allow users access to Amazon WorkDocs.
    - For **PrivateSubnet1** and **PrivateSubnet2**, access the drop-down menu for each one and select the desired subnets. These parameters install the two domain controllers in separate subnets that must be in a different Availability Zone. Note that a VPC with at least two subnets is needed for Simple AD to install correctly.
    - For **SimpleADPW**, create a password for the domain admin.

- For **SimpleADShortName**, enter a name for the NetBIOS domain for this directory. Note that you can use the domain name provided earlier.
- For **Size**, choose the size of the directory that you want. Your options are either **Small** or **Large**. For more information about sizes, refer to Simple Active Directory in the *AWS Directory Service Admin Guide*.
- For **VPCID**, enter the VPC ID for the directory.

7. Choose **Launch Product** to launch the Simple AD service.

On the Service Catalog Provisioned products page, review the directory name and status. It takes several minutes for the directory to be created. Once created, the **Status** value changes to **Active**. For additional information about Simple AD, refer to Create a Simple AD directory in the *AWS Directory Service Admin Guide*.

Launch Amazon WorkSpaces

To allow Amazon WorkSpaces to use an existing AWS Directory Service directory, you must register it with Amazon WorkSpaces. After you register a directory, you can launch WorkSpaces in that directory. Refer to register a directory in the *Amazon WorkSpaces Admin Guide*.

> **Note:** Before you can launch Amazon WorkSpaces, verify that your Simple AD is registered.

Before you can launch **WorkSpaces with Simple AD**, you must import the end-user computing portfolio into the customer's AWS account. For the import steps, refer to Import a portfolio into a customer's AWS account in the Automated deployment section of this guide. Then use the following steps to launch **WorkSpaces with Simple AD**:

1. Sign in to the AWS Service Catalog console.
2. From the left navigation pane, select **Products**.
3. On the **Products** page, select **WorkSpaces with Simple AD**.
4. On the **WorkSpaces with Simple AD** page, choose **Launch product**.
5. Under **Parameters**, take the following actions:

- For **Simple AD Directory ID**, enter the name of the Simple AD directory that you created earlier.
- For the **WorkSpaces Bundle**, select a bundle. For information about WorkSpaces Bundles and Images, refer to the *Amazon WorkSpaces Admin Guide*.

> **Note:** The following WorkSpaces bundles are included in the CloudFormation template:
>
> - wsb-bh8rsxt14: Value configuration with Windows 10

- wsb-8vbljg4r6 – Standard configuration with Windows 10
- wsb-gm4d5tx2v – Performance configuration with Windows 10

Additional bundle IDs can be added to the template by AWS partners. You can list all bundles by running the following AWS CLI command: `aws workspaces describe-workspace-bundles --owner AMAZON`

- For **WorkSpaces Running mode**, choose a running mode.
- For **Workspace Auto stop Timeout**, **Workspace Root Volume Size**, and **Workspace User Volume Size**, you can either keep the default values or select a different value that meets your business needs.

6. For the Username, enter a unique name that you have not used in WorkSpaces before.
7. For the EmailAddress, enter an email to receive notification of the WorkSpaces status.
8. Enter a FirstName and LastName and create a temporary Password. This Password can be reset by the user when they access WorkSpaces.
9. Select **Launch product** to provision Amazon Workspaces.

For additional information about Amazon WorkSpaces, refer to Get Started with Amazon WorkSpaces in the *Amazon WorkSpaces* Admin *Guide*.

(Optional) Add products to the AWS Service Catalog portfolio

You can add portfolios and products to AWS Blueprints by either editing the CloudFormation template or creating a new portfolio in AWS Service Catalog. To add products and portfolios in AWS Service Catalog, refer to Managing portfolios in the *AWS Service Catalog Admin Guide*.

If you choose to edit the CloudFormation template in AWS Blueprints, you must first complete the following prerequisite activities:

- Create an IAM role and attach the proper a policy (AWSCloudFormationFullAccess) that can launch the CloudFormation template.
- Create an AWS CloudFormation template to launch your product.
- Before adding your new template to AWS Blueprints, we recommend testing your new product template using the AWS Command Line Interface (AWS CLI) or manually from the AWS CloudFormation console.
- Once tested, upload your new product template to an S3 bucket and update the AWS Blueprints CloudFormation template stack.

After completing the prerequisite activities, use the following steps to edit the Blueprints CloudFormation template:

1. Open the AWS Blueprints CloudFormation template in a text editor.
2. Under the **Resources** section, add a new entry that defines the new portfolio. Note that you can use existing information for guidance in creating your new entry.
   - Enter a Type, which defines the portfolio that the product is a part of
   - Enter the Properties, which include a Description, DisplayName, and ProviderName.
   - Add **LoadTemplateFromURL**, and enter the location of the template
3. Save the template.
4. Sign into the AWS CloudFormation console and launch the updated template using the **Create Stack** option.

(Optional) Add ISV products from AWS Marketplace to AWS Service Catalog

You can add independent software vendor (ISV) products from AWS Marketplace to the AWS Service Catalog portfolios and share those portfolios in your customer accounts. Refer to Adding AWS Marketplace Products to Your Portfolio in the *AWS Service Catalog Admin Guide*.

The following examples are recommended AWS Marketplace/ISV products that you can add to the Backup & Recovery and Security portfolios.

For the Backup & Recovery portfolio, we recommend Veeam Backup for AWS Free Edition and Veritas Backup Exec™ for AWS from the AWS Marketplace.

- Veeam Backup for AWS Free Edition delivers native, fully automated AWS backup and disaster recovery to protect and manage Amazon EC2 and Amazon RDS data. This product is available a Linux-based EC2 instance image. To install, you must first configure installation settings in AWS Marketplace and then perform the initial configuration in the Veeam Backup for AWS Web UI. For information about installation, refer to Installing Veeam Backup for AWS from the Veeam Help Center.

- Veritas Backup Exec™ for AWS delivers secure offsite backup to AWS for your in-house virtual and physical environments, and also protects cloud-based workloads in AWS. This product provides flexible options and features to help you customize backups based on your business needs. Public cloud connectors to AWS allow data to be written directly to hot or cold cloud tiers across supported AWS storage Regions. For additional information, refer to the Usage Information.

For the Security portfolio, we recommend Trend Micro Deep Security from the AWS Marketplace. This product is a host-based security product that provides Anti-Malware, Host Firewall, Intrusion Prevention, File Integrity Monitoring, Log Inspection, Web Application Firewalling, and Content Filtering modules in a single agent running in the guest operating

system. For deployment guidance, refer to Deployment Steps in the *Trend Micro Deep Security on AWS Quick Start* guide.

Note: For launching the AWS Marketplace products in the customer account, you must subscribe to the AWS Marketplace product from the AWS account.

Additional Resources

AWS services

- AWS CloudFormation
- AWS Organizations
- Amazon Virtual Private Cloud (VPC)
- Amazon S3
- AWS WAF
- Amazon EC2
- Amazon Inspector
- AWS Directory Service
- AWS Single Sign-On
- Amazon ElasticSearch
- Amazon CloudWatch
- AWS Key Management Service
- Amazon Elastic Block Store

Related AWS resources

- Customizations for AWS Control Tower

To help your AWS Blueprints deployment, we recommend reviewing the following training resources.

AWS Control Tower

- What is AWS Control Tower?
- AWS Control Tower overview – Re:Inforce presentation providing an overview of multi-account structure and how to set this up in AWS Control Tower.
- AWS Control Tower lab – A core lab resource to help you set up AWS Control Tower and create and manage accounts.

AWS Service Catalog

- Introduction to AWS Service Catalog – An AWS video course that introduces AWS Service Catalog and how it helps you create and manage catalogs of IT services that are approved for use on AWS.
- AWS Service Catalog - Getting Started

AWS Service Catalog portfolios

- What is end-user computing? This course is available to AWS Distributors and AWS Solution Providers via Partner Central and provides a technical introduction to Amazon WorkSpaces and Amazon AppStream 2.0, the AWS service that provides managed end-user computing services.

  - AWS Solutions Training for Partners: Desktop and Application Streaming with AWS – Technical (Digital) - Module 1
  - Desktop and Application Streaming with AWS - Business (Digital)
- Best practices to automate end-user computing deployments – Reviews best practices for deploying end-user computing services
- Data Analytics Fundamentals – A self-paced e-learning course that helps you learn about the process for planning data analysis solutions and the various data analytic processes that are involved.
- Data Lake Foundation on AWS Quick Start
- Magento on AWS Quick Start
- WordPress High Availability by Bitnami on AWS Quick Start

Deployment models for AWS Blueprints

AWS Blueprints provides AWS Distributors and AWS Solution Providers the flexibility to choose deployment and delivery models that meet customers' needs. In this context, an AWS partner is defined as anyone who works directly with AWS as a Solution Provider or works with an AWS Distributor as a Distribution Seller.

Deployment model is defined as a framework or architecture that AWS Distributors and AWS Solution Providers can implement in their management account to manage customer AWS accounts for billing, access management, policies, etc. Two-tier and single-tier architectures are used respectively by AWS Distributors and AWS Solution Providers.

Delivery model is defined as a mechanism by which AWS Distributors and AWS Solution Providers deliver their value-added services like managed services to their customers as part of this deployment.

Distributor model

The Distributor model used by AWS Distributors is a two-tier deployment model where Distributors own the management account and manage multiple Distribution Seller accounts at scale. As illustrated in Figure 6, an OU acts as a virtual layer to differentiate partners and their associated customer AWS accounts, for the purpose of account management, consolidated billing, service control policies, etc. In this model, customers buy AWS services from the partners rather than directly from the Distribution Seller. Note that Distributors can potentially create more than one OU for the same Distribution Seller, however, a customer account can be part of only one OU at any point in time. A Distribution Seller can invite the customer accounts that already exist to join their OU.

After AWS Blueprints has been deployed in the Distributor's management account, a list of portfolios and products in the AWS Service Catalog is created (refer to the Architecture

overview section of this guide for the list of portfolios). These portfolios can be selectively shared across various Distribution Sellers at scale through the respective OUs that are assigned to each Distribution Seller. The individual AWS services and third-party applications (for example, WordPress) can then be launched by the customer or by the Distribution Seller.

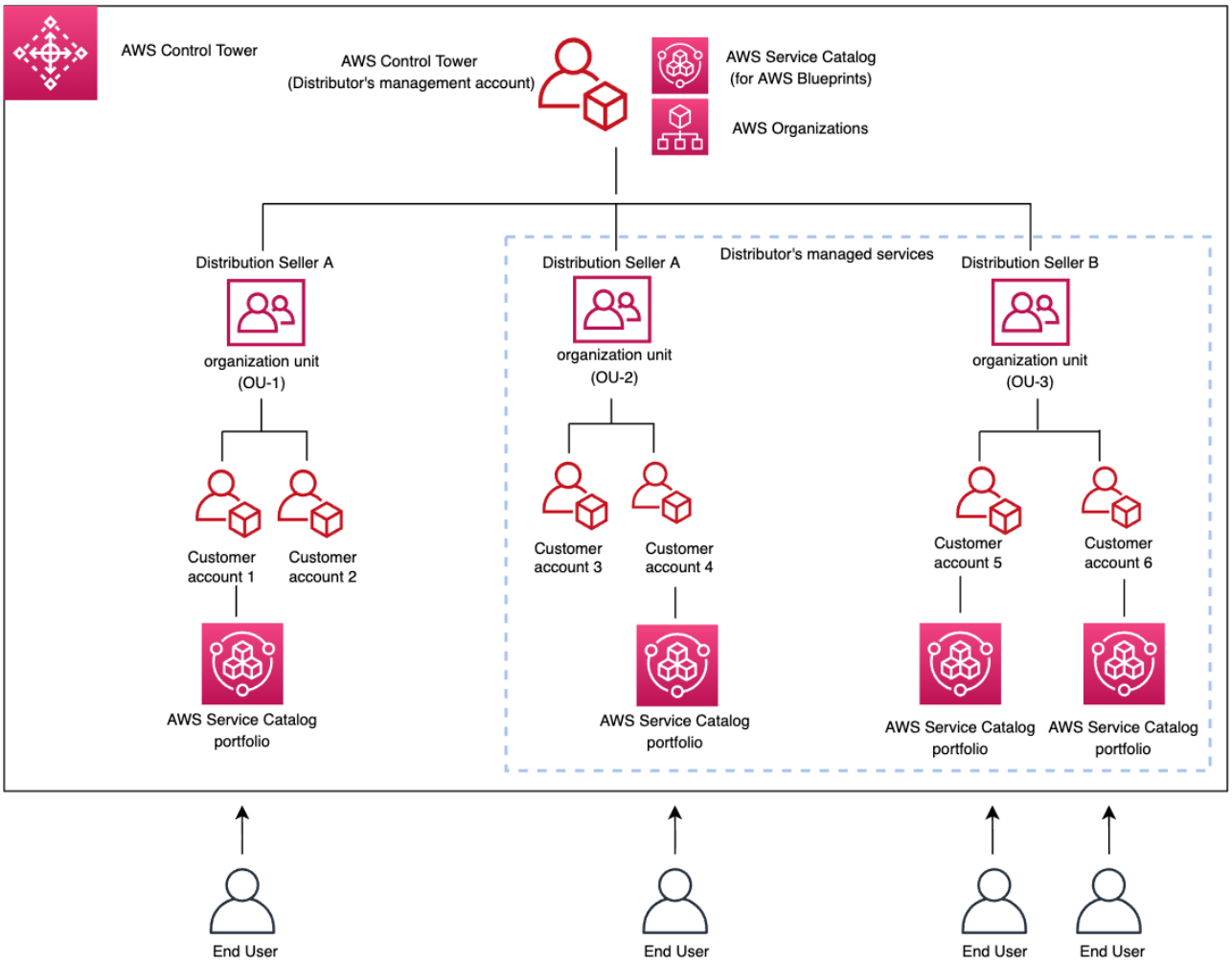

Figure 6: Distributor deployment model

Solution Provider model

The Solution Provider model used by AWS Solution Providers is a single-tier deployment model where Solution Providers own the control tower management account. As illustrated in Figure 7, an organizational unit (OU) acts as a virtual layer to differentiate customers for the purpose of account management, consolidated billing, service control policies, etc. Note that the providers can potentially create more than one OU for the same customer, however, a customer can have more than one account and each account can be part of only one OU at any point in time. Customer accounts that already exist can be invited to join this Solution Provider's AWS organization and can be assigned to an OU.

After AWS Blueprints has been deployed in the management account, a list of portfolios and products in the AWS Service Catalog is created (refer to the Architecture overview section of this guide for the list of portfolios). These portfolios can be selectively shared across various customer AWS accounts through the OUs. The individual AWS services and third-party applications (for example, WordPress) within these portfolios can then be launched by either the customer or Solution Provider. For example, if the customer wants to manage and deploy the portfolios, partners can create a delegated admin using AWS Identity and Access Management (IAM) for that customer. The customer can then manage portfolio assignments to users under that OU.

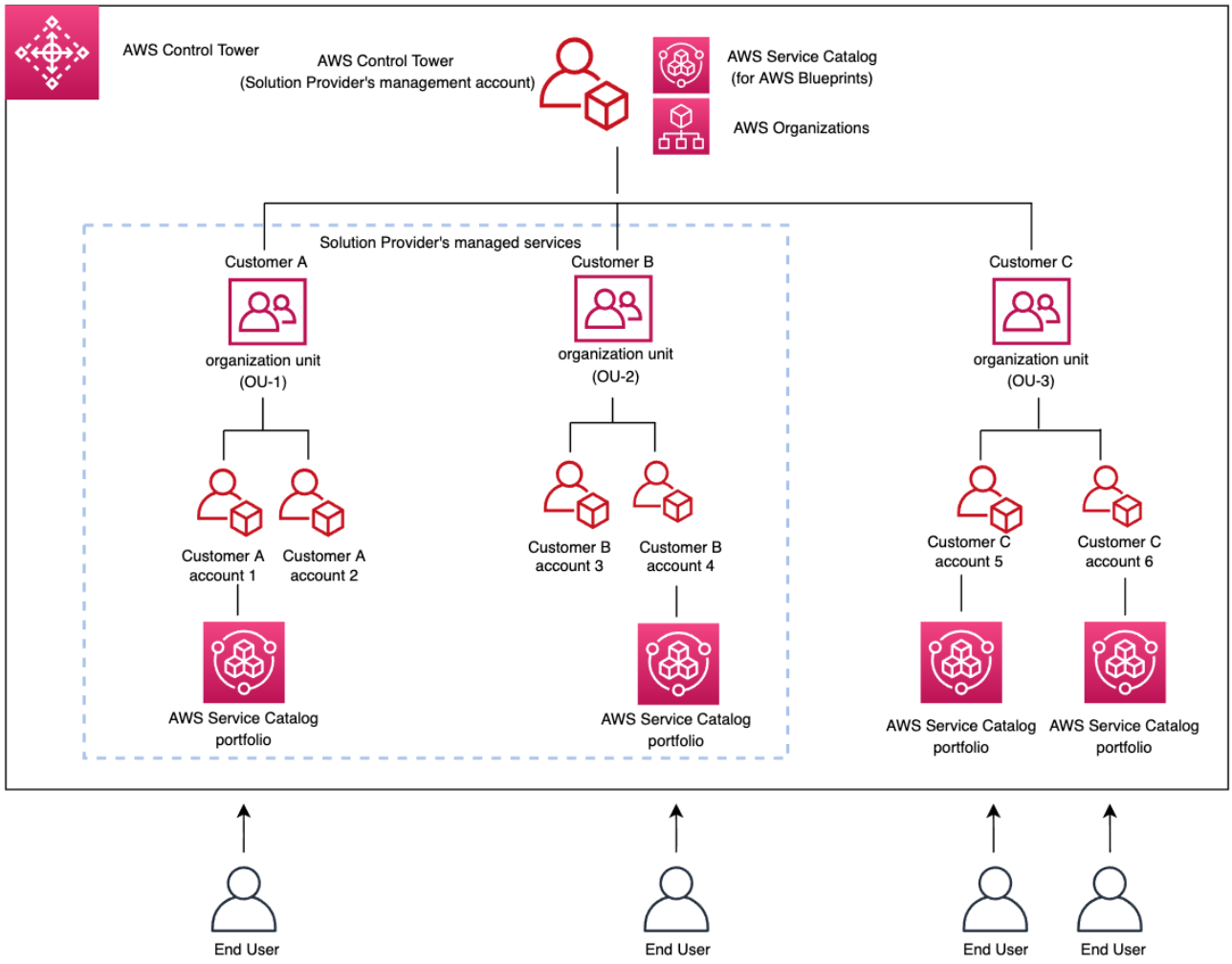

Figure 7: AWS Solution Provider deployment model

Delivery models for AWS Blueprints

The delivery model for AWS Blueprints works in conjunction with the deployment model, serving as a mechanism by which the AWS Service Catalog portfolios are launched in the customer's accounts and managed by AWS Distributors and AWS Solution Providers.

Table 2 shows the possible delivery model scenarios that AWS Distributors and AWS Solution Providers can adapt for the Distributor and Solution Provider deployment models.

For example, in Delivery Model 1, the customer assumes responsibility for both deploying and managing the individual products within the AWS Service Catalog portfolio. In this case, the Distribution Seller delegates the administrator permissions to the customer for their respective account. The delegated administrator can then import the portfolios assigned by the Distribution Seller into their AWS customer account. The delegated administrator can also assign the necessary IAM permissions to account users so they can launch the products from the imported portfolios.

For example, Delivery Model 6 identifies an AWS Solution Provider sharing the AWS Service Catalog portfolio with the customer and launches it in that customer's account. The Solution Provider manages the portfolio on an ongoing basis. The act of launching the portfolio into the customer's account can be classified as a consulting service while the management aspect is a managed service.

Table 2: Delivery model scenarios

Roles:	Billing Owner	Implementer	Managed Service Provider
Distributor – Delivery Model			
Delivery Model 1	Distribution sellers	Customer	Customer
Delivery Model 2	Distribution sellers	Distribution sellers	Customer
Delivery Model 3	Distribution sellers	Distribution sellers	Distribution sellers
Solution Provider – Delivery Model			
Delivery Model 4	Solution Provider	Customer	Customer
Delivery Model 5	Solution Provider	Solution Provider	Customer
Delivery Model 6	Solution Provider	Solution Provider	Solution Provider

AWS Systems Manager

AWS Systems Manager helps you view and control your infrastructure on AWS. Using the Systems Manager console, you can view operational data from multiple AWS services and automate operational tasks across your AWS resources. Systems Manager helps you maintain security and compliance by scanning your managed instances and reporting on (or taking corrective action on) any policy violations it detects.

The benefits of using Systems Manager with AWS Blueprints includes shortening the time to detect problems, automating tasks, improving visibility and control, managing hybrid environments, and maintaining security and compliance.

Operations Management

OpsCenter provides a central location where operations engineers and IT professionals can view, investigate, and resolve operational work items (OpsItems) related to AWS resources. OpsCenter is designed to reduce mean time to resolution for issues impacting AWS resources. This Systems Manager capability aggregates and standardizes OpsItems across services while providing contextual investigation data about each OpsItem, related OpsItems, and related resources. OpsCenter also provides Systems Manager Automation documents (runbooks) that you can use to quickly resolve issues. You can specify searchable, custom data for each OpsItem. You can also view automatically-generated summary reports about OpsItems by status and source.

OpsCenter is integrated with Amazon CloudWatch Events. This means you can create CloudWatch Events rules that automatically create OpsItems for any AWS service that publishes events to CloudWatch Events. For example, you can configure SSM OpsItems as the target for the following types of events, and hundreds more:

- Security issues, such as alerts from AWS Security Hub
- Performance issues, such as a throttling event for Amazon DynamoDB or degraded Amazon Elastic Block Store (EBS) volume performance
- Failures, such as an Amazon EC2 Auto Scaling group failure to launch an instance or a Systems Manager Automation execution failure
- Health alerts, such as an AWS Health alert for scheduled maintenance
- State changes, such as an EC2 instance state change from Running to Stopped

Explorer builds on top of OpsCenter for customizable operations dashboard that reports information about your AWS resources, aggregated view of operations data (OpsData) for your AWS accounts and across Regions, allows for S3 export. The OpsData includes, metadata about your Amazon EC2 instances, patch compliance details and operational work items (OpsItems).

Compliance is an AWS Provided Dashboard tool within Systems Manager that allows administrators to quickly understand the state of their State Manager Associations or Patch Manager applications

- You can influence the severity levels so the things that are important in your organization are categorized correctly
- Security patches = Critical
- AWS Systems Manager Agent (SSM Agent) Update = Medium

For additional information about using Systems Manager to effectively manage operational tasks, refer to the AWS Systems Manager Operational Capabilities whitepaper.

IAM Roles and policies for Lambda functions

In order to reduce the impact of a compromised asset, each AWS Lambda operation is provisioned with a dedicated role following separation of privilege and least privilege. The following list details each Lambda function and its respective policies.

```
LambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
        - Effect: Allow
          Principal:
            Service:
            - lambda.amazonaws.com
          Action:
          - sts:AssumeRole
      Path: "/"
      Policies:
      - PolicyName: root
        PolicyDocument:
          Version: '2012-10-17'
          Statement:
          -
            Action:
            - "logs:CreateLogGroup"
            - "logs:DeleteLogGroup"
            - "logs:CreateLogStream"
            - "logs:DeleteLogStream"
            - "logs:PutLogEvents"
            Effect: Allow
            Resource: "*"
          -
            Action:
            - "workdocs:DescribeUsers"
            - "workdocs:CreateUser"
            - "ds:DescribeDirectories"
            - "ec2:DescribeVpcs"
            - "ec2:DescribeSubnets"
            Effect: Allow
            Resource: "*"
          -
            Action:
            -  "ds:DescribeTrusts"
            -  "ds:DescribeDirectories"
```

```
              -  "ec2:AuthorizeSecurityGroupEgress"
              -  "ec2:AuthorizeSecurityGroupIngress"
              -  "ec2:CreateNetworkInterface"
              -  "ec2:CreateSecurityGroup"
              -  "ec2:DeleteNetworkInterface"
              -  "ec2:DeleteSecurityGroup"
              -  "ec2:DescribeNetworkInterfaces"
              -  "ec2:DescribeSubnets"
              -  "ec2:DescribeVpcs"
              -  "ec2:RevokeSecurityGroupEgress"
              -  "ec2:RevokeSecurityGroupIngress"
              -  "ec2:DescribeSecurityGroups"
              -  "sns:GetTopicAttributes"
              -  "sns:ListSubscriptions"
              -  "sns:ListSubscriptionsByTopic"
              -  "sns:ListTopics"
              -  "iam:ListRoles"
              -  "organizations:ListAccountsForParent"
              -  "organizations:ListRoots"
              -  "organizations:ListAccounts"
              -  "organizations:DescribeOrganization"
              -  "organizations:DescribeAccount"
              -
"organizations:ListOrganizationalUnitsForParent"
              -
"organizations:ListAWSServiceAccessForOrganization"
            Effect: Allow
            Resource: "*"
          -
              Action:
              -  "workdocs:RemoveUserFromGroup"
              -  "workdocs:AddUserToGroup"
              -  "workspaces:ModifyWorkspaceProperties"
              -  "workspaces:TerminateWorkspaces"
              -  "workspaces:RebuildWorkspaces"
              -  "workspaces:CreateWorkspaces"
              -  "workspaces:StopWorkspaces"
              -  "workspaces:CreateTags"
              -  "workspaces:DeleteTags"
              -  "workspaces:Describe*"
              -  "workspaces:StartWorkspaces"
              -  "workspaces:RebootWorkspaces"
              Effect: Allow
              Resource: "*"
```

Uninstall the solution

You can uninstall AWS Blueprints from the AWS Management Console or by using the AWS Command Line Interface. However, before you can delete the solution stack, you must first delete the following:

- The products provisioned by the CloudFormation stack including -
- The products that have been shared in the portfolios
- The portfolios that you have shared with your customers

In addition, if you choose to delete this solution, you should also delete the portfolios that you shared in your customer's AWS accounts to avoid charges in their accounts. For information about AWS Service Catalog administration, refer to Managing Catalogs in the *AWS Service Catalog Admin Guide*.

- For steps to delete products, refer to Deleting products in the *AWS Service Catalog Admin Guide*.
- For steps to delete portfolios, refer to Creating and Deleting Portfolios in the *AWS Service Catalog Admin Guide*.

Using the AWS Management Console

The main catalog launched in the AWS management account can be uninstalled by choosing the delete stack option from AWS Cloud Formation. Below are the steps that need to be followed to delete a stack:

1. Sign in to the AWS CloudFormation console.
2. Select this solution's installation stack.
3. Choose **Delete**.

Using AWS Command Line Interface

Determine whether the AWS Command Line Interface (AWS CLI) is available in your environment. For installation instructions, refer to What Is the AWS Command Line Interface in the *AWS CLI User Guide*. After confirming that the AWS CLI is available, run the following command.

```
$ aws cloudformation delete-stack --stack-name
<installation-stack-name>
```

Collection of operational metrics

This solution includes an option to send anonymous operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. When invoked, the following information is collected and sent to AWS:

- **Solution ID:** The AWS solution identifier
- **Unique ID (UUID):** Randomly generated, unique identifier for each <solution-name> deployment
- **Timestamp:** Data-collection timestamp

AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Policy. To opt out of this feature, modify the AWS CloudFormation template mapping section as follows:

```
"Send" : {
   "AnonymousUsage" : { "Data" : "Yes" }
},
```

to

```
"Send" : {
   "AnonymousUsage" : { "Data" : "No" }
},
```

Source Code

Visit the AWS Blueprints GitHub repository to download the templates and scripts for this solution, and to share your customizations with others.

Document Revisions

Date	Change
April 2021	Initial Release

Contributors

- Sai Reddy Thangirala
- Bharath Terala

- Gandhi Raketla
- Siva Thangavelu

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents AWS current product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. AWS responsibilities and liabilities to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.