

Contents

[Azure Blueprints documentation](#)

[Overview](#)

[What is Azure Blueprints?](#)

[Quickstarts](#)

[Create a blueprint - Portal](#)

[Create a blueprint - Azure PowerShell](#)

[Create a blueprint - Azure CLI](#)

[Create a blueprint - REST API](#)

[Create a blueprint - ARM template](#)

[Tutorials](#)

[Create from a blueprint sample](#)

[Protect new resources with blueprint resource locks](#)

[Learn: Govern multiple subscriptions by using Azure Blueprints](#)

[Samples](#)

[Index](#)

[Azure Security Benchmark](#)

[Azure Security Benchmark Foundation](#)

[Overview](#)

[Steps to deploy](#)

[Australian Government ISM PROTECTED](#)

[Overview](#)

[Control mapping](#)

[Steps to deploy](#)

[Canada Federal PBMM](#)

[CIS Microsoft Azure Foundations Benchmark v1.3.0](#)

[CIS Microsoft Azure Foundations Benchmark v1.1.0](#)

[CMMC Level 3](#)

[DoD Impact Level 4](#)

[Overview](#)

[Control mapping](#)

[Steps to deploy](#)

[DoD Impact Level 5](#)

[Overview](#)

[Control mapping](#)

[Steps to deploy](#)

[FedRAMP Moderate](#)

[Overview](#)

[Control mapping](#)

[Steps to deploy](#)

[FedRAMP High](#)

[Overview](#)

[Control mapping](#)

[Steps to deploy](#)

[HIPAA HITRUST 9.2](#)

[IRS 1075](#)

[ISO 27001](#)

[ISO 27001 - Shared Services](#)

[Overview](#)

[Control mapping](#)

[Steps to deploy](#)

[ISO 27001 - ASE/SQL Workload](#)

[Overview](#)

[Control mapping](#)

[Steps to deploy](#)

[Media](#)

[Overview](#)

[Control mapping](#)

[Steps to deploy](#)

[New Zealand ISM Restricted](#)

[NIST SP 800-53 R4](#)

[NIST SP 800-171 R2](#)

PCI-DSS v3.2.1

Overview

Control mapping

Steps to deploy

SWIFT CSP v2020

Overview

Control mapping

Steps to deploy

UK OFFICIAL and UK NHS

CAF Foundation

Overview

Steps to deploy

CAF Migrate landing zone

Overview

Steps to deploy

Concepts

Lifecycle of a blueprint

Stages of a blueprint deployment

Dynamic parameters in a blueprint

Sequencing order of blueprint deployment

Resource locking in Azure Blueprints

How-to guides

Manage assignments with PowerShell

Import and export with PowerShell

Update existing assignments from the portal

Configure your environment for a Blueprint Operator

Manage Blueprints as Code (community)

Troubleshoot

Reference

Azure CLI

Azure PowerShell

Azure SDK for .NET

[REST](#)

[PSGallery \(Az.Blueprint module\)](#)

[PSGallery \(community module\)](#)

[Blueprint functions](#)

[Resources](#)

[GitHub - Azure Blueprints samples](#)

[Microsoft Q&A for Azure Blueprints](#)

[Governance YouTube Channel](#)

[Azure Friday - Azure Blueprints Overview](#)

[Azure roadmap](#)

[Pricing calculator](#)

[UserVoice](#)

What is Azure Blueprints?

5/3/2021 • 7 minutes to read • [Edit Online](#)

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

The Azure Blueprints service is backed by the globally distributed [Azure Cosmos DB](#). Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, regardless of which region Azure Blueprints deploys your resources to.

How it's different from ARM templates

The service is designed to help with *environment setup*. This setup often consists of a set of resource groups, policies, role assignments, and ARM template deployments. A blueprint is a package to bring each of these *artifact* types together and allow you to compose and version that package, including through a continuous integration and continuous delivery (CI/CD) pipeline. Ultimately, each is assigned to a subscription in a single operation that can be audited and tracked.

Nearly everything that you want to include for deployment in Azure Blueprints can be accomplished with an ARM template. However, an ARM template is a document that doesn't exist natively in Azure - each is stored either locally or in source control. The template gets used for deployments of one or more Azure resources, but once those resources deploy there's no active connection or relationship to the template.

With Azure Blueprints, the relationship between the blueprint definition (what *should be* deployed) and the blueprint assignment (what *was* deployed) is preserved. This connection supports improved tracking and auditing of deployments. Azure Blueprints can also upgrade several subscriptions at once that are governed by the same blueprint.

There's no need to choose between an ARM template and a blueprint. Each blueprint can consist of zero or more ARM template *artifacts*. This support means that previous efforts to develop and maintain a library of ARM templates are reusable in Azure Blueprints.

How it's different from Azure Policy

A blueprint is a package or container for composing focus-specific sets of standards, patterns, and requirements related to the implementation of Azure cloud services, security, and design that can be reused to maintain consistency and compliance.

A [policy](#) is a default allow and explicit deny system focused on resource properties during deployment and for

already existing resources. It supports cloud governance by validating that resources within a subscription adhere to requirements and standards.

Including a policy in a blueprint enables the creation of the right pattern or design during assignment of the blueprint. The policy inclusion makes sure that only approved or expected changes can be made to the environment to protect ongoing compliance to the intent of the blueprint.

A policy can be included as one of many *artifacts* in a blueprint definition. Blueprints also support using parameters with policies and initiatives.

Blueprint definition

A blueprint is composed of *artifacts*. Azure Blueprints currently supports the following resources as artifacts:

RESOURCE	HIERARCHY OPTIONS	DESCRIPTION
Resource Groups	Subscription	Create a new resource group for use by other artifacts within the blueprint. These placeholder resource groups enable you to organize resources exactly the way you want them structured and provides a scope limiter for included policy and role assignment artifacts and ARM templates.
ARM template	Subscription, Resource Group	Templates, including nested and linked templates, are used to compose complex environments. Example environments: a SharePoint farm, Azure Automation State Configuration, or a Log Analytics workspace.
Policy Assignment	Subscription, Resource Group	Allows assignment of a policy or initiative to the subscription the blueprint is assigned to. The policy or initiative must be within the scope of the blueprint definition location. If the policy or initiative has parameters, these parameters are assigned at creation of the blueprint or during blueprint assignment.
Role Assignment	Subscription, Resource Group	Add an existing user or group to a built-in role to make sure the right people always have the right access to your resources. Role assignments can be defined for the entire subscription or nested to a specific resource group included in the blueprint.

Blueprint definition locations

When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a [management group](#) or subscription that you have **Contributor** access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

Blueprint parameters

Blueprints can pass parameters to either a policy/initiative or an ARM template. When adding either *artifact* to a blueprint, the author decides to provide a defined value for each blueprint assignment or to allow each blueprint assignment to provide a value at assignment time. This flexibility provides the option to define a pre-determined

value for all uses of the blueprint or to enable that decision to be made at the time of assignment.

NOTE

A blueprint can have its own parameters, but these can currently only be created if a blueprint is generated from REST API instead of through the Portal.

For more information, see [blueprint parameters](#).

Blueprint publishing

When a blueprint is first created, it's considered to be in **Draft** mode. When it's ready to be assigned, it needs to be **Published**. Publishing requires defining a **Version** string (letters, numbers, and hyphens with a max length of 20 characters) along with optional **Change notes**. The **Version** differentiates it from future changes to the same blueprint and allows each version to be assigned. This versioning also means different **Versions** of the same blueprint can be assigned to the same subscription. When additional changes are made to the blueprint, the **Published Version** still exists, as do the **Unpublished changes**. Once the changes are complete, the updated blueprint is **Published** with a new and unique **Version** and can now also be assigned.

Blueprint assignment

Each **Published Version** of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription. In the portal, the blueprint defaults the **Version** to the one **Published** most recently. If there are artifact parameters or blueprint parameters, then the parameters are defined during the assignment process.

NOTE

Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription. To perform a management group assignment, the [Create Or Update REST API](#) must be used and the request body must include a value for `properties.scope` to define the target subscription.

Permissions in Azure Blueprints

To use blueprints, you must be granted permissions through [Azure role-based access control \(Azure RBAC\)](#). To read or view a blueprint in Azure portal, your account must have read access to the scope where the blueprint definition is located.

To create blueprints, your account needs the following permissions:

- `Microsoft.Blueprint/blueprints/write` - Create a blueprint definition
- `Microsoft.Blueprint/blueprints/artifacts/write` - Create artifacts on a blueprint definition
- `Microsoft.Blueprint/blueprints/versions/write` - Publish a blueprint

To delete blueprints, your account needs the following permissions:

- `Microsoft.Blueprint/blueprints/delete`
- `Microsoft.Blueprint/blueprints/artifacts/delete`
- `Microsoft.Blueprint/blueprints/versions/delete`

NOTE

The blueprint definition permissions must be granted or inherited on the management group or subscription scope where it is saved.

To assign or unassign a blueprint, your account needs the following permissions:

- `Microsoft.Blueprint/blueprintAssignments/write` - Assign a blueprint
- `Microsoft.Blueprint/blueprintAssignments/delete` - Unassign a blueprint

NOTE

As blueprint assignments are created on a subscription, the blueprint assign and unassign permissions must be granted on a subscription scope or be inherited onto a subscription scope.

The following built-in roles are available:

AZURE ROLE	DESCRIPTION
Owner	In addition to other permissions, includes all Azure Blueprint related permissions.
Contributor	In addition to other permissions, can create and delete blueprint definitions, but doesn't have blueprint assignment permissions.
Blueprint Contributor	Can manage blueprint definitions, but not assign them.
Blueprint Operator	Can assign existing published blueprints, but can't create new blueprint definitions. Blueprint assignment only works if the assignment is done with a user-assigned managed identity.

If these built-in roles don't fit your security needs, consider creating a [custom role](#).

NOTE

If using a system-assigned managed identity, the service principal for Azure Blueprints requires the **Owner** role on the assigned subscription in order to enable deployment. If using the portal, this role is automatically granted and revoked for the deployment. If using the REST API, this role must be manually granted, but is still automatically revoked after the deployment completes. If using a user-assigned managed identity, only the user creating the blueprint assignment needs the `Microsoft.Blueprint/blueprintAssignments/write` permission, which is included in both the **Owner** and **Blueprint Operator** built-in roles.

Naming limits

The following limitations exist for certain fields:

OBJECT	FIELD	ALLOWED CHARACTERS	MAX. LENGTH
Blueprint	Name	letters, numbers, hyphens, and periods	48

OBJECT	FIELD	ALLOWED CHARACTERS	MAX. LENGTH
Blueprint	Version	letters, numbers, hyphens, and periods	20
Blueprint assignment	Name	letters, numbers, hyphens, and periods	90
Blueprint artifact	Name	letters, numbers, hyphens, and periods	48

Video overview

The following overview of Azure Blueprints is from Azure Fridays. For video download, visit [Azure Fridays - An overview of Azure Blueprints](#) on Channel 9.

Next steps

- [Create a blueprint - Portal.](#)
- [Create a blueprint - PowerShell.](#)
- [Create a blueprint - REST API.](#)

Quickstart: Define and assign a blueprint in the portal

5/26/2021 • 10 minutes to read • [Edit Online](#)

When you learn how to create and assign blueprints, you can define common patterns to develop reusable and rapidly deployable configurations based on Azure Resource Manager templates (ARM templates), policy, security, and more. In this tutorial, you learn to use Azure Blueprints to do some of the common tasks related to creating, publishing, and assigning a blueprint within your organization. These tasks include:

Prerequisites

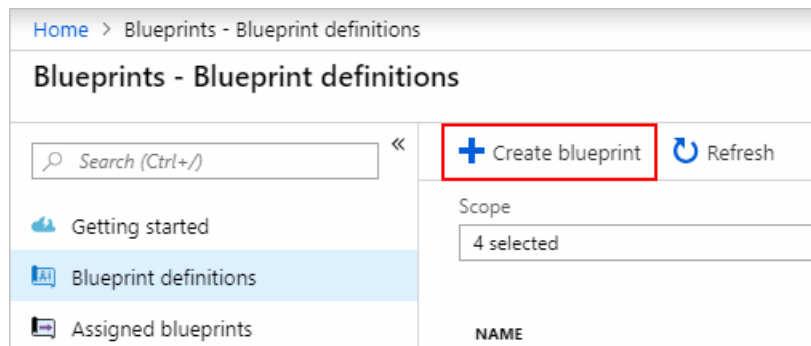
If you don't have an Azure subscription, create a [free account](#) before you begin.

Create a blueprint

The first step in defining a standard pattern for compliance is to compose a blueprint from the available resources. In this example, create a new blueprint named **MyBlueprint** to configure role and policy assignments for the subscription. Then add a new resource group, and create a Resource Manager template and role assignment on the new resource group.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select **Blueprint definitions** from the page on the left and select the **+ Create blueprint** button at the top of the page.

Or, select **Create** from the **Getting started** page to go straight to creating a blueprint.




3. Select **Start with blank blueprint** from the card at the top of the built-in blueprints list.
4. Provide a **Blueprint name** such as **MyBlueprint**. (Use up to 48 letters and numbers, but no spaces or special characters). Leave **Blueprint description** blank for now.
5. In the **Definition location** box, select the ellipsis on the right, select the [management group](#) or subscription where you want to save the blueprint, and choose **Select**.
6. Verify that the information is correct. The **Blueprint name** and **Definition location** fields can't be changed later. Then select **Next : Artifacts** at the bottom of the page or the **Artifacts** tab at the top of the page.
7. Add a role assignment at the subscription level:
 - a. Select the **+ Add artifact** row under **Subscription**. The **Add artifact** window opens on the right side of the browser.

- b. Select **Role assignment** for **Artifact type**.
- c. Under **Role**, select **Contributor**. Leave the **Add user, app or group** box with the check box that indicates a dynamic parameter.
- d. Select **Add** to add this artifact to the blueprint.

*** Artifact type**

Role assignment



You can choose to fill these parameters in now or when assigning the blueprint.

Role ⓘ

Contributor

Add user, app or group ⓘ

Search by name or email

☒ This value should be specified when the blueprint is assigned

NOTE

Most artifacts support parameters. A parameter that's assigned a value during blueprint creation is a *static parameter*. If the parameter is assigned during blueprint assignment, it's a *dynamic parameter*. For more information, see [Blueprint parameters](#).

8. Add a policy assignment at the subscription level:
 - a. Select the + **Add artifact** row under the role assignment artifact.
 - b. Select **Policy assignment** for **Artifact type**.
 - c. Change **Type** to **Built-in**. In **Search**, enter **tag**.
 - d. Change focus out of **Search** for the filtering to occur. Select **Append tag and its value to resource groups**.
 - e. Select **Add** to add this artifact to the blueprint.
9. Select the row of the policy assignment **Append tag and its value to resource groups**.
10. The window to provide parameters to the artifact as part of the blueprint definition opens and allows setting the parameters for all assignments (static parameters) based on this blueprint instead of during assignment (dynamic parameters). This example uses dynamic parameters during blueprint assignment, so leave the defaults and select **Cancel**.
11. Add a resource group at the subscription level:
 - a. Select the + **Add artifact** row under **Subscription**.
 - b. Select **Resource group** for **Artifact type**.
 - c. Leave the **Artifact display name**, **Resource Group Name**, and **Location** boxes blank, but make sure that the check box is checked for each parameter property to make them dynamic parameters.
 - d. Select **Add** to add this artifact to the blueprint.

12. Add a template under the resource group:

- a. Select the + **Add artifact** row under the **ResourceGroup** entry.
- b. Select **Azure Resource Manager template** for **Artifact type**, set **Artifact display name** to **StorageAccount**, and leave **Description** blank.
- c. On the **Template** tab in the editor box, paste the following ARM template. After you paste the template, select the **Parameters** tab and note that the template parameters **storageAccountType** and **location** were detected. Each parameter was automatically detected and populated, but configured as a dynamic parameter.

IMPORTANT

If you're importing the template, ensure that the file is only JSON and doesn't include HTML. When you're pointing to a URL on GitHub, ensure that you have selected **RAW** to get the pure JSON file and not the one wrapped with HTML for display on GitHub. An error occurs if the imported template is not purely JSON.

```


{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "storageAccountType": {
      "type": "string",
      "defaultValue": "Standard_LRS",
      "allowedValues": [
        "Standard_LRS",
        "Standard_GRS",
        "Standard_ZRS",
        "Premium_LRS"
      ],
      "metadata": {
        "description": "Storage Account type"
      }
    },
    "location": {
      "type": "string",
      "defaultValue": "[resourceGroup().location]",
      "metadata": {
        "description": "Location for all resources."
      }
    }
  },
  "variables": {
    "storageAccountName": "[concat('store', uniquestring(resourceGroup().id))]"
  },
  "resources": [{
    "type": "Microsoft.Storage/storageAccounts",
    "name": "[variables('storageAccountName')]",
    "location": "[parameters('location')]",
    "apiVersion": "2018-07-01",
    "sku": {
      "name": "[parameters('storageAccountType')]"
    },
    "kind": "StorageV2",
    "properties": {}
  }],
  "outputs": {
    "storageAccountName": {
      "type": "string",
      "value": "[variables('storageAccountName')]"
    }
  }
}

```

- d. Clear the **storageAccountType** check box and note that the dropdown list contains only values included in the ARM template under **allowedValues**. Select the box to set it back to a dynamic parameter.
- e. Select **Add** to add this artifact to the blueprint.

Template

Parameters



You can choose to fill these parameters in now or when assigning the blueprint.

storageAccountType ⓘ

Standard_LRS

▼






☒ This value should be specified when the blueprint is assigned

location ⓘ

[resourceGroups('ResourceGroup').location]

☒ This value should be specified when the blueprint is assigned

13. Your completed blueprint should look similar to the following. Notice that each artifact has *x out of y* parameters populated in the **Parameters** column. The dynamic parameters are set during each assignment of the blueprint.

Create blueprint		
<div>Basics</div> <div>Artifacts</div>		
Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.		
NAME	ARTIFACT TYPE	PARAMETERS
<div>▼  Subscription</div>		
 [User group or application name] : Contributor	Role assignment	0 out of 1 parameters populated
 Apply tag and its default value to resource groups	Policy assignment	0 out of 2 parameters populated
<div>+</div> <div>Add artifact...</div>		
<div>▼  ResourceGroup</div>		
 StorageAccount	Azure Resource Manager template	0 out of 2 parameters populated
<div>+</div> <div>Add artifact...</div>		

14. Now that all planned artifacts have been added, select **Save Draft** at the bottom of the page.

Edit a blueprint

In [Create a blueprint](#), you didn't provide a description or add the role assignment to the new resource group. You can fix both by following these steps:

1. Select **Blueprint definitions** from the page on the left.
2. In the list of blueprints, select and hold (or right-click) the one that you previously created and select **Edit blueprint**.
3. In **Blueprint description**, provide some information about the blueprint and the artifacts that compose it. In this case, enter something like: **This blueprint sets tag policy and role assignment on the subscription, creates a ResourceGroup, and deploys a resource template and role assignment to that ResourceGroup.**
4. Select **Next : Artifacts** at the bottom of the page or the **Artifacts** tab at the top of the page.
5. Add a role assignment under the resource group:
 - a. Select the **+ Add artifact** row directly under the **ResourceGroup** entry.
 - b. Select **Role assignment** for **Artifact type**.
 - c. Under **Role**, select **Owner**, and clear the check box under the **Add user, app or group** box.

- d. Search for and select a user, app, or group to add. This artifact uses a static parameter set the same in every assignment of this blueprint.
- e. Select **Add** to add this artifact to the blueprint.

*** Artifact type**

Role assignment

i You can choose to fill these parameters in now or when assigning the blueprint.

Role

Owner

Add user, app or group

Contoso

☐ This value should be specified when the blueprint is assigned

6. Your completed blueprint should look similar to the following. Notice that the newly added role assignment shows **1 out of 1 parameters populated**. That means it's a static parameter.

Edit blueprint		
<div> <div>Basics</div> <div>Artifacts</div> </div>		
Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.		
NAME	ARTIFACT TYPE	PARAMETERS
<div> <div>Subscription</div> </div>		
<div> <div></div> <div>[User group or application name] : Contributor</div> </div>	Role assignment	0 out of 1 parameters populated
<div> <div></div> <div>Apply tag and its default value to resource groups</div> </div>	Policy assignment	0 out of 2 parameters populated
<div> <div>+</div> <div>Add artifact...</div> </div>		
<div> <div>ResourceGroup</div> </div>		
<div> <div></div> <div>StorageAccount</div> </div>	Azure Resource Manager template	0 out of 2 parameters populated
<div> <div></div> <div>Contoso : Owner</div> </div>	Role assignment	1 out of 1 parameters populated
<div> <div>+</div> <div>Add artifact...</div> </div>		

7. Select **Save Draft** now that it has been updated.

Publish a blueprint

Now that all the planned artifacts have been added to the blueprint, it's time to publish it. Publishing makes the blueprint available to be assigned to a subscription.

1. Select **Blueprint definitions** from the page on the left.
2. In the list of blueprints, select and hold (or right-click) the one you previously created and select **Publish blueprint**.
3. In the pane that opens, provide a **Version** (letters, numbers, and hyphens with a maximum length of 20 characters), such as **v1**. Optionally, enter text in **Change notes**, such as **First publish**.
4. Select **Publish** at the bottom of the page.

Assign a blueprint

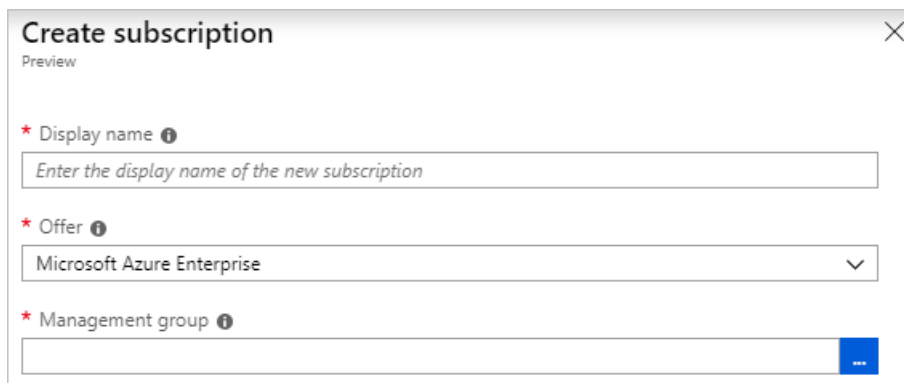
After a blueprint has been published, it can be assigned to a subscription. Assign the blueprint that you created

to one of the subscriptions under your management group hierarchy. If the blueprint is saved to a subscription, it can only be assigned to that subscription.

1. Select **Blueprint definitions** from the page on the left.
2. In the list of blueprints, select and hold (or right-click) the one that you previously created (or select the ellipsis) and select **Assign blueprint**.
3. On the **Assign blueprint** page, in the **Subscription** dropdown list, select the subscriptions that you want to deploy this blueprint to.

If there are supported Enterprise offerings available from [Azure Billing](#), a **Create new** link is activated under the **Subscription** box. Follow these steps:

- a. Select the **Create new** link to create a new subscription instead of selecting existing ones.
- b. Provide a **Display name** for the new subscription.
- c. Select the available **Offer** from the dropdown list.
- d. Use the ellipsis to select the [management group](#) that the subscription will be a child of.
- e. Select **Create** at the bottom of the page.



IMPORTANT

The new subscription is created immediately after you select **Create**.

NOTE

An assignment is created for each subscription that you select. You can make changes to a single subscription assignment at a later time without forcing changes on the remainder of the selected subscriptions.

4. For **Assignment name**, provide a unique name for this assignment.
5. In **Location**, select a region for the managed identity and subscription deployment object to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [Managed identities for Azure resources](#).
6. Leave the **Blueprint definition version** dropdown list selection of **Published** versions on the **v1** entry. (The default is the most recently published version.)
7. For **Lock Assignment**, leave the default of **Don't Lock**. For more information, see [Blueprints resource locking](#).

Lock Assignment

Don't Lock

Read Only

Do Not Delete

The assignment is not locked. Users, groups, and service principals with permissions can modify and delete deployed resources. [Learn more](#)

Managed Identity ⓘ

☒ System assigned
☐ User assigned

8. Under **Managed Identity**, leave the default of **System assigned**.
9. For the subscription level role assignment [User group or application name] : **Contributor**, search for and select a user, app, or group.
10. For the subscription level policy assignment, set **Tag Name** to **CostCenter** and the **Tag Value** to **ContosoIT**.
11. For **ResourceGroup**, provide a **Name** of **StorageAccount** and a **Location** of **East US 2** from the dropdown list.

NOTE

For each artifact that you added under the resource group during blueprint definition, that artifact is indented to align with the resource group or object that you'll deploy it with. Artifacts that either don't take parameters or have no parameters to be defined at assignment are listed only for contextual information.

12. On the ARM template **StorageAccount**, select **Standard_GRS** for the **storageAccountType** parameter.
13. Read the information box at the bottom of the page, and then select **Assign**.

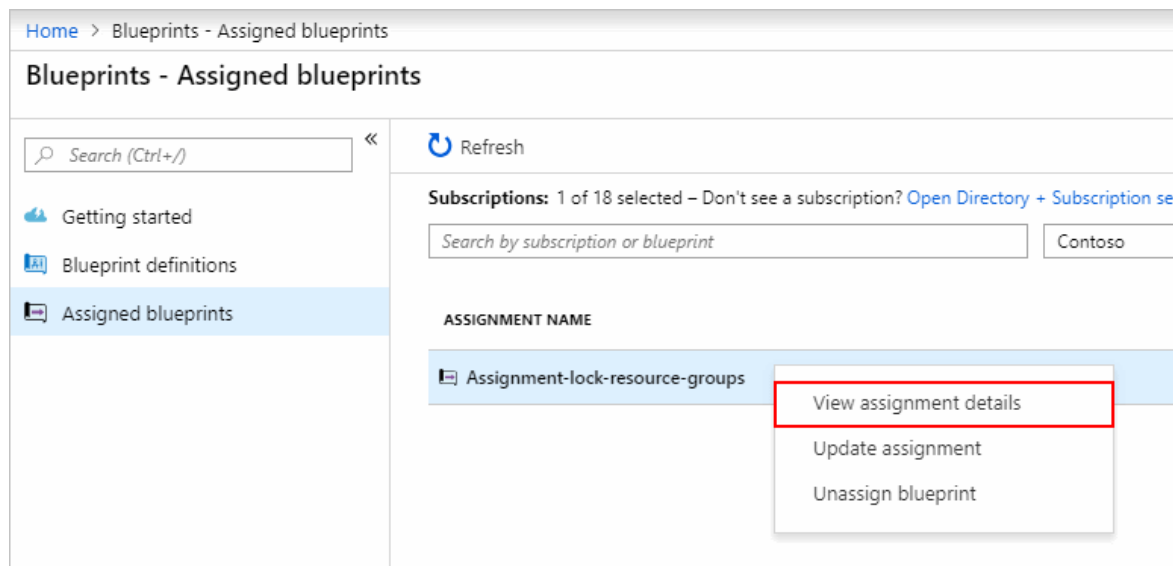
Track deployment of a blueprint

When a blueprint has been assigned to one or more subscriptions, two things happen:

- The blueprint is added to the **Assigned blueprints** page for each subscription.
- The process of deploying all the artifacts defined by the blueprint begins.

Now that the blueprint has been assigned to a subscription, verify the progress of the deployment:

1. Select **Assigned blueprints** from the page on the left.
2. In the list of blueprints, select and hold (or right-click) the one that you previously assigned and select **View assignment details**.



3. On the **Blueprint assignment** page, validate that all artifacts were successfully deployed and that there were no errors during the deployment. If errors occurred, see [Troubleshooting blueprints](#) for steps to determine what went wrong.

Clean up resources

Unassign a blueprint

If you no longer need a blueprint assignment, remove it from a subscription. The blueprint might have been replaced by a newer blueprint with updated patterns, policies, and designs. When a blueprint is removed, the artifacts assigned as part of that blueprint are left behind. To remove a blueprint assignment, follow these steps:

1. Select **Assigned blueprints** from the page on the left.
2. In the list of blueprints, select the blueprint that you want to unassign. Then select the **Unassign blueprint** button at the top of the page.
3. Read the confirmation message and then select **OK**.

Delete a blueprint

1. Select **Blueprint definitions** from the page on the left.
2. Right-click the blueprint that you want to delete, and select **Delete blueprint**. Then select **Yes** in the confirmation dialog box.

NOTE

Deleting a blueprint in this method also deletes all published versions of the selected blueprint. To delete a single version, open the blueprint, select the **Published versions** tab, select the version that you want to delete, and then select **Delete This Version**. Also, you can't delete a blueprint until you've deleted all blueprint assignment of that blueprint definition.

Next steps

In this quickstart, you've created, assigned, and removed a blueprint with Azure portal. To learn more about Azure Blueprints, continue to the [blueprint lifecycle](#) article.

[Learn about the blueprint lifecycle](#)

Quickstart: Define and Assign an Azure Blueprint with PowerShell

5/3/2021 • 9 minutes to read • [Edit Online](#)

Learning how to create and assign blueprints enables the definition of common patterns to develop reusable and rapidly deployable configurations based on Azure Resource Manager templates (ARM templates), policy, security, and more. In this tutorial, you learn to use Azure Blueprints to do some of the common tasks related to creating, publishing, and assigning a blueprint within your organization, such as:

Prerequisites




- If you don't have an Azure subscription, create a [free account](#) before you begin.
- If it isn't already installed, follow the instructions in [Add the Az.Blueprint module](#) to install and validate the **Az.Blueprint** module from the PowerShell Gallery.
- If you've not used Azure Blueprints before, register the resource provider through Azure PowerShell with

```
Register-AzResourceProvider -ProviderNamespace Microsoft.Blueprint .
```

Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

OPTION	EXAMPLE/LINK
Select Try It in the upper-right corner of a code block. Selecting Try It doesn't automatically copy the code to Cloud Shell.	
Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser.	
Select the Cloud Shell button on the menu bar at the upper right in the Azure portal .	

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

Create a blueprint

The first step in defining a standard pattern for compliance is to compose a blueprint from the available resources. We'll create a blueprint named 'MyBlueprint' to configure role and policy assignments for the subscription. Then we'll add a resource group, an ARM template, and a role assignment on the resource group.

NOTE

When using PowerShell, the *blueprint* object is created first. For each *artifact* to be added that has parameters, the parameters need to be defined in advance on the initial *blueprint*.

1. Create the initial *blueprint* object. The **BlueprintFile** parameter takes a JSON file that includes properties about the blueprint, any resource groups to create, and all of the blueprint level parameters. The parameters are set during assignment and used by the artifacts added in later steps.
 - JSON file - blueprint.json

```

{
  "properties": {
    "description": "This blueprint sets tag policy and role assignment on the
subscription, creates a ResourceGroup, and deploys a resource template and role assignment to
that ResourceGroup.",
    "targetScope": "subscription",
    "parameters": {
      "storageAccountType": {
        "type": "string",
        "defaultValue": "Standard_LRS",
        "allowedValues": [
          "Standard_LRS",
          "Standard_GRS",
          "Standard_ZRS",
          "Premium_LRS"
        ],
        "metadata": {
          "displayName": "storage account type.",
          "description": null
        }
      },
      "tagName": {
        "type": "string",
        "metadata": {
          "displayName": "The name of the tag to provide the policy assignment.",
          "description": null
        }
      },
      "tagValue": {
        "type": "string",
        "metadata": {
          "displayName": "The value of the tag to provide the policy assignment.",
          "description": null
        }
      },
      "contributors": {
        "type": "array",
        "metadata": {
          "description": "List of AAD object IDs that is assigned Contributor role
at the subscription",
          "strongType": "PrincipalId"
        }
      },
      "owners": {
        "type": "array",
        "metadata": {
          "description": "List of AAD object IDs that is assigned Owner role at the
resource group",
          "strongType": "PrincipalId"
        }
      },
      "resourceGroups": {
        "storageRG": {
          "description": "Contains the resource template deployment and a role
assignment."
        }
      }
    }
  }
}

```

- PowerShell command

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get a reference to the new blueprint object, we'll use it in subsequent steps
$blueprint = New-AzBlueprint -Name 'MyBlueprint' -BlueprintFile .\blueprint.json
```

NOTE

Use the filename *blueprint.json* when creating your blueprint definitions programmatically. This file name is used when calling [Import-AzBlueprintWithArtifact](#).

The blueprint object is created in the default subscription by default. To specify the management group, use parameter **ManagementGroupId**. To specify the subscription, use parameter **SubscriptionId**.

2. Add role assignment at subscription. The **ArtifactFile** defines the *kind* of artifact, the properties align to the role definition identifier, and the principal identities are passed as an array of values. In the following example, the principal identities granted the specified role are configured to a parameter that is set during blueprint assignment. This example uses the *Contributor* built-in role with a GUID of

```
b24988ac-6180-42a0-ab88-20f7382dd24c .
```

- JSON file - \artifacts\roleContributor.json

```
{
  "kind": "roleAssignment",
  "properties": {
    "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c",
    "principalIds": "[parameters('contributors')]"
  }
}
```

- PowerShell command

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintArtifact -Blueprint $blueprint -Name 'roleContributor' -ArtifactFile
.\artifacts\roleContributor.json
```

3. Add policy assignment at subscription. The **ArtifactFile** defines the *kind* of artifact, the properties that align to a policy or initiative definition, and configures the policy assignment to use the defined blueprint parameters to configure during blueprint assignment. This example uses the *Apply tag and its default value to resource groups* built-in policy with a GUID of

```
49c88fc8-6fd1-46fd-a676-f12d1d3a4c71
```

 .

- JSON file - \artifacts\policyTags.json

```
{
  "kind": "policyAssignment",
  "properties": {
    "displayName": "Apply tag and its default value to resource groups",
    "description": "Apply tag and its default value to resource groups",
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-6fd1-46fd-a676-f12d1d3a4c71",
    "parameters": {
      "tagName": {
        "value": "[parameters('tagName')]"
      },
      "tagValue": {
        "value": "[parameters('tagValue')]"
      }
    }
  }
}
```

- PowerShell command

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintArtifact -Blueprint $blueprint -Name 'policyTags' -ArtifactFile
.\artifacts\policyTags.json
```

4. Add another policy assignment for Storage tag (reusing *storageAccountType* parameter) at subscription. This additional policy assignment artifact demonstrates that a parameter defined on the blueprint is usable by more than one artifact. In the example, the **storageAccountType** is used to set a tag on the resource group. This value provides information about the storage account that is created in the next step. This example uses the *Apply tag and its default value to resource groups* built-in policy with a GUID of `49c88fc8-6fd1-46fd-a676-f12d1d3a4c71`.

- JSON file - \artifacts\policyStorageTags.json

```
{
  "kind": "policyAssignment",
  "properties": {
    "displayName": "Apply storage tag to resource group",
    "description": "Apply storage tag and the parameter also used by the template to resource groups",
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-6fd1-46fd-a676-f12d1d3a4c71",
    "parameters": {
      "tagName": {
        "value": "StorageType"
      },
      "tagValue": {
        "value": "[parameters('storageAccountType')]"
      }
    }
  }
}
```

- PowerShell command

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintArtifact -Blueprint $blueprint -Name 'policyStorageTags' -ArtifactFile
.\artifacts\policyStorageTags.json
```

5. Add template under resource group. The **TemplateFile** for an ARM template includes the normal JSON

component of the template. The template also reuses the **storageAccountType**, **tagName**, and **tagValue** blueprint parameters by passing each to the template. The blueprint parameters are available to the template by using parameter **TemplateParameterFile** and inside the template JSON that key-value pair is used to inject the value. The blueprint and template parameter names could be the same.

- JSON ARM template file - \artifacts\templateStorage.json

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "storageAccountTypeFromBP": {
      "type": "string",
      "metadata": {
        "description": "Storage Account type"
      }
    },
    "tagNameFromBP": {
      "type": "string",
      "defaultValue": "NotSet",
      "metadata": {
        "description": "Tag name from blueprint"
      }
    },
    "tagValueFromBP": {
      "type": "string",
      "defaultValue": "NotSet",
      "metadata": {
        "description": "Tag value from blueprint"
      }
    }
  },
  "variables": {
    "storageAccountName": "[concat(uniquestring(resourceGroup().id), 'standardsa')]"
  },
  "resources": [{
    "type": "Microsoft.Storage/storageAccounts",
    "name": "[variables('storageAccountName')]",
    "apiVersion": "2016-01-01",
    "tags": {
      "[parameters('tagNameFromBP')]": "[parameters('tagValueFromBP')]"
    },
    "location": "[resourceGroup().location]",
    "sku": {
      "name": "[parameters('storageAccountTypeFromBP')]"
    },
    "kind": "Storage",
    "properties": {}
  }],
  "outputs": {
    "storageAccountSku": {
      "type": "string",
      "value": "[variables('storageAccountName')]"
    }
  }
}
```

- JSON ARM template parameter file - \artifacts\templateStorageParams.json


```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "storageAccountTypeFromBP": {
      "value": "[parameters('storageAccountType')]"
    },
    "tagNameFromBP": {
      "value": "[parameters('tagName')]"
    },
    "tagValueFromBP": {
      "value": "[parameters('tagValue')]"
    }
  }
}
```

- PowerShell command

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintArtifact -Blueprint $blueprint -Type TemplateArtifact -Name 'templateStorage' -
TemplateFile .\artifacts\templateStorage.json -TemplateParameterFile
.\artifacts\templateStorageParams.json -ResourceGroupName storageRG
```

6. Add role assignment under resource group. Similar to the previous role assignment entry, the example below uses the definition identifier for the **Owner** role and provides it a different parameter from the blueprint. This example uses the *Owner* built-in role with a GUID of

```
8e3af657-a8ff-443c-a75c-2fe8c4bcb635 .
```

- JSON file - \artifacts\roleOwner.json

```
{
  "kind": "roleAssignment",
  "properties": {
    "resourceGroup": "storageRG",
    "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
    "principalIds": "[parameters('owners')]"
  }
}
```

- PowerShell command

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintArtifact -Blueprint $blueprint -Name 'roleOwner' -ArtifactFile
.\artifacts\roleOwner.json
```

Publish a blueprint

Now that the artifacts have been added to the blueprint, it's time to publish it. Publishing makes it available to assign to a subscription.

```
# Use the reference to the new blueprint object from the previous steps
Publish-AzBlueprint -Blueprint $blueprint -Version '{BlueprintVersion}'
```

The value for `{BlueprintVersion}` is a string of letters, numbers, and hyphens (no spaces or other special

characters) with a max length of 20 characters. Use something unique and informational such as v20180622-135541.

Assign a blueprint

Once a blueprint is published using PowerShell, it's assignable to a subscription. Assign the blueprint you created to one of the subscriptions under your management group hierarchy. If the blueprint is saved to a subscription, it can only be assigned to that subscription. The **Blueprint** parameter specifies the blueprint to assign. To provide name, location, identity, lock, and blueprint parameters, use the matching PowerShell parameters on the `New-AzBlueprintAssignment` cmdlet or provide them in the **AssignmentFile** parameter JSON file.

1. Run the blueprint deployment by assigning it to a subscription. As the **contributors** and **owners** parameters require an array of objectIds of the principals to be granted the role assignment, use [Azure Active Directory Graph API](#) for gathering the objectIds for use in the **AssignmentFile** for your own users, groups, or service principals.

- JSON file - blueprintAssignment.json

```
{
  "properties": {
    "blueprintId":
"/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint",
    "resourceGroups": {
      "storageRG": {
        "name": "StorageAccount",
        "location": "eastus2"
      }
    },
    "parameters": {
      "storageAccountType": {
        "value": "Standard_GRS"
      },
      "tagName": {
        "value": "CostCenter"
      },
      "tagValue": {
        "value": "ContosoIT"
      },
      "contributors": {
        "value": [
          "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
          "38833b56-194d-420b-90ce-cff578296714"
        ]
      },
      "owners": {
        "value": [
          "44254d2b-a0c7-405f-959c-f829ee31c2e7",
          "316deb5f-7187-4512-9dd4-21e7798b0ef9"
        ]
      }
    }
  },
  "identity": {
    "type": "systemAssigned"
  },
  "location": "westus"
}
```

- PowerShell command

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintAssignment -Blueprint $blueprint -Name 'assignMyBlueprint' -AssignmentFile
.\blueprintAssignment.json
```

- User-assigned managed identity

A blueprint assignment can also use a [user-assigned managed identity](#). In this case, the **identity** portion of the JSON assignment file changes as follows. Replace `{tenantId}`, `{subscriptionId}`, `{yourRG}`, and `{userIdentity}` with your tenantId, subscriptionId, resource group name, and the name of your user-assigned managed identity, respectively.

```
"identity": {
  "type": "userAssigned",
  "tenantId": "{tenantId}",
  "userAssignedIdentities": {

    "/subscriptions/{subscriptionId}/resourceGroups/{yourRG}/providers/Microsoft.ManagedIdentity/u
serAssignedIdentities/{userIdentity}": {}
  }
},
```

The **user-assigned managed identity** can be in any subscription and resource group the user assigning the blueprint has permissions to.

IMPORTANT

Azure Blueprints doesn't manage the user-assigned managed identity. Users are responsible for assigning sufficient roles and permissions or the blueprint assignment will fail.

Clean up resources

Unassign a blueprint

You can remove a blueprint from a subscription. Removal is often done when the artifact resources are no longer needed. When a blueprint is removed, the artifacts assigned as part of that blueprint are left behind. To remove a blueprint assignment, use the `Remove-AzBlueprintAssignment` cmdlet:

assignMyBlueprint

```
Remove-AzBlueprintAssignment -Name 'assignMyBlueprint'
```

Next steps

In this quickstart, you've created, assigned, and removed a blueprint with PowerShell. To learn more about Azure Blueprints, continue to the [blueprint lifecycle](#) article.

[Learn about the blueprint lifecycle](#)

Quickstart: Define and Assign an Azure Blueprint with Azure CLI

5/3/2021 • 9 minutes to read • [Edit Online](#)

Learning how to create and assign blueprints enables the definition of common patterns to develop reusable and rapidly deployable configurations based on Azure Resource Manager templates (ARM templates), policy, security, and more. In this tutorial, you learn to use Azure Blueprints to do some of the common tasks related to creating, publishing, and assigning a blueprint within your organization, such as:

Prerequisites




- If you don't have an Azure subscription, create a [free account](#) before you begin.
- If you've not used Azure Blueprints before, register the resource provider through Azure CLI with

```
az provider register --namespace Microsoft.Blueprint .
```

Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

OPTION	EXAMPLE/LINK
Select Try It in the upper-right corner of a code block. Selecting Try It doesn't automatically copy the code to Cloud Shell.	
Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser.	
Select the Cloud Shell button on the menu bar at the upper right in the Azure portal .	

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

Add the Blueprint extension

To enable Azure CLI to manage blueprint definitions and assignments, the extension must be added. This extension works wherever Azure CLI can be used, including [bash on Windows 10](#), [Cloud Shell](#) (both standalone

and inside the portal), the [Azure CLI Docker image](#), or locally installed.

1. Check that the latest Azure CLI is installed (at least 2.0.76). If it isn't yet installed, follow [these instructions](#).
2. In your Azure CLI environment of choice, import it with the following command:

```
# Add the Blueprint extension to the Azure CLI environment
az extension add --name blueprint
```

3. Validate that the extension has been installed and is the expected version (at least 0.1.0):

```
# Check the extension list (note that you may have other extensions installed)
az extension list

# Run help for extension options
az blueprint -h
```

Create a blueprint

The first step in defining a standard pattern for compliance is to compose a blueprint from the available resources. We'll create a blueprint named 'MyBlueprint' to configure role and policy assignments for the subscription. Then we'll add a resource group, an ARM template, and a role assignment on the resource group.

NOTE

When using Azure CLI, the *blueprint* object is created first. For each *artifact* to be added that has parameters, the parameters need to be defined in advance on the initial *blueprint*.

1. Create the initial *blueprint* object. The **parameters** parameter takes a JSON file that includes all of the blueprint level parameters. The parameters are set during assignment and used by the artifacts added in later steps.
 - JSON file - blueprintparms.json

```
{
  "storageAccountType": {
    "type": "string",
    "defaultValue": "Standard_LRS",
    "allowedValues": [
      "Standard_LRS",
      "Standard_GRS",
      "Standard_ZRS",
      "Premium_LRS"
    ],
    "metadata": {
      "displayName": "storage account type.",
      "description": null
    }
  },
  "tagName": {
    "type": "string",
    "metadata": {
      "displayName": "The name of the tag to provide the policy assignment.",
      "description": null
    }
  },
  "tagValue": {
    "type": "string",
    "metadata": {
      "displayName": "The value of the tag to provide the policy assignment.",
      "description": null
    }
  },
  "contributors": {
    "type": "array",
    "metadata": {
      "description": "List of AAD object IDs that is assigned Contributor role at the subscription",
      "strongType": "PrincipalId"
    }
  },
  "owners": {
    "type": "array",
    "metadata": {
      "description": "List of AAD object IDs that is assigned Owner role at the resource group",
      "strongType": "PrincipalId"
    }
  }
}
```

- Azure CLI command

```
# Login first with az login if not using Cloud Shell

# Create the blueprint object
az blueprint create \
  --name 'MyBlueprint' \
  --description 'This blueprint sets tag policy and role assignment on the subscription, creates a ResourceGroup, and deploys a resource template and role assignment to that ResourceGroup.' \
  --parameters blueprintparms.json
```

NOTE

Use the filename *blueprint.json* when importing your blueprint definitions. This file name is used when calling `az blueprint import`.

The blueprint object is created in the default subscription by default. To specify the management group, use parameter **managementgroup**. To specify the subscription, use parameter **subscription**.

2. Add the resource group for the storage artifacts to the definition.

```
az blueprint resource-group add \  
  --blueprint-name 'MyBlueprint' \  
  --artifact-name 'storageRG' \  
  --description 'Contains the resource template deployment and a role assignment.'
```

3. Add role assignment at subscription. In the following example, the principal identities granted the specified role are configured to a parameter that is set during blueprint assignment. This example uses the *Contributor* built-in role with a GUID of `b24988ac-6180-42a0-ab88-20f7382dd24c`.

```
az blueprint artifact role create \  
  --blueprint-name 'MyBlueprint' \  
  --artifact-name 'roleContributor' \  
  --role-definition-id '/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c' \  
  --principal-ids "[parameters('contributors')]"
```

4. Add policy assignment at subscription. This example uses the *Apply tag and its default value to resource groups* built-in policy with a GUID of `49c88fc8-6fd1-46fd-a676-f12d1d3a4c71`.

- JSON file - artifacts\policyTags.json

```
{  
  "tagName": {  
    "value": "[parameters('tagName')]"  
  },  
  "tagValue": {  
    "value": "[parameters('tagValue')]"  
  }  
}
```

- Azure CLI command

```
az blueprint artifact policy create \  
  --blueprint-name 'MyBlueprint' \  
  --artifact-name 'policyTags' \  
  --policy-definition-id '/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-6fd1-46fd-a676-f12d1d3a4c71' \  
  --display-name 'Apply tag and its default value to resource groups' \  
  --description 'Apply tag and its default value to resource groups' \  
  --parameters artifacts\policyTags.json
```

NOTE

When using `az blueprint` on a Mac, replace `\` with `/` for parameter values that include the path. In this case, the value for **parameters** becomes `artifacts/policyTags.json`.

5. Add another policy assignment for Storage tag (reusing *storageAccountType* parameter) at subscription. This additional policy assignment artifact demonstrates that a parameter defined on the blueprint is usable by more than one artifact. In the example, the **storageAccountType** is used to set a tag on the resource group. This value provides information about the storage account that is created in the next step. This example uses the *Apply tag and its default value to resource groups* built-in policy with a GUID of `49c88fc8-6fd1-46fd-a676-f12d1d3a4c71`.

- JSON file - `artifacts\policyStorageTags.json`

```
{
  "tagName": {
    "value": "StorageType"
  },
  "tagValue": {
    "value": "[parameters('storageAccountType')]"
  }
}
```

- Azure CLI command

```
az blueprint artifact policy create \
  --blueprint-name 'MyBlueprint' \
  --artifact-name 'policyStorageTags' \
  --policy-definition-id '/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-6fd1-46fd-a676-f12d1d3a4c71' \
  --display-name 'Apply storage tag to resource group' \
  --description 'Apply storage tag and the parameter also used by the template to resource groups' \
  --parameters artifacts\policyStorageTags.json
```

NOTE

When using `az blueprint` on a Mac, replace `\` with `/` for parameter values that include the path. In this case, the value for **parameters** becomes `artifacts/policyStorageTags.json`.

6. Add template under resource group. The **template** parameter for an ARM template includes the normal JSON components of the template. The template also reuses the **storageAccountType**, **tagName**, and **tagValue** blueprint parameters by passing each to the template. The blueprint parameters are available to the template by using parameter **parameters** and inside the template JSON that key-value pair is used to inject the value. The blueprint and template parameter names could be the same.

- JSON ARM template file - `artifacts\templateStorage.json`


```

{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "storageAccountTypeFromBP": {
      "type": "string",
      "metadata": {
        "description": "Storage Account type"
      }
    },
    "tagNameFromBP": {
      "type": "string",
      "defaultValue": "NotSet",
      "metadata": {
        "description": "Tag name from blueprint"
      }
    },
    "tagValueFromBP": {
      "type": "string",
      "defaultValue": "NotSet",
      "metadata": {
        "description": "Tag value from blueprint"
      }
    }
  },
  "variables": {
    "storageAccountName": "[concat(uniquestring(resourceGroup().id), 'standardsa')]"
  },
  "resources": [{
    "type": "Microsoft.Storage/storageAccounts",
    "name": "[variables('storageAccountName')]",
    "apiVersion": "2016-01-01",
    "tags": {
      "[parameters('tagNameFromBP')]" : "[parameters('tagValueFromBP')]"
    },
    "location": "[resourceGroup().location]",
    "sku": {
      "name": "[parameters('storageAccountTypeFromBP')]"
    },
    "kind": "Storage",
    "properties": {}
  }],
  "outputs": {
    "storageAccountSku": {
      "type": "string",
      "value": "[variables('storageAccountName')]"
    }
  }
}

```

- JSON ARM template parameter file - artifacts\templateStorageParams.json

```

{
  "storageAccountTypeFromBP": {
    "value": "[parameters('storageAccountType')]"
  },
  "tagNameFromBP": {
    "value": "[parameters('tagName')]"
  },
  "tagValueFromBP": {
    "value": "[parameters('tagValue')]"
  }
}

```

- Azure CLI command

```
az blueprint artifact template create \  
  --blueprint-name 'MyBlueprint' \  
  --artifact-name 'templateStorage' \  
  --template artifacts\templateStorage.json \  
  --parameters artifacts\templateStorageParams.json \  
  --resource-group-art 'storageRG'
```

NOTE

When using `az blueprint` on a Mac, replace `\` with `/` for parameter values that include the path. In this case, the value for **template** becomes `artifacts/templateStorage.json` and **parameters** becomes `artifacts/templateStorageParams.json`.

7. Add role assignment under resource group. Similar to the previous role assignment entry, the example below uses the definition identifier for the **Owner** role and provides it a different parameter from the blueprint. This example uses the *Owner* built-in role with a GUID of

```
8e3af657-a8ff-443c-a75c-2fe8c4bcb635
```

```
az blueprint artifact role create \  
  --blueprint-name 'MyBlueprint' \  
  --artifact-name 'roleOwner' \  
  --role-definition-id '/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635' \  
  --principal-ids "[parameters('owners')]" \  
  --resource-group-art 'storageRG'
```

Publish a blueprint

Now that the artifacts have been added to the blueprint, it's time to publish it. Publishing makes it available to assign to a subscription.

```
az blueprint publish --blueprint-name 'MyBlueprint' --version '{BlueprintVersion}'
```

The value for `{BlueprintVersion}` is a string of letters, numbers, and hyphens (no spaces or other special characters) with a max length of 20 characters. Use something unique and informational such as `v20200605-135541`.

Assign a blueprint

Once a blueprint is published using the Azure CLI, it's assignable to a subscription. Assign the blueprint you created to one of the subscriptions under your management group hierarchy. If the blueprint is saved to a subscription, it can only be assigned to that subscription. The **blueprint-name** parameter specifies the blueprint to assign. To provide name, location, identity, lock, and blueprint parameters, use the matching Azure CLI parameters on the `az blueprint assignment create` command or provide them in the **parameters** JSON file.

1. Run the blueprint deployment by assigning it to a subscription. As the **contributors** and **owners** parameters require an array of objectIds of the principals to be granted the role assignment, use [Azure Active Directory Graph API](#) for gathering the objectIds for use in the **parameters** for your own users, groups, or service principals.

- JSON file - blueprintAssignment.json

```
{
  "storageAccountType": {
    "value": "Standard_GRS"
  },
  "tagName": {
    "value": "CostCenter"
  },
  "tagValue": {
    "value": "ContosoIT"
  },
  "contributors": {
    "value": [
      "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
      "38833b56-194d-420b-90ce-cff578296714"
    ]
  },
  "owners": {
    "value": [
      "44254d2b-a0c7-405f-959c-f829ee31c2e7",
      "316deb5f-7187-4512-9dd4-21e7798b0ef9"
    ]
  }
}
```

- Azure CLI command

```
az blueprint assignment create \
  --name 'assignMyBlueprint' \
  --location 'westus' \
  --resource-group-value artifact_name=storageRG name=StorageAccount location=eastus \
  --parameters blueprintAssignment.json
```

- User-assigned managed identity

A blueprint assignment can also use a [user-assigned managed identity](#). In this case, the **identity-type** parameter is set to *UserAssigned* and the **user-assigned-identities** parameter specifies the identity. Replace `{userIdentity}` with the name of your user-assigned managed identity.

```
az blueprint assignment create \
  --name 'assignMyBlueprint' \
  --location 'westus' \
  --identity-type UserAssigned \
  --user-assigned-identities {userIdentity} \
  --resource-group-value artifact_name=storageRG name=StorageAccount location=eastus \
  --parameters blueprintAssignment.json
```

The **user-assigned managed identity** can be in any subscription and resource group the user assigning the blueprint has permissions to.

IMPORTANT

Azure Blueprints doesn't manage the user-assigned managed identity. Users are responsible for assigning sufficient roles and permissions or the blueprint assignment will fail.

Clean up resources

Unassign a blueprint

You can remove a blueprint from a subscription. Removal is often done when the artifact resources are no longer needed. When a blueprint is removed, the artifacts assigned as part of that blueprint are left behind. To remove a blueprint assignment, use the `az blueprint assignment delete` command:

```
az blueprint assignment delete --name 'assignMyBlueprint'
```

Next steps

In this quickstart, you've created, assigned, and removed a blueprint with Azure CLI. To learn more about Azure Blueprints, continue to the [blueprint lifecycle](#) article.

[Learn about the blueprint lifecycle](#)

Quickstart: Define and Assign an Azure Blueprint with REST API

5/3/2021 • 10 minutes to read • [Edit Online](#)

Learning how to create and assign blueprints enables the definition of common patterns to develop reusable and rapidly deployable configurations based on Azure Resource Manager templates (ARM templates), policy, security, and more. In this tutorial, you learn to use Azure Blueprints to do some of the common tasks related to creating, publishing, and assigning a blueprint within your organization, such as:




Prerequisites

- If you don't have an Azure subscription, create a [free account](#) before you begin.
- Register the `Microsoft.Blueprint` resource provider. For directions, see [Resource providers and types](#).

Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

OPTION	EXAMPLE/LINK
Select Try It in the upper-right corner of a code block. Selecting Try It doesn't automatically copy the code to Cloud Shell.	
Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser.	
Select the Cloud Shell button on the menu bar at the upper right in the Azure portal .	

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

Getting started with REST API

If you're unfamiliar with REST API, start by reviewing [Azure REST API Reference](#) to get a general understanding of REST API, specifically request URI and request body. This article uses these concepts to provide directions for working with Azure Blueprints and assumes a working knowledge of them. Tools such as [ARMClient](#) and others

may handle authorization automatically and are recommended for beginners.

For the Azure Blueprints specs, see [Azure Blueprints REST API](#).

REST API and PowerShell

If you don't already have a tool for making REST API calls, consider using PowerShell for these instructions. Following is a sample header for authenticating with Azure. Generate an authentication header, sometimes called a **Bearer token**, and provide the REST API URI to connect to with any parameters or a **Request Body**:

```
# Log in first with Connect-AzAccount if not using Cloud Shell

$azContext = Get-AzContext
$azProfile =
[Microsoft.Azure.Commands.Common.Authentication.Abstractions.AzureRmProfileProvider]::Instance.Profile
$profileClient = New-Object -TypeName Microsoft.Azure.Commands.ResourceManager.Common.RMProfileClient -
ArgumentList ($azProfile)
$token = $profileClient.AcquireAccessToken($azContext.Subscription.TenantId)
$authHeader = @{
    'Content-Type'='application/json'
    'Authorization'='Bearer ' + $token.AccessToken
}

# Invoke the REST API
$restUri = 'https://management.azure.com/subscriptions/{subscriptionId}?api-version=2020-01-01'
$response = Invoke-RestMethod -Uri $restUri -Method Get -Headers $authHeader
```

Replace `{subscriptionId}` in the `$restUri` variable above to get information about your subscription. The `$response` variable holds the result of the `Invoke-RestMethod` cmdlet, which can be parsed with cmdlets such as [ConvertFrom-Json](#). If the REST API service endpoint expects a **Request Body**, provide a JSON formatted variable to the `-Body` parameter of `Invoke-RestMethod`.

Create a blueprint

The first step in defining a standard pattern for compliance is to compose a blueprint from the available resources. We'll create a blueprint named 'MyBlueprint' to configure role and policy assignments for the subscription. Then we'll add a resource group, an ARM template, and a role assignment on the resource group.

NOTE

When using the REST API, the *blueprint* object is created first. For each *artifact* to be added that has parameters, the parameters need to be defined in advance on the initial *blueprint*.

In each REST API URI, there are variables that are used that you need to replace with your own values:

- `{YourMG}` - Replace with the ID of your management group
- `{subscriptionId}` - Replace with your subscription ID

NOTE

Blueprints may also be created at the subscription level. To see an example, see [create blueprint at subscription example](#).

1. Create the initial *blueprint* object. The **Request Body** includes properties about the blueprint, any resource groups to create, and all of the blueprint level parameters. The parameters are set during assignment and used by the artifacts added in later steps.

- REST API URI

PUT

https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint?api-version=2018-11-01-preview

- Request Body

```
{
  "properties": {
    "description": "This blueprint sets tag policy and role assignment on the subscription, creates a ResourceGroup, and deploys a resource template and role assignment to that ResourceGroup.",
    "targetScope": "subscription",
    "parameters": {
      "storageAccountType": {
        "type": "string",
        "metadata": {
          "displayName": "storage account type.",
          "description": null
        }
      },
      "tagName": {
        "type": "string",
        "metadata": {
          "displayName": "The name of the tag to provide the policy assignment.",
          "description": null
        }
      },
      "tagValue": {
        "type": "string",
        "metadata": {
          "displayName": "The value of the tag to provide the policy assignment.",
          "description": null
        }
      },
      "contributors": {
        "type": "array",
        "metadata": {
          "description": "List of AAD object IDs that is assigned Contributor role at the subscription"
        }
      },
      "owners": {
        "type": "array",
        "metadata": {
          "description": "List of AAD object IDs that is assigned Owner role at the resource group"
        }
      },
      "resourceGroups": {
        "storageRG": {
          "description": "Contains the resource template deployment and a role assignment."
        }
      }
    }
  }
}
```

2. Add role assignment at subscription. The **Request Body** defines the *kind* of artifact, the properties align to the role definition identifier, and the principal identities are passed as an array of values. In the following example, the principal identities granted the specified role are configured to a parameter that is set during blueprint assignment. This example uses the *Contributor* built-in role with a GUID of

b24988ac-6180-42a0-ab88-20f7382dd24c .

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/artifacts/roleContributor?api-version=2018-11-01-preview
```

- Request Body

```
{
  "kind": "roleAssignment",
  "properties": {
    "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c",
    "principalIds": "[parameters('contributors')]"
  }
}
```

3. Add policy assignment at subscription. The **Request Body** defines the *kind* of artifact, the properties that align to a policy or initiative definition, and configures the policy assignment to use the defined blueprint parameters to configure during blueprint assignment. This example uses the *Apply tag and its default value to resource groups* built-in policy with a GUID of `49c88fc8-6fd1-46fd-a676-f12d1d3a4c71`.

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/artifacts/policyTags?api-version=2018-11-01-preview
```

- Request Body

```
{
  "kind": "policyAssignment",
  "properties": {
    "description": "Apply tag and its default value to resource groups",
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-6fd1-46fd-a676-f12d1d3a4c71",
    "parameters": {
      "tagName": {
        "value": "[parameters('tagName')]"
      },
      "tagValue": {
        "value": "[parameters('tagValue')]"
      }
    }
  }
}
```

4. Add another policy assignment for Storage tag (reusing *storageAccountType* parameter) at subscription. This additional policy assignment artifact demonstrates that a parameter defined on the blueprint is usable by more than one artifact. In the example, the **storageAccountType** is used to set a tag on the resource group. This value provides information about the storage account that is created in the next step. This example uses the *Apply tag and its default value to resource groups* built-in policy with a GUID of `49c88fc8-6fd1-46fd-a676-f12d1d3a4c71`.

- REST API URI


```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/artifacts/policyStorageTags?api-version=2018-11-01-preview
```

- Request Body

```
{
  "kind": "policyAssignment",
  "properties": {
    "description": "Apply storage tag and the parameter also used by the template to resource groups",
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-6fd1-46fd-a676-f12d1d3a4c71",
    "parameters": {
      "tagName": {
        "value": "StorageType"
      },
      "tagValue": {
        "value": "[parameters('storageAccountType')]"
      }
    }
  }
}
```

5. Add template under resource group. The **Request Body** for an ARM template includes the normal JSON component of the template and defines the target resource group with **properties.resourceGroup**. The template also reuses the **storageAccountType**, **tagName**, and **tagValue** blueprint parameters by passing each to the template. The blueprint parameters are available to the template by defining **properties.parameters** and inside the template JSON that key-value pair is used to inject the value. The blueprint and template parameter names could be the same, but were made different to illustrate how each passes from the blueprint to the template artifact.

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/artifacts/templateStorage?api-version=2018-11-01-preview
```

- Request Body

```
{
  "kind": "template",
  "properties": {
    "template": {
      "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
      "contentVersion": "1.0.0.0",
      "parameters": {
        "storageAccountTypeFromBP": {
          "type": "string",
          "defaultValue": "Standard_LRS",
          "allowedValues": [
            "Standard_LRS",
            "Standard_GRS",
            "Standard_ZRS",
            "Premium_LRS"
          ]
        },
        "metadata": {
          "description": "Storage Account type"
```

```

        description: "Storage Account type"
      }
    },
    "tagNameFromBP": {
      "type": "string",
      "defaultValue": "NotSet",
      "metadata": {
        "description": "Tag name from blueprint"
      }
    },
    "tagValueFromBP": {
      "type": "string",
      "defaultValue": "NotSet",
      "metadata": {
        "description": "Tag value from blueprint"
      }
    }
  },
  "variables": {
    "storageAccountName": "[concat(uniquestring(resourceGroup().id),
'standardsa')]"
  },
  "resources": [{
    "type": "Microsoft.Storage/storageAccounts",
    "name": "[variables('storageAccountName')]",
    "apiVersion": "2016-01-01",
    "tags": {
      "[parameters('tagNameFromBP')]" : "[parameters('tagValueFromBP')]"
    },
    "location": "[resourceGroups('storageRG').location]",
    "sku": {
      "name": "[parameters('storageAccountTypeFromBP')]"
    },
    "kind": "Storage",
    "properties": {}
  }],
  "outputs": {
    "storageAccountSku": {
      "type": "string",
      "value": "[variables('storageAccountName')]"
    }
  }
},
"resourceGroup": "storageRG",
"parameters": {
  "storageAccountTypeFromBP": {
    "value": "[parameters('storageAccountType')]"
  },
  "tagNameFromBP": {
    "value": "[parameters('tagName')]"
  },
  "tagValueFromBP": {
    "value": "[parameters('tagValue')]"
  }
}
}
}

```

6. Add role assignment under resource group. Similar to the previous role assignment entry, the example below uses the definition identifier for the **Owner** role and provides it a different parameter from the blueprint. This example uses the *Owner* built-in role with a GUID of

```
8e3af657-a8ff-443c-a75c-2fe8c4bcb635
```

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/artifacts/roleOwner?api-version=2018-11-01-preview
```

- Request Body

```
{
  "kind": "roleAssignment",
  "properties": {
    "resourceGroup": "storageRG",
    "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
    "principalIds": "[parameters('owners')]"
  }
}
```

Publish a blueprint

Now that the artifacts have been added to the blueprint, it's time to publish it. Publishing makes it available to assign to a subscription.

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/versions/{BlueprintVersion}?api-version=2018-11-01-preview
```

The value for `{BlueprintVersion}` is a string of letters, numbers, and hyphens (no spaces or other special characters) with a max length of 20 characters. Use something unique and informational such as `v20180622-135541`.

Assign a blueprint

Once a blueprint is published using REST API, it's assignable to a subscription. Assign the blueprint you created to one of the subscriptions under your management group hierarchy. If the blueprint is saved to a subscription, it can only be assigned to that subscription. The **Request Body** specifies the blueprint to assign, provides name and location to any resource groups in the blueprint definition, and provides all parameters defined on the blueprint and used by one or more attached artifacts.

In each REST API URI, there are variables that are used that you need to replace with your own values:

- `{tenantId}` - Replace with your tenant ID
- `{YourMG}` - Replace with the ID of your management group
- `{subscriptionId}` - Replace with your subscription ID

1. Provide the Azure Blueprint service principal the **Owner** role on the target subscription. The AppId is static (`f71766dc-90d9-4b7d-bd9d-4499c4331c3f`), but the service principal ID varies by tenant. Details can be requested for your tenant using the following REST API. It uses [Azure Active Directory Graph API](#), which has different authorization.

- REST API URI

```
GET https://graph.windows.net/{tenantId}/servicePrincipals?api-version=1.6&$filter=appId eq 'f71766dc-90d9-4b7d-bd9d-4499c4331c3f'
```

2. Run the blueprint deployment by assigning it to a subscription. As the **contributors** and **owners** parameters require an array of objectIds of the principals to be granted the role assignment, use [Azure Active Directory Graph API](#) for gathering the objectIds for use in the **Request Body** for your own users, groups, or service principals.

- REST API URI

```
PUT
https://management.azure.com/subscriptions/{subscriptionId}/providers/Microsoft.Blueprint/blueprintAssignments/assignMyBlueprint?api-version=2018-11-01-preview
```

- Request Body

```
{
  "properties": {
    "blueprintId":
"/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint",
    "resourceGroups": {
      "storageRG": {
        "name": "StorageAccount",
        "location": "eastus2"
      }
    },
    "parameters": {
      "storageAccountType": {
        "value": "Standard_GRS"
      },
      "tagName": {
        "value": "CostCenter"
      },
      "tagValue": {
        "value": "ContosoIT"
      },
      "contributors": {
        "value": [
          "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
          "38833b56-194d-420b-90ce-cff578296714"
        ]
      },
      "owners": {
        "value": [
          "44254d2b-a0c7-405f-959c-f829ee31c2e7",
          "316deb5f-7187-4512-9dd4-21e7798b0ef9"
        ]
      }
    }
  },
  "identity": {
    "type": "systemAssigned"
  },
  "location": "westus"
}
```

- User-assigned managed identity

A blueprint assignment can also use a [user-assigned managed identity](#). In this case, the **identity** portion of the request body changes as follows. Replace `{yourRG}` and `{userIdentity}` with your

resource group name and the name of your user-assigned managed identity, respectively.

```
"identity": {
  "type": "userAssigned",
  "tenantId": "{tenantId}",
  "userAssignedIdentities": {

"/subscriptions/{subscriptionId}/resourceGroups/{yourRG}/providers/Microsoft.ManagedIdentity/userAssignedIdentities/{userIdentity}": {}
  }
},
```

The **user-assigned managed identity** can be in any subscription and resource group the user assigning the blueprint has permissions to.

IMPORTANT

Azure Blueprints doesn't manage the user-assigned managed identity. Users are responsible for assigning sufficient roles and permissions or the blueprint assignment will fail.

Clean up resources

Unassign a blueprint

You can remove a blueprint from a subscription. Removal is often done when the artifact resources are no longer needed. When a blueprint is removed, the artifacts assigned as part of that blueprint are left behind. To remove a blueprint assignment, use the following REST API operation:

- REST API URI

```
DELETE
https://management.azure.com/subscriptions/{subscriptionId}/providers/Microsoft.Blueprint/blueprintAssignments/assignMyBlueprint?api-version=2018-11-01-preview
```

Delete a blueprint

To remove the blueprint itself, use the following REST API operation:

- REST API URI

```
DELETE
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint?api-version=2018-11-01-preview
```

Next steps

In this quickstart, you've created, assigned, and removed a blueprint with REST API. To learn more about Azure Blueprints, continue to the blueprint lifecycle article.

[Learn about the blueprint lifecycle](#)

Subscription deployments with ARM templates

5/11/2021 • 10 minutes to read • [Edit Online](#)

To simplify the management of resources, you can use an Azure Resource Manager template (ARM template) to deploy resources at the level of your Azure subscription. For example, you can deploy [policies](#) and [Azure role-based access control \(Azure RBAC\)](#) to your subscription, which applies them across your subscription. You can also create resource groups within the subscription and deploy resources to resource groups in the subscription.

NOTE

You can deploy to 800 different resource groups in a subscription level deployment.

To deploy templates at the subscription level, use Azure CLI, PowerShell, REST API, or the portal.

Supported resources

Not all resource types can be deployed to the subscription level. This section lists which resource types are supported.

For Azure Blueprints, use:

- [artifacts](#)
- [blueprints](#)
- [blueprintAssignments](#)
- [versions \(Blueprints\)](#)

For Azure Policies, use:

- [policyAssignments](#)
- [policyDefinitions](#)
- [policySetDefinitions](#)
- [remediations](#)

For Azure role-based access control (Azure RBAC), use:

- [roleAssignments](#)
- [roleDefinitions](#)

For nested templates that deploy to resource groups, use:

- [deployments](#)

For creating new resource groups, use:

- [resourceGroups](#)

For managing your subscription, use:

- [Advisor configurations](#)
- [budgets](#)
- [Change Analysis profile](#)
- [supportPlanTypes](#)

- [tags](#)

Other supported types include:

- [scopeAssignments](#)
- [eventSubscriptions](#)
- [peerAsns](#)

Schema

The schema you use for subscription-level deployments is different than the schema for resource group deployments.

For templates, use:

```
{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  ...
}
```

The schema for a parameter file is the same for all deployment scopes. For parameter files, use:

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",
  ...
}
```

Deployment commands

To deploy to a subscription, use the subscription-level deployment commands.

- [Azure CLI](#)
- [PowerShell](#)

For Azure CLI, use [az deployment sub create](#). The following example deploys a template to create a resource group:

```
az deployment sub create \
  --name demoSubDeployment \
  --location centralus \
  --template-uri "https://raw.githubusercontent.com/Azure/azure-docs-json-samples/master/azure-resource-manager/emptyRG.json" \
  --parameters rgName=demoResourceGroup rgLocation=centralus
```

For more detailed information about deployment commands and options for deploying ARM templates, see:

- [Deploy resources with ARM templates and Azure portal](#)
- [Deploy resources with ARM templates and Azure CLI](#)
- [Deploy resources with ARM templates and Azure PowerShell](#)
- [Deploy resources with ARM templates and Azure Resource Manager REST API](#)
- [Use a deployment button to deploy templates from GitHub repository](#)
- [Deploy ARM templates from Cloud Shell](#)

Deployment location and name

For subscription level deployments, you must provide a location for the deployment. The location of the deployment is separate from the location of the resources you deploy. The deployment location specifies where to store deployment data. [Management group](#) and [tenant](#) deployments also require a location. For [resource group](#) deployments, the location of the resource group is used to store the deployment data.

You can provide a name for the deployment, or use the default deployment name. The default name is the name of the template file. For example, deploying a template named *azuredeploy.json* creates a default deployment name of **azuredeploy**.

For each deployment name, the location is immutable. You can't create a deployment in one location when there's an existing deployment with the same name in a different location. For example, if you create a subscription deployment with the name **deployment1** in **centralus**, you can't later create another deployment with the name **deployment1** but a location of **westus**. If you get the error code `InvalidDeploymentLocation`, either use a different name or the same location as the previous deployment for that name.

Deployment scopes

When deploying to a subscription, you can deploy resources to:

- the target subscription from the operation
- any subscription in the tenant
- resource groups within the subscription or other subscriptions
- the tenant for the subscription

An [extension resource](#) can be scoped to a target that is different than the deployment target.

The user deploying the template must have access to the specified scope.

This section shows how to specify different scopes. You can combine these different scopes in a single template.

Scope to target subscription

To deploy resources to the target subscription, add those resources to the resources section of the template.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "resources": [
    subscription-level-resources
  ],
  "outputs": {}
}
```

For examples of deploying to the subscription, see [Create resource groups](#) and [Assign policy definition](#).

Scope to other subscription

To deploy resources to a subscription that is different than the subscription from the operation, add a nested deployment. Set the `subscriptionId` property to the ID of the subscription you want to deploy to. Set the `location` property for the nested deployment.


```
{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "resources": [
    {
      "type": "Microsoft.Resources/deployments",
      "apiVersion": "2020-06-01",
      "name": "nestedDeployment",
      "subscriptionId": "00000000-0000-0000-0000-000000000000",
      "location": "westus",
      "properties": {
        "mode": "Incremental",
        "template": {
          subscription-resources
        }
      }
    }
  ],
  "outputs": {}
}
```

Scope to resource group

To deploy resources to a resource group within the subscription, add a nested deployment and include the `resourceGroup` property. In the following example, the nested deployment targets a resource group named `demoResourceGroup`.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "resources": [
    {
      "type": "Microsoft.Resources/deployments",
      "apiVersion": "2020-06-01",
      "name": "nestedDeployment",
      "resourceGroup": "demoResourceGroup",
      "properties": {
        "mode": "Incremental",
        "template": {
          resource-group-resources
        }
      }
    }
  ],
  "outputs": {}
}
```

For an example of deploying to a resource group, see [Create resource group and resources](#).

Scope to tenant

To create resources at the tenant, set the `scope` to `/`. The user deploying the template must have the [required access to deploy at the tenant](#).

To use a nested deployment, set `scope` and `location`.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "resources": [
    {
      "type": "Microsoft.Resources/deployments",
      "apiVersion": "2020-06-01",
      "name": "nestedDeployment",
      "location": "centralus",
      "scope": "/",
      "properties": {
        "mode": "Incremental",
        "template": {
          $ref: "#/tenant-resources"
        }
      }
    }
  ],
  "outputs": {}
}
```

Or, you can set the scope to `/` for some resource types, like management groups.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "mgName": {
      "type": "string",
      "defaultValue": "[concat('mg-', uniqueString(newGuid()))]"
    }
  },
  "resources": [
    {
      "type": "Microsoft.Management/managementGroups",
      "apiVersion": "2020-05-01",
      "name": "[parameters('mgName')]",
      "scope": "/",
      "location": "eastus",
      "properties": {}
    }
  ],
  "outputs": {
    "output": {
      "type": "string",
      "value": "[parameters('mgName')]"
    }
  }
}
```

For more information, see [Management group](#).

Resource groups

Create resource groups

To create a resource group in an ARM template, define a [Microsoft.Resources/resourceGroups](#) resource with a name and location for the resource group.

The following template creates an empty resource group.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "rgName": {
      "type": "string"
    },
    "rgLocation": {
      "type": "string"
    }
  },
  "variables": {},
  "resources": [
    {
      "type": "Microsoft.Resources/resourceGroups",
      "apiVersion": "2020-10-01",
      "name": "[parameters('rgName')]",
      "location": "[parameters('rgLocation')]",
      "properties": {}
    }
  ],
  "outputs": {}
}
```

Use the [copy element](#) with resource groups to create more than one resource group.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "rgNamePrefix": {
      "type": "string"
    },
    "rgLocation": {
      "type": "string"
    },
    "instanceCount": {
      "type": "int"
    }
  },
  "variables": {},
  "resources": [
    {
      "type": "Microsoft.Resources/resourceGroups",
      "apiVersion": "2020-10-01",
      "location": "[parameters('rgLocation')]",
      "name": "[concat(parameters('rgNamePrefix'), copyIndex())]",
      "copy": {
        "name": "rgCopy",
        "count": "[parameters('instanceCount')]"
      },
      "properties": {}
    }
  ],
  "outputs": {}
}
```

For information about resource iteration, see [Resource iteration in ARM templates](#), and [Tutorial: Create multiple resource instances with ARM templates](#).

Create resource group and resources

To create the resource group and deploy resources to it, use a nested template. The nested template defines the resources to deploy to the resource group. Set the nested template as dependent on the resource group to make

sure the resource group exists before deploying the resources. You can deploy to up to 800 resource groups.

The following example creates a resource group, and deploys a storage account to the resource group.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "rgName": {
      "type": "string"
    },
    "rgLocation": {
      "type": "string"
    },
    "storagePrefix": {
      "type": "string",
      "maxLength": 11
    }
  },
  "variables": {
    "storageName": "[concat(parameters('storagePrefix'), uniqueString(subscription().id, parameters('rgName')))]"
  },
  "resources": [
    {
      "type": "Microsoft.Resources/resourceGroups",
      "apiVersion": "2020-10-01",
      "name": "[parameters('rgName')]",
      "location": "[parameters('rgLocation')]",
      "properties": {}
    },
    {
      "type": "Microsoft.Resources/deployments",
      "apiVersion": "2020-10-01",
      "name": "storageDeployment",
      "resourceGroup": "[parameters('rgName')]",
      "dependsOn": [
        "[resourceId('Microsoft.Resources/resourceGroups/', parameters('rgName'))]"
      ],
      "properties": {
        "mode": "Incremental",
        "template": {
          "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
          "contentVersion": "1.0.0.0",
          "parameters": {},
          "variables": {},
          "resources": [
            {
              "type": "Microsoft.Storage/storageAccounts",
              "apiVersion": "2019-06-01",
              "name": "[variables('storageName')]",
              "location": "[parameters('rgLocation')]",
              "sku": {
                "name": "Standard_LRS"
              },
              "kind": "StorageV2"
            }
          ],
          "outputs": {}
        }
      }
    }
  ],
  "outputs": {}
}
```

Azure Policy

Assign policy definition

The following example assigns an existing policy definition to the subscription. If the policy definition takes parameters, provide them as an object. If the policy definition doesn't take parameters, use the default empty object.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "policyDefinitionID": {
      "type": "string"
    },
    "policyName": {
      "type": "string"
    },
    "policyParameters": {
      "type": "object",
      "defaultValue": {}
    }
  },
  "variables": {},
  "resources": [
    {
      "type": "Microsoft.Authorization/policyAssignments",
      "apiVersion": "2018-03-01",
      "name": "[parameters('policyName')]",
      "properties": {
        "scope": "[subscription().id]",
        "policyDefinitionId": "[parameters('policyDefinitionID')]",
        "parameters": "[parameters('policyParameters')]"
      }
    }
  ]
}
```

To deploy this template with Azure CLI, use:

```
# Built-in policy definition that accepts parameters
definition=$(az policy definition list --query "[?displayName=='Allowed locations'].id" --output tsv)

az deployment sub create \
  --name demoDeployment \
  --location centralus \
  --template-uri "https://raw.githubusercontent.com/Azure/azure-docs-json-samples/master/azure-resource-manager/policyassign.json" \
  --parameters policyDefinitionID=$definition policyName=setLocation policyParameters="{
    'listOfAllowedLocations': {
      'value': ['westus']
    }
  }"
```

To deploy this template with PowerShell, use:

```

$definition = Get-AzPolicyDefinition | Where-Object { $_.Properties.DisplayName -eq 'Allowed locations' }

$locations = @("westus", "westus2")
$policyParams = @{listOfAllowedLocations = @{ value = $locations}}

New-AzSubscriptionDeployment `
  -Name policyassign `
  -Location centralus `
  -TemplateUri "https://raw.githubusercontent.com/Azure/azure-docs-json-samples/master/azure-resource-
manager/policyassign.json" `
  -policyDefinitionID $definition.PolicyDefinitionId `
  -policyName setLocation `
  -policyParameters $policyParams

```

Create and assign policy definitions

You can [define](#) and assign a policy definition in the same template.

```

{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {},
  "variables": {},
  "resources": [
    {
      "type": "Microsoft.Authorization/policyDefinitions",
      "apiVersion": "2018-05-01",
      "name": "locationpolicy",
      "properties": {
        "policyType": "Custom",
        "parameters": {},
        "policyRule": {
          "if": {
            "field": "location",
            "equals": "northeurope"
          },
          "then": {
            "effect": "deny"
          }
        }
      }
    },
    {
      "type": "Microsoft.Authorization/policyAssignments",
      "apiVersion": "2018-05-01",
      "name": "location-lock",
      "dependsOn": [
        "locationpolicy"
      ],
      "properties": {
        "scope": "[subscription().id]",
        "policyDefinitionId": "[subscriptionResourceId('Microsoft.Authorization/policyDefinitions',
'locationpolicy')]"
      }
    }
  ]
}

```

To create the policy definition in your subscription, and assign it to the subscription, use the following CLI command:

```
az deployment sub create \  
  --name demoDeployment \  
  --location centralus \  
  --template-uri "https://raw.githubusercontent.com/Azure/azure-docs-json-samples/master/azure-resource-manager/policydefineandassign.json"
```

To deploy this template with PowerShell, use:

```
New-AzSubscriptionDeployment `\  
  -Name definePolicy `\  
  -Location centralus `\  
  -TemplateUri "https://raw.githubusercontent.com/Azure/azure-docs-json-samples/master/azure-resource-manager/policydefineandassign.json"
```

Azure Blueprints

Create blueprint definition

You can [create](#) a blueprint definition from a template.

```

{
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "blueprintName": {
      "defaultValue": "sample-blueprint",
      "type": "String",
      "metadata": {
        "description": "The name of the blueprint definition."
      }
    }
  },
  "resources": [
    {
      "type": "Microsoft.Blueprint/blueprints",
      "apiVersion": "2018-11-01-preview",
      "name": "[parameters('blueprintName')]",
      "properties": {
        "targetScope": "subscription",
        "description": "Blueprint with a policy assignment artifact.",
        "resourceGroups": {
          "sampleRg": {
            "description": "Resource group to add the assignment to."
          }
        },
        "parameters": {
          "listOfResourceTypesNotAllowed": {
            "type": "array",
            "metadata": {
              "displayName": "Resource types to pass to the policy assignment artifact."
            },
            "defaultValue": [
              "Citrix.Cloud/accounts"
            ]
          }
        }
      },
    },
    {
      "type": "Microsoft.Blueprint/blueprints/artifacts",
      "apiVersion": "2018-11-01-preview",
      "name": "[concat(parameters('blueprintName'), '/policyArtifact')]",
      "kind": "policyAssignment",
      "dependsOn": [
        "[parameters('blueprintName')]"
      ],
      "properties": {
        "displayName": "Blocked Resource Types policy definition",
        "description": "Block certain resource types",
        "policyDefinitionId": "[tenantResourceId('Microsoft.Authorization/policyDefinitions', '6c112d4e-5bc7-47ae-a041-ea2d9dccc749')]",
        "resourceGroup": "sampleRg",
        "parameters": {
          "listOfResourceTypesNotAllowed": {
            "value": "[parameters('listOfResourceTypesNotAllowed')]"
          }
        }
      },
    }
  ]
}

```

To create the blueprint definition in your subscription, use the following CLI command:


```
az deployment sub create \  
  --name demoDeployment \  
  --location centralus \  
  --template-uri "https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/subscription-deployments/blueprints-new-blueprint/azuredeploy.json"
```

To deploy this template with PowerShell, use:

```
New-AzSubscriptionDeployment `\  
  -Name demoDeployment `\  
  -Location centralus `\  
  -TemplateUri "https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/subscription-deployments/blueprints-new-blueprint/azuredeploy.json"
```

Access control

To learn about assigning roles, see [Add Azure role assignments using Azure Resource Manager templates](#).

The following example creates a resource group, applies a lock to it, and assigns a role to a principal.

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",  
  "contentVersion": "1.0.0.0",  
  "parameters": {  
    "rgName": {  
      "type": "string",  
      "metadata": {  
        "description": "Name of the resourceGroup to create"  
      }  
    },  
    "rgLocation": {  
      "type": "string",  
      "metadata": {  
        "description": "Location for the resourceGroup"  
      }  
    },  
    "principalId": {  
      "type": "string",  
      "metadata": {  
        "description": "principalId of the user that will be given contributor access to the resourceGroup"  
      }  
    },  
    "roleDefinitionId": {  
      "type": "string",  
      "defaultValue": "b24988ac-6180-42a0-ab88-20f7382dd24c",  
      "metadata": {  
        "description": "roleDefinition to apply to the resourceGroup - default is contributor"  
      }  
    },  
    "roleAssignmentName": {  
      "type": "string",  
      "defaultValue": "[guid(parameters('principalId'), parameters('roleDefinitionId'),  
parameters('rgName'))]",  
      "metadata": {  
        "description": "Unique name for the roleAssignment in the format of a guid"  
      }  
    }  
  },  
  "variables": { },  
  "resources": [  
    {  
      "type": "Microsoft.Resources/resourceGroups",  
      "apiVersion": "2019-10-01",
```

```

    "name": "[parameters('rgName')]",
    "location": "[parameters('rgLocation')]",
    "tags": {
      "Note": "subscription level deployment"
    },
    "properties": {}
  },
  {
    "type": "Microsoft.Resources/deployments",
    "apiVersion": "2019-10-01",
    "name": "applyLock",
    "resourceGroup": "[parameters('rgName')]",
    "dependsOn": [
      "[parameters('rgName')]"
    ],
    "properties": {
      "mode": "Incremental",
      "template": {
        "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
        "contentVersion": "1.0.0.0",
        "resources": [
          {
            "type": "Microsoft.Authorization/locks",
            "apiVersion": "2017-04-01",
            "name": "DontDelete",
            "properties": {
              "level": "CanNotDelete",
              "notes": "Prevent deletion of the resourceGroup"
            }
          },
          {
            "type": "Microsoft.Authorization/roleAssignments",
            "apiVersion": "2020-04-01-preview",
            "name": "[guid(parameters('roleAssignmentName'))]",
            "properties": {
              "roleDefinitionId": "[subscriptionResourceId('Microsoft.Authorization/roleDefinitions',
parameters('roleDefinitionId'))]",
              "principalId": "[parameters('principalId')]",
              "scope": "[subscriptionResourceId('Microsoft.Resources/resourceGroups',
parameters('rgName'))]"
            }
          }
        ]
      }
    }
  }
]
}

```

Next steps

- For an example of deploying workspace settings for Azure Security Center, see [deployASCwithWorkspaceSettings.json](#).
- Sample templates can be found at [GitHub](#).
- You can also deploy templates at [management group level](#) and [tenant level](#).

Tutorial: Create an environment from a blueprint sample

5/3/2021 • 9 minutes to read • [Edit Online](#)

Sample blueprints provide examples of what can be done using Azure Blueprints. Each is a sample with a specific intent or purpose, but doesn't create a complete environment by themselves. Each is intended as a starting place to explore using Azure Blueprints with various combinations of included artifacts, designs, and parameters.

The following tutorial uses the **Resource Groups with RBAC** blueprint sample to showcase different aspects of the Azure Blueprints service. The following steps are covered:

- Create a new blueprint definition from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription
- Inspect deployed resources for the assignment
- Unassign the blueprint to remove the locks

Prerequisites

To complete this tutorial, an Azure subscription is needed. If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint definition from sample

First, implement the blueprint sample. Importing creates a new blueprint in your environment based on the sample.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **Resource Groups with RBAC** blueprint sample under *Other Samples* and select it.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the blueprint sample. For this tutorial, we'll use the name *two-rgs-with-role-assignments*.
 - **Definition location:** Use the ellipsis and select the management group or subscription to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. This sample defines two resource groups, with display names of *ProdRG* and *PreProdRG*. The final name and location of each resource group are set during blueprint assignment. The *ProdRG* resource group is assigned the *Contributor* role and the *PreProdRG* resource group is assigned the *Owner* and *Readers* roles. The roles assigned in the definition are static, but user, app, or group that is assigned the role is set during blueprint assignment.
7. Select **Save Draft** when you've finished reviewing the blueprint sample.

This step creates a copy of the sample blueprint definition in the selected management group or subscription. The saved blueprint definition is managed like any blueprint created from scratch. You may save the sample to

your management group or subscription as many times as needed. However, each copy must be provided a unique name.

Once the **Saving blueprint definition succeeded** portal notification appears, move to the next step.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs. For this tutorial, we won't make any changes.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find the *two-rgs-with-role-assignments* blueprint definition and then select it.
3. Select **Publish blueprint** at the top of the page. In the new pane on the right, provide **Version** as *1.0* for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the resource groups with RBAC blueprint sample." Then select **Publish** at the bottom of the page.

This step makes it possible to assign the blueprint to a subscription. Once published, changes can still be made. Additional changes require publishing with a new **Version** value to track differences between different versions of the same blueprint definition.

Once the **Publishing blueprint definition succeeded** portal notification appears, move to the next step.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find the *two-rgs-with-role-assignments* blueprint definition and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint definition.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#). For this tutorial, select *East US 2*.
 - **Blueprint definition version**: Pick the **Published** version *1.0* of your copy of the sample blueprint definition.
 - Lock Assignment

Select the *Read Only* blueprint lock mode. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *System assigned* option. For more information, see [managed identities](#).

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For each artifact, set the parameter value to what is defined in the **Value** column. For `{Your ID}`, select your Azure user account.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	VALUE	DESCRIPTION
ProdRG resource group	Resource group	Name	ProductionRG	Defines the name of the first resource group.
ProdRG resource group	Resource group	Location	West US 2	Sets the location of the first resource group.
Contributor	Role assignment	User or Group	{Your ID}	Defines which user or group to grant the <i>Contributor</i> role assignment within the first resource group.
PreProdRG resource group	Resource group	Name	PreProductionRG	Defines the name of the second resource group.
PreProdRG resource group	Resource group	Location	West US	Sets the location of the second resource group.
Owner	Role assignment	User or Group	{Your ID}	Defines which user or group to grant the <i>Owner</i> role assignment within the second resource group.
Readers	Role assignment	User or Group	{Your ID}	Defines which user or group to grant the <i>Readers</i> role assignment within the second resource group.

5. Once all parameters have been entered, select **Assign** at the bottom of the page.

This step deploys the defined resources and configures the selected **Lock Assignment**. Blueprint locks can take up to 30 minutes to apply.

Once the **Assigning blueprint definition succeeded** portal notification appears, move to the next step.

Inspect resources deployed by the assignment

The blueprint assignment creates and tracks the artifacts defined in the blueprint definition. We can see the status of the resources from the blueprint assignment page and by looking at the resources directly.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Assigned blueprints** page on the left. Use the filters to find the *Assignment-two-rgs-with-role-assignments* blueprint assignment and then select it.

From this page, we can see the assignment succeeded and the list of created resources along with their blueprint lock state. If the assignment is updated, the **Assignment operation** dropdown list shows details about the deployment of each definition version. Each listed resource that was created can be selected and opens that resources property page.

3. Select the **ProductionRG** resource group.

We see that the name of the resource group is **ProductionRG** and not the artifact display name *ProdRG*. This name matches the value set during the blueprint assignment.

4. Select the **Access control (IAM)** page on the left and then the **Role assignments** tab.

Here we see that your account has been granted the *Contributor* role on the scope of *This resource*. The *Assignment-two-rgs-with-role-assignments* blueprint assignment has the *Owner* role as it was used to create the resource group. These permissions are also used to manage resources with configured blueprint locks.

5. From the Azure portal breadcrumb, select **Assignment-two-rgs-with-role-assignments** to go back one page, then select the **PreProductionRG** resource group.

6. Select the **Access control (IAM)** page on the left and then the **Role assignments** tab.

Here we see that your account has been granted both the *Owner* and *Reader* roles, both on the scope of *This resource*. The blueprint assignment also has the *Owner* role like the first resource group.

7. Select the **Deny assignments** tab.

The blueprint assignment created a [deny assignment](#) on the deployed resource group to enforce the *Read Only* blueprint lock mode. The deny assignment prevents someone with appropriate rights on the *Role assignments* tab from taking specific actions. The deny assignment affects *All principals*.

8. Select the deny assignment, then select the **Denied Permissions** page on the left.

The deny assignment is preventing all operations with the *** and **Action** configuration, but allows read access by excluding **/read* via **NotActions**.

9. From the Azure portal breadcrumb, select **PreProductionRG - Access control (IAM)**. Then select the **Overview** page on the left and then the **Delete resource group** button. Enter the name *PreProductionRG* to confirm the delete and select **Delete** at the bottom of the pane.

The portal notification **Delete resource group PreProductionRG failed** is displayed. The error states that while your account has permission to delete the resource group, access is denied by the blueprint assignment. Remember that we selected the *Read Only* blueprint lock mode during blueprint assignment. The blueprint lock prevents an account with permission, even *Owner*, from deleting the resource. For more information, see [blueprints resource locking](#).

These steps show that our resources were created as defined and the blueprint locks prevented unwanted deletion, even from an account with permission.

Unassign the blueprint

The last step is to remove the assignment of the blueprint and the resources that it deployed. Removing the

assignment doesn't remove the deployed artifacts.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Assigned blueprints** page on the left. Use the filters to find the *Assignment-two-rgs-with-role-assignments* blueprint assignment and then select it.
3. Select the **Unassign blueprint** button at the top of the page. Read the warning in the confirmation dialog, then select **OK**.

With the blueprint assignment removed, the blueprint locks are also removed. The created resources can once again be deleted by an account with permissions.

4. Select **Resource groups** from the Azure menu, then select **ProductionRG**.
5. Select the **Access control (IAM)** page on the left and then the **Role assignments** tab.

The security for each resource group still has the deployed role assignments, but the blueprint assignment no longer has *Owner* access.

Once the **Removing blueprint assignment succeeded** portal notification appears, move to the next step.

Clean up resources

When finished with this tutorial, delete the following resources:

- Resource group *ProductionRG*
- Resource group *PreProductionRG*
- Blueprint definition *two-rgs-with-role-assignments*

Next steps

In this tutorial, you've learned how to create a new blueprint from a sample definition. To learn more about Azure Blueprints, continue to the blueprint lifecycle article.

[Learn about the blueprint lifecycle](#)

Tutorial: Protect new resources with Azure Blueprints resource locks

5/3/2021 • 8 minutes to read • [Edit Online](#)

With Azure Blueprints [resource locks](#), you can protect newly deployed resources from being tampered with, even by an account with the *Owner* role. You can add this protection in the blueprint definitions of resources created by an Azure Resource Manager template (ARM template) artifact. The Blueprint resource lock is set during blueprint assignment.

In this tutorial, you'll complete these steps:

- Create a blueprint definition
- Mark your blueprint definition as **Published**
- Assign your blueprint definition to an existing subscription (**set resource locks**)
- Inspect the new resource group
- Unassign the blueprint to remove the locks

Prerequisites

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create a blueprint definition

First, create the blueprint definition.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. On the **Getting started** page on the left, select **Create** under **Create a blueprint**.
3. Find the **Blank Blueprint** blueprint sample at the top of the page. Select **Start with blank blueprint**.
4. Enter this information on the **Basics** tab:
 - **Blueprint name**: Provide a name for your copy of the blueprint sample. For this tutorial, we'll use the name **locked-storageaccount**.
 - **Blueprint description**: Add a description for the blueprint definition. Use **For testing blueprint resource locking on deployed resources**.
 - **Definition location**: Select the ellipsis button (...) and then select the management group or subscription to save your blueprint definition to.
5. Select the **Artifacts** tab at the top of the page, or select **Next: Artifacts** at the bottom of the page.
6. Add a resource group at the subscription level:
 - a. Select the **Add artifact** row under **Subscription**.
 - b. Select **Resource Group** under **Artifact type**.
 - c. Set the **Artifact display name** to **RGtoLock**.
 - d. Leave the **Resource Group Name** and **Location** boxes blank, but make sure the check box is selected on each property to make them **dynamic parameters**.
 - e. Select **Add** to add the artifact to the blueprint.
7. Add a template under the resource group:

- a. Select the **Add artifact** row under the **RGtoLock** entry.
- b. Select **Azure Resource Manager template** under **Artifact type**, set **Artifact display name** to **StorageAccount**, and leave **Description** blank.
- c. On the **Template** tab, paste the following ARM template into the editor box. After you paste in the template, select **Add** to add the artifact to the blueprint.

NOTE

This step defines the resources to be deployed that get locked by the Blueprint resource lock, but doesn't include the Blueprint resource locks. Blueprint resource locks are set as a parameter of the blueprint assignment.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "storageAccountType": {
      "type": "string",
      "defaultValue": "Standard_LRS",
      "allowedValues": [
        "Standard_LRS",
        "Standard_GRS",
        "Standard_ZRS",
        "Premium_LRS"
      ],
      "metadata": {
        "description": "Storage Account type"
      }
    }
  },
  "variables": {
    "storageAccountName": "[concat('store', uniquestring(resourceGroup().id))]"
  },
  "resources": [{
    "type": "Microsoft.Storage/storageAccounts",
    "name": "[variables('storageAccountName')]",
    "location": "[resourceGroup().location]",
    "apiVersion": "2018-07-01",
    "sku": {
      "name": "[parameters('storageAccountType')]"
    },
    "kind": "StorageV2",
    "properties": {}
  }],
  "outputs": {
    "storageAccountName": {
      "type": "string",
      "value": "[variables('storageAccountName')]"
    }
  }
}
```

8. Select **Save Draft** at the bottom of the page.

This step creates the blueprint definition in the selected management group or subscription.

After the **Saving blueprint definition succeeded** portal notification appears, go to the next step.

Publish the blueprint definition

Your blueprint definition has now been created in your environment. It's created in **Draft** mode and must be published before it can be assigned and deployed.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find the **locked-storageaccount** blueprint definition, and then select it.
3. Select **Publish blueprint** at the top of the page. In the new pane on the right, enter **1.0** as the **Version**. This property is useful if you make a change later. Enter **Change notes**, such as **First version published for locking blueprint deployed resources**. Then select **Publish** at the bottom of the page.

This step makes it possible to assign the blueprint to a subscription. After the blueprint definition is published, you can still make changes. If you make changes, you need to publish the definition with a new version value to track differences between versions of the same blueprint definition.

After the **Publishing blueprint definition succeeded** portal notification appears, go to the next step.

Assign the blueprint definition

After the blueprint definition is published, you can assign it to a subscription within the management group where you saved it. In this step, you provide parameters to make each deployment of the blueprint definition unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find the **locked-storageaccount** blueprint definition, and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:

- **Basics**

- **Subscriptions:** Select one or more of the subscriptions that are in the management group where you saved your blueprint definition. If you select more than one subscription, an assignment will be created for each subscription, using the parameters you enter.
- **Assignment name:** The name is pre-populated based on the name of the blueprint definition. We want this assignment to represent locking the new resource group, so change the assignment name to **assignment-locked-storageaccount-TestingBPLocks**.
- **Location:** Select a region in which to create the managed identity. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#). For this tutorial, select **East US 2**.
- **Blueprint definition version:** Select the published version **1.0** of the blueprint definition.

- **Lock Assignment**

Select the **Read Only** blueprint lock mode. For more information, see [blueprints resource locking](#).

NOTE

This step configures the Blueprint resource lock on the newly deployed resources.

- **Managed Identity**

Use the default option: **System assigned**. For more information, see [managed identities](#).

- **Artifact parameters**

The parameters defined in this section apply to the artifact under which they're defined. These parameters are [dynamic parameters](#) because they're defined during the assignment of the blueprint. For each artifact, set the parameter value to what you see in the **Value** column.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	VALUE	DESCRIPTION
RGtoLock resource group	Resource group	Name	TestingBPLocks	Defines the name of the new resource group to apply blueprint locks to.
RGtoLock resource group	Resource group	Location	West US 2	Defines the location of the new resource group to apply blueprint locks to.
StorageAccount	Resource Manager template	storageAccountType (StorageAccount)	Standard_GRS	The storage SKU. The default value is <i>Standard_LRS</i> .

5. After you've entered all parameters, select **Assign** at the bottom of the page.

This step deploys the defined resources and configures the selected **Lock Assignment**. It can take up to 30 minutes to apply blueprint locks.

After the **Assigning blueprint definition succeeded** portal notification appears, go to the next step.

Inspect resources deployed by the assignment

The assignment creates the resource group *TestingBPLocks* and the storage account deployed by the ARM template artifact. The new resource group and the selected lock state are shown on the assignment details page.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Assigned blueprints** page on the left. Use the filters to find the **assignment-locked-storageaccount-TestingBPLocks** blueprint assignment, and then select it.

From this page, we can see that the assignment succeeded and that the resources were deployed with the new blueprint lock state. If the assignment is updated, the **Assignment operation** dropdown list shows details about the deployment of each definition version. You can select the resource group to open the property page.

3. Select the **TestingBPLocks** resource group.
4. Select the **Access control (IAM)** page on the left. Then select the **Role assignments** tab.

Here we see that the *assignment-locked-storageaccount-TestingBPLocks* blueprint assignment has the *Owner* role. It has this role because this role was used to deploy and lock the resource group.

5. Select the **Deny assignments** tab.

The blueprint assignment created a [deny assignment](#) on the deployed resource group to enforce the **Read Only** blueprint lock mode. The deny assignment prevents someone with appropriate rights on the **Role assignments** tab from taking specific actions. The deny assignment affects *All principals*.

For information about excluding a principal from a deny assignment, see [blueprints resource locking](#).

6. Select the deny assignment, and then select the **Denied Permissions** page on the left.

The deny assignment is preventing all operations with the ***** and **Action** configuration, but it allows read access by excluding ***/read** via **NotActions**.

7. In the Azure portal breadcrumb, select **TestingBPLocks - Access control (IAM)**. Then select the **Overview** page on the left and then the **Delete resource group** button. Enter the name **TestingBPLocks** to confirm the delete and then select **Delete** at the bottom of the pane.

The portal notification **Delete resource group TestingBPLocks failed** appears. The error states that although your account has permission to delete the resource group, access is denied by the blueprint assignment. Remember that we selected the **Read Only** blueprint lock mode during blueprint assignment. The blueprint lock prevents an account with permission, even *Owner*, from deleting the resource. For more information, see [blueprints resource locking](#).

These steps show that our deployed resources are now protected with blueprint locks that prevent unwanted deletion, even from an account that has permission to delete the resources.

Unassign the blueprint

The last step is to remove the assignment of the blueprint definition. Removing the assignment doesn't remove the associated artifacts.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Assigned blueprints** page on the left. Use the filters to find the **assignment-locked-storageaccount-TestingBPLocks** blueprint assignment, and then select it.
3. Select **Unassign blueprint** at the top of the page. Read the warning in the confirmation dialog box, and then select **OK**.

When the blueprint assignment is removed, the blueprint locks are also removed. The resources can once again be deleted by an account with appropriate permissions.

4. Select **Resource groups** from the Azure menu, and then select **TestingBPLocks**.
5. Select the **Access control (IAM)** page on the left and then select the **Role assignments** tab.

The security for the resource group shows that the blueprint assignment no longer has *Owner* access.

After the **Removing blueprint assignment succeeded** portal notification appears, go to the next step.

Clean up resources

When you're finished with this tutorial, delete these resources:

- Resource group *TestingBPLocks*
- Blueprint definition *locked-storageaccount*

Next steps

In this tutorial, you've learned how to protect new resources deployed with Azure Blueprints. To learn more about Azure Blueprints, continue to the [blueprint lifecycle](#) article.

[Learn about the blueprint lifecycle](#)

Azure Blueprints samples

5/4/2021 • 3 minutes to read • [Edit Online](#)

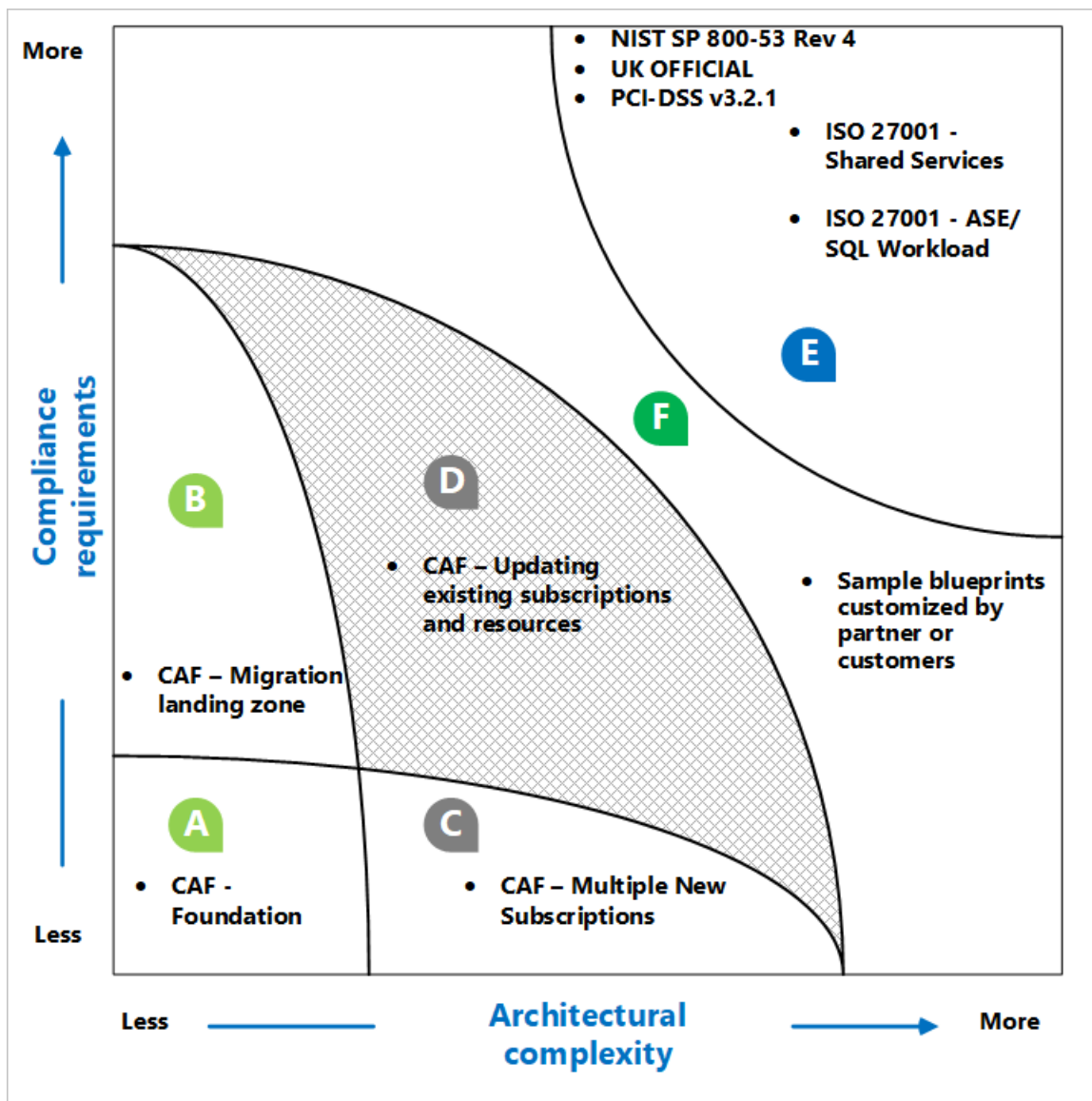
The following table includes links to samples for Azure Blueprints. Each sample is production quality and ready to deploy today to assist you in meeting your various compliance needs.

Standards-based blueprint samples

SAMPLE	DESCRIPTION
Australian Government ISM PROTECTED	Provides guardrails for compliance to Australian Government ISM PROTECTED.
Azure Security Benchmark	Provides guardrails for compliance to Azure Security Benchmark .
Azure Security Benchmark Foundation	Deploys and configures Azure Security Benchmark Foundation.
Canada Federal PBMM	Provides guardrails for compliance to Canada Federal Protected B, Medium Integrity, Medium Availability (PBMM).
CIS Microsoft Azure Foundations Benchmark v1.3.0	Provides a set of policies to help comply with CIS Microsoft Azure Foundations Benchmark v1.3.0 recommendations.
CIS Microsoft Azure Foundations Benchmark v1.1.0	Provides a set of policies to help comply with CIS Microsoft Azure Foundations Benchmark v1.1.0 recommendations.
CMMC Level 3	Provides guardrails for compliance with CMMC Level 3.
DoD Impact Level 4	Provides a set of policies to help comply with DoD Impact Level 4.
DoD Impact Level 5	Provides a set of policies to help comply with DoD Impact Level 5.
FedRAMP Moderate	Provides a set of policies to help comply with FedRAMP Moderate.
FedRAMP High	Provides a set of policies to help comply with FedRAMP High.
HIPAA HITRUST 9.2	Provides a set of policies to help comply with HIPAA HITRUST.
IRS 1075 September 2016	Provides guardrails for compliance with IRS 1075.
ISO 27001	Provides guardrails for compliance with ISO 27001.
ISO 27001 Shared Services	Provides a set of compliant infrastructure patterns and policy guardrails that help toward ISO 27001 attestation.

SAMPLE	DESCRIPTION
ISO 27001 App Service Environment/SQL Database workload	Provides more infrastructure to the ISO 27001 Shared Services blueprint sample.
Media	Provides a set of policies to help comply with Media MPAA.
New Zealand ISM Restricted	Assigns policies to address specific New Zealand Information Security Manual controls.
NIST SP 800-53 R4	Provides guardrails for compliance with NIST SP 800-53 R4.
NIST SP 800-171 R2	Provides guardrails for compliance with NIST SP 800-171 R2.
PCI-DSS v3.2.1	Provides a set of policies to aide in PCI-DSS v3.2.1 compliance.
SWIFT CSP-CSCF v2020	Aides in SWIFT CSP-CSCF v2020 compliance.
UK OFFICIAL and UK NHS Governance	Provides a set of compliant infrastructure patterns and policy guardrails that help toward UK OFFICIAL and UK NHS attestation.
CAF Foundation	Provides a set of controls to help you manage your cloud estate in alignment with the Microsoft Cloud Adoption Framework for Azure (CAF) .
CAF Migrate landing zone	Provides a set of controls to help you set up for migrating your first workload and manage your cloud estate in alignment with the Microsoft Cloud Adoption Framework for Azure (CAF) .

Samples strategy



Describes a coordinate system where architectural complexity is on the X axis and compliance requirements are on the Y axis. As architectural complexity and compliance requirements increase, adopt standard Blueprint samples from the portal designated in region E. For customers getting started with Azure use Cloud Adoption Framework (CAF) based Foundation and Landing Zone blueprints designated by region A and B. The remaining space is attributed to custom blueprints created by customers or partners for regions C, D, and F.

The CAF foundation and the CAF Migrate landing zone blueprints assume that the customer is preparing an existing clean single subscription for migrating on-premises assets and workloads into Azure. (Region A and B in the figure).

There's an opportunity to iterate on the sample blueprints and look for patterns of customizations that a customer is applying. There is also an opportunity to proactively address blueprints that are industry-specific like financial services and e-commerce (top end of Region B). Similarly, we envision building blueprints for complex architectural considerations like, multiple subscriptions, high availability, cross region resources and customers who are implementing controls over existing subscriptions and resources (Region C and D).

There are sample blueprints that address customer scenarios where the compliance requirements are high and the architectural complexities are high (Region E in the figure). Region F in the figure is one that is addressed by customers and partners who are applying the sample blueprints and customizing each for their unique needs.

Next steps

- Learn about the [blueprint lifecycle](#).

- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).

Azure Security Benchmark blueprint sample

5/3/2021 • 6 minutes to read • [Edit Online](#)

The Azure Security Benchmark blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific [Azure Security Benchmark v1](#) controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture where they intend to implement Azure Security Benchmark controls.

Control mapping

The [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **compliance domains** and **controls** in the Azure Security Benchmark. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints Azure Security Benchmark blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **Azure Security Benchmark v1** blueprint sample under *Other Samples* and select the name to select this sample.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the Azure Security Benchmark blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that are included in the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with Azure Security Benchmark recommendations.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the Azure Security Benchmark blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - Managed Identity

Leave the default *system assigned* managed identity option.
 - Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are **priced by product**. Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	List of users excluded from Windows VM Administrators group	A semicolon-separated list of members that should be excluded in the Administrators local group. Ex: Administrator; myUser1; myUser2
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	List of users that must be included in Windows VM Administrators group	A semicolon-separated list of members that should be included in the Administrators local group. Ex: Administrator; myUser1; myUser2
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	List of users that Windows VM Administrators group must <i>only</i> include	A semicolon-separated list of all the expected members of the Administrators local group. Ex: Administrator; myUser1; myUser2
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	List of regions where Network Watcher should be enabled	To see a complete list of regions use Get-AzLocation
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	Virtual network where VMs should be connected	Example: /subscriptions/YourSubscriptionId/resourceGroups/YourResourceGroupName/providers/Microsoft.Network/virtualNetworks/Name
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	Network gateway that virtual networks should use	Example: /subscriptions/YourSubscriptionId/resourceGroups/YourResourceGroup/providers/Microsoft.Network/virtualNetworkGateways/Name
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	List of workspace IDs where Log Analytics agents should connect	A semicolon-separated list of the workspace IDs that the Log Analytics agent should be connected to

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	List of resource types that should have diagnostic logs enabled	Audit diagnostic setting for selected resource types
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	Latest PHP version	Latest supported PHP version for App Services
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	Latest Java version	Latest supported Java version for App Services
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	Latest Windows Python version	Latest supported Python version for App Services
Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	Latest Linux Python version	Latest supported Python version for App Services

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

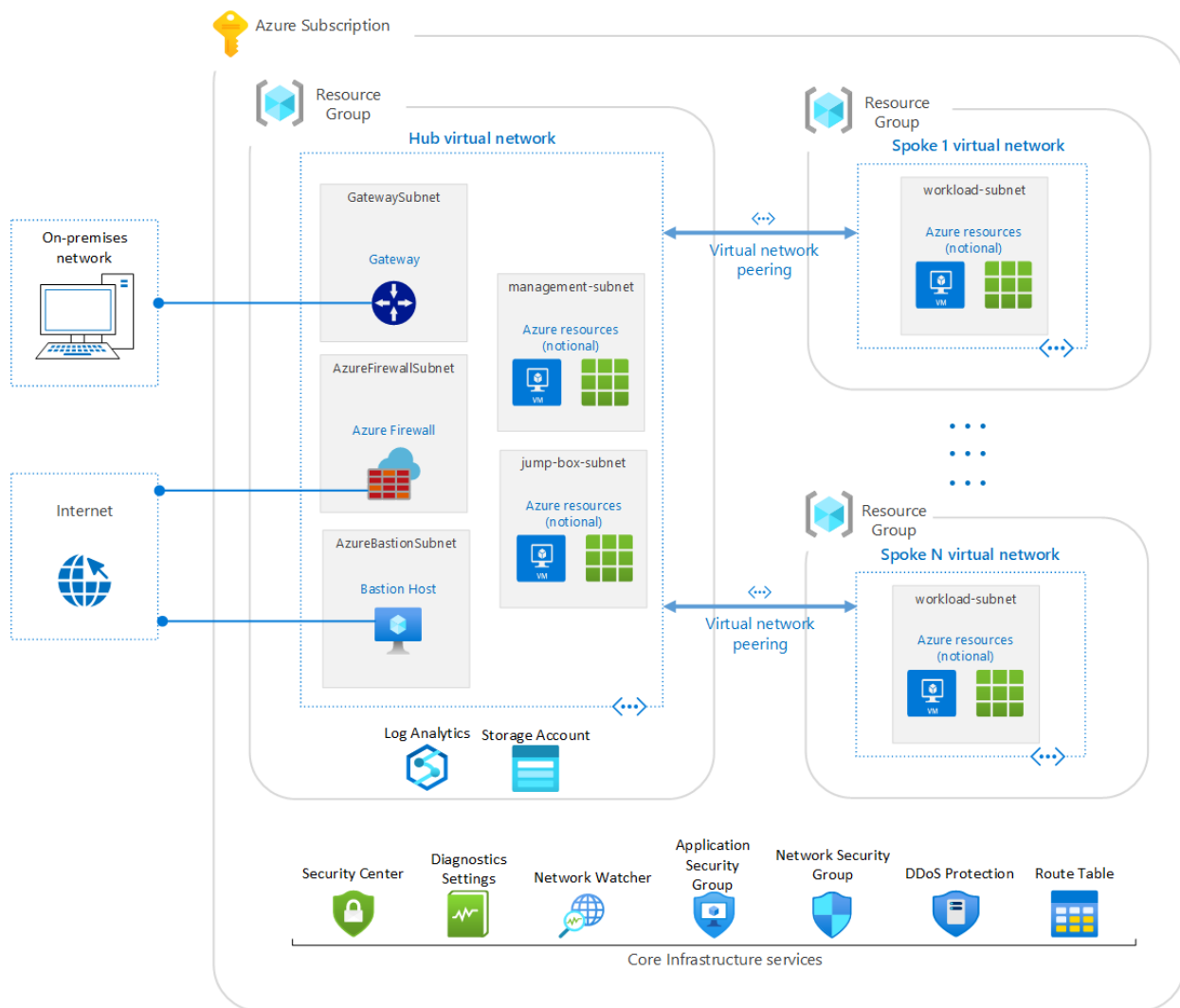
Overview of the Azure Security Benchmark Foundation blueprint sample

5/2/2021 • 3 minutes to read • [Edit Online](#)

The Azure Security Benchmark Foundation blueprint sample provides a set of baseline infrastructure patterns to help you build a secure and compliant Azure environment. The blueprint helps you deploy a cloud-based architecture that offers solutions to scenarios that have accreditation or compliance requirements. This foundational blueprint sample is an extension of the [Azure Security Benchmark sample blueprint](#). It deploys and configures network boundaries, monitoring, and other resources in alignment with the policies and other guardrails defined in the [Azure Security Benchmark](#).

Architecture

The foundational environment created by this blueprint sample is based on the architecture principals of a [hub and spoke model](#). The blueprint deploys a hub virtual network that contains common and shared resources, services, and artifacts such as Azure Bastion, gateway and firewall for connectivity, management and jump box subnets to host additional/optional management, maintenance, administration, and connectivity infrastructure. One or more spoke virtual networks are deployed to host application workloads such as web and database services. Spoke virtual networks are connected to the hub virtual network using Azure virtual network peering for seamless and secure connectivity. Additional spokes can be added by reassigning the sample blueprint or manually creating an Azure virtual network and peering it with the hub virtual network. All external connectivity to the spoke virtual network(s) and subnet(s) is configured to route through the hub virtual network and, via firewall, gateway, and management jump boxes.



This blueprint deploys several Azure services to provide a secure, monitored, enterprise-ready foundation. This environment is composed of:

- [Azure Monitor Logs](#) and an Azure storage account to ensure resource logs, activity logs, metrics, and networks traffic flows are stored in a central location for easy querying, analytics, archival, and alerting.
- [Azure Security Center](#) (standard version) to provide threat protection for Azure resources.
- [Azure Virtual Network](#) in the hub supporting subnets for connectivity back to an on-premises network, an ingress and egress stack to/from Internet connectivity, and optional subnets for deployment of additional administrative or management services. Virtual Network in the spoke contains subnets for hosting application workloads. Additional subnets can be created after deployment as needed to support applicable scenarios.
- [Azure Firewall](#) to route all outbound internet traffic and to enable inbound internet traffic via jump box. (Default firewall rules block all internet inbound and outbound traffic and rules must be configured after deployment, as applicable.)
- [Network security groups](#) (NSGs) assigned to all subnets (except service-owned subnets such as Azure Bastion, Gateway and Azure Firewall) configured to block all internet inbound and outbound traffic.
- [Application security groups](#) to enable grouping of Azure virtual machines to apply common network security policies.
- [Route tables](#) to route all outbound internet traffic from subnets through the firewall. (Azure Firewall and NSG rules will need to be configured after deployment to open connectivity.)
- [Azure Network Watcher](#) to monitor, diagnose, and view metrics of resources in the Azure virtual network.
- [Azure DDoS Protection Standard](#) to protect Azure resources against DDoS attacks.
- [Azure Bastion](#) to provide seamless and secure connectivity to a virtual machine that does not require a public IP address, agent, or special client software.

- [Azure VPN Gateway](#) to enable encrypted traffic between an Azure virtual network and an on-premises location over the public Internet.

NOTE

The Azure Security Benchmark Foundation lays out a foundational architecture for workloads. The architecture diagram above includes several notional resources to demonstrate potential use of subnets. You still need to deploy workloads on this foundational architecture.

Next steps

You've reviewed the overview and architecture of the Azure Security Benchmark Foundation blueprint sample.

[Azure Security Benchmark Foundation blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the Azure Security Benchmark Foundation blueprint sample

5/3/2021 • 8 minutes to read • [Edit Online](#)

To deploy the Azure Security Benchmark Foundation blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **Azure Security Benchmark Foundation** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the Azure Security Benchmark Foundation blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from the Azure Security Benchmark Foundation blueprint.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the Azure Security Benchmark Foundation blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in.
 - Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.

- Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Choose either the default *system assigned* managed identity option or the *user assigned* identity option.

- Blueprint parameters

The parameters defined in this section are used by many of the artifacts in the blueprint definition to provide consistency.

- **Prefix for resources and resource groups**: This string is used as a prefix for all resource and resource group names
- **Hub name**: Name for the hub
- **Log retention (days)**: Number of days that logs are retained; entering '0' retains logs indefinitely
- **Deploy hub**: Enter 'true' or 'false' to specify whether the assignment deploys the hub components of the architecture
- **Hub location**: Location for the hub resource group
- **Destination IP addresses**: Destination IP addresses for outbound connectivity; comma-separated list of IP addresses or IP range prefixes
- **Network Watcher name**: Name for the Network Watcher resource
- **Network Watcher resource group name**: Name for the Network Watcher resource group
- **Enable DDoS protection**: Enter 'true' or 'false' to specify whether or not DDoS Protection is enabled in the virtual network

NOTE

If Network Watcher is already enabled, it's recommended that you use the existing Network Watcher resource group. You must also provide the location for the existing Network Watcher resource group for the artifact parameter **Network Watcher resource group location**.

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint.

For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Hub resource group	Resource group	Resource group name	Locked - Concatenates prefix with hub name
Hub resource group	Resource group	Resource group location	Locked - Uses hub location
Azure Firewall template	Resource Manager template	Azure Firewall private IP address	
Azure Log Analytics and Diagnostics template	Resource Manager template	Log Analytics workspace location	Location where Log Analytics workspace is created; run <pre>Get-AzLocation Where-Object Providers -like 'Microsoft.OperationalInsights' Select DisplayName</pre> in Azure PowerShell to see available regions
Azure Log Analytics and Diagnostics template	Resource Manager template	Azure Automation account ID (optional)	Automation account resource ID; used to create a linked service between Log Analytics and an Automation account
Azure Network Security Group template	Resource Manager template	Enable NSG flow logs	Enter 'true' or 'false' to enable or disable NSG flow logs

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Azure Virtual Network hub template	Resource Manager template	Virtual network address prefix	Virtual network address prefix for hub virtual network
Azure Virtual Network hub template	Resource Manager template	Firewall subnet address prefix	Firewall subnet address prefix for hub virtual network
Azure Virtual Network hub template	Resource Manager template	Bastion subnet address prefix	Bastion subnet address prefix for hub virtual network
Azure Virtual Network hub template	Resource Manager template	Gateway subnet address prefix	Gateway subnet address prefix for hub virtual network
Azure Virtual Network hub template	Resource Manager template	Management subnet address prefix	Management subnet address prefix for hub virtual network
Azure Virtual Network hub template	Resource Manager template	Jump box subnet address prefix	Jump box subnet address prefix for hub virtual network
Azure Virtual Network hub template	Resource Manager template	Subnet address names (optional)	Array of subnet names to deploy to the hub virtual network; for example, "subnet1","subnet2"
Azure Virtual Network hub template	Resource Manager template	Subnet address prefixes (optional)	Array of IP address prefixes for optional subnets for hub virtual network; for example, "10.0.7.0/24","10.0.8.0/24"
Spoke resource group	Resource group	Resource group name	Locked - Concatenates prefix with spoke name
Spoke resource group	Resource group	Resource group location	Locked - Uses hub location
Azure Virtual Network spoke template	Resource Manager template	Deploy spoke	Enter 'true' or 'false' to specify whether the assignment deploys the spoke components of the architecture
Azure Virtual Network spoke template	Resource Manager template	Hub subscription ID	Subscription ID where hub is deployed; default value is the subscription where the blueprint definition is located
Azure Virtual Network spoke template	Resource Manager template	Spoke name	Name of the spoke

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Azure Virtual Network spoke template	Resource Manager template	Virtual Network address prefix	Virtual Network address prefix for spoke virtual network
Azure Virtual Network spoke template	Resource Manager template	Subnet address prefix	Subnet address prefix for spoke virtual network
Azure Virtual Network spoke template	Resource Manager template	Subnet address names (optional)	Array of subnet names to deploy to the spoke virtual network; for example, "subnet1","subnet2"
Azure Virtual Network spoke template	Resource Manager template	Subnet address prefixes (optional)	Array of IP address prefixes for optional subnets for the spoke virtual network; for example, "10.0.7.0/24","10.0.8.0/24"
Azure Virtual Network spoke template	Resource Manager template	Deploy spoke	Enter 'true' or 'false' to specify whether the assignment deploys the spoke components of the architecture
Azure Network Watcher template	Resource Manager template	Network Watcher location	Location for the Network Watcher resource
Azure Network Watcher template	Resource Manager template	Network Watcher resource group location	If Network Watcher is already enabled, this parameter value must match the location of the existing Network Watcher resource group.

Troubleshooting

If you encounter the error

```
The resource group 'NetworkWatcherRG' failed to deploy due to the following error: Invalid resource group location '{location}'. The Resource group already exists in location '{location}'.
```

, check that the blueprint parameter **Network Watcher resource group name** specifies the existing Network Watcher resource group name and that the artifact parameter **Network Watcher resource group location** specifies the existing Network Watcher resource group location.

Next steps

Now that you've reviewed the steps to deploy the Azure Security Benchmark Foundation blueprint sample, visit the following article to learn about the architecture:

[Azure Security Benchmark Foundation blueprint - Overview](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).

- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the Australian Government ISM PROTECTED blueprint sample

5/3/2021 • 2 minutes to read • [Edit Online](#)

ISM Governance blueprint sample provides a set of governance guardrails using [Azure Policy](#) which help toward ISM PROTECTED attestation (Feb 2020 version). This Blueprint helps customers deploy a core set of policies for any Azure-deployed architecture requiring accreditation or compliance with the ISM framework.

Control mapping

The control mapping section provides details on policies included within this blueprint and how these policies address various controls in ISM PROTECTED. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policies. For more information, see [Azure Policy](#).

Next steps

You've reviewed the overview and of the ISM PROTECTED blueprint sample. Next, visit the following articles to learn about the control mapping and how to deploy this sample:

[ISM PROTECTED blueprint - Control mapping](#) [ISM PROTECTED blueprint - Deploy steps](#)

Addition articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Control mapping of the Australian Government ISM PROTECTED blueprint sample

5/2/2021 • 15 minutes to read • [Edit Online](#)

The following article details how the Azure Blueprints Australian Government ISM PROTECTED blueprint sample maps to the ISM PROTECTED controls. For more information about the controls, see [ISM PROTECTED](#).

The following mappings are to the **ISM PROTECTED** controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an [Azure Policy](#) initiative. To review the complete initiative, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements built-in policy initiative**.

IMPORTANT

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy definitions for this compliance blueprint sample may change over time. To view the change history, see the [GitHub Commit History](#).

Location Constraints

This blueprint helps you restrict the location for the deployment of all resources and resource groups to "Australia Central", "Australia Central2", "Australia East" and "Australia Southeast" by assigning following Azure Policy definitions:

- Allowed locations (has been hard coded to "Australia Central", "Australia Central2", "Australia East" and "Australia Southeast")
- Allowed locations for resource groups (has been hard coded to "Australia Central", "Australia Central2", "Australia East" and "Australia Southeast")

Guidelines for Personnel Security - Access to systems and their resources

0414 Personnel granted access to a system and its resources are uniquely identifiable

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription
- MFA should be enabled on accounts with read permissions on your subscription

1503 Standard access to systems, applications and data repositories is limited to that required for personnel to undertake their duties

- A maximum of 3 owners should be designated for your subscription
- There should be more than one owner assigned to your subscription
- Show audit results from Windows VMs in which the Administrators group contains any of the specified members

- Deploy prerequisites to audit Windows VMs in which the Administrators group contains any of the specified members

1507 Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis

- Show audit results from Windows VMs in which the Administrators group contains any of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group contains any of the specified members

1508 Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties

- A maximum of 3 owners should be designated for your subscription
- There should be more than one owner assigned to your subscription
- Show audit results from Windows VMs in which the Administrators group contains any of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group contains any of the specified members
- Just-In-Time network access control should be applied on virtual machines

0415 The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable

- Show audit results from Windows VMs in which the Administrators group contains any of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group contains any of the specified members

0445 Privileged users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access

- Show audit results from Windows VMs in which the Administrators group contains any of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group contains any of the specified members

0430 Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription

0441 When personnel are granted temporary access to a system, effective security controls are put in place to restrict their access to only information required for them to undertake their duties

- External accounts with owner permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription
- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription

Guidelines for System Hardening - Operating system hardening

1407 The latest version (N), or N-1 version, of an operating system is used for Standard Operating Environments (SOEs)

- System updates should be installed on your machines
- System updates on virtual machine scale sets should be installed

0380 Unneeded operating system accounts, software, components, services and functionality are removed or

disabled

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription

1490 An application whitelisting solution is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set

- Adaptive Application Controls should be enabled on virtual machines

1417 Antivirus software is implemented on workstations and servers and configured with: signature-based detection enabled and set to a high level, heuristic-based detection enabled and set to a high level, detection signatures checked for currency and updated on at least a daily basis, automatic and regular scanning configured for all fixed disks and removable media

- Microsoft IaaS Antimalware extension should be deployed on Windows servers
- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center

Guidelines for System Hardening - Authentication hardening

1546 Users are authenticated before they are granted access to a system and its resources

- Audit unrestricted network access to storage accounts
- Service Fabric clusters should only use Azure Active Directory for client authentication
- Show audit results from Linux VMs that allow remote connections from accounts without passwords
- Deploy prerequisites to audit Linux VMs that allow remote connections from accounts without passwords
- Show audit results from Linux VMs that have accounts without passwords
- Deploy prerequisites to audit Linux VMs that have accounts without passwords

0974 Multi-factor authentication is used to authenticate standard users

- MFA should be enabled on accounts with read permissions on your subscription

1173 Multi-factor authentication is used to authenticate all privileged users and any other positions of trust

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription

0421 Passphrases used for single-factor authentication are a minimum of 14 characters with complexity, ideally as 4 random words

- Show audit results from Windows VMs configurations in 'Security Settings - Account Policies'
- Deploy prerequisites to audit Windows VMs configurations in 'Security Settings - Account Policies'

Guidelines for System Management - System administration

1384 Multi-factor authentication is used to authenticate users each time they perform privileged actions

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription
- MFA should be enabled on accounts with read permissions on your subscription

1386 Management traffic is only allowed to originate from network zones that are used to administer systems and applications

- Just-In-Time network access control should be applied on virtual machines
- Remote debugging should be turned off for API Apps
- Remote debugging should be turned off for Function Apps
- Remote debugging should be turned off for Web Applications

Guidelines for System Management - System patching

1144 Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users

- Vulnerabilities on your SQL databases should be remediated
- Vulnerability assessment should be enabled on your SQL servers
- Vulnerability assessment should be enabled on your SQL managed instances
- Vulnerability Assessment should be enabled on Machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities in container security configurations should be remediated
- Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports

0940 Security vulnerabilities in applications and drivers assessed as high risk are patched, updated or mitigated within two weeks of the security vulnerability being identified by vendors, independent third parties, system managers or users

- Vulnerabilities on your SQL databases should be remediated
- Vulnerability assessment should be enabled on your SQL servers
- Vulnerability assessment should be enabled on your SQL managed instances
- Vulnerability Assessment should be enabled on Virtual Machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities in container security configurations should be remediated
- Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports

1472 Security vulnerabilities in applications and drivers assessed as moderate or low risk are patched, updated or mitigated within one month of the security vulnerability being identified by vendors, independent third parties, system managers or users

- Vulnerabilities on your SQL databases should be remediated
- Vulnerability assessment should be enabled on your SQL servers
- Vulnerability assessment should be enabled on your SQL managed instances
- Vulnerability Assessment should be enabled on Virtual Machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities in container security configurations should be remediated
- Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports

1494 Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users

- Vulnerabilities on your SQL databases should be remediated
- Vulnerability assessment should be enabled on your SQL servers
- Vulnerability assessment should be enabled on your SQL managed instances
- Vulnerability Assessment should be enabled on Virtual Machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your machines should be remediated

- Vulnerabilities in container security configurations should be remediated
- Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports

1495 Security vulnerabilities in operating systems and firmware assessed as high risk are patched, updated or mitigated within two weeks of the security vulnerability being identified by vendors, independent third parties, system managers or users

- Vulnerabilities on your SQL databases should be remediated
- Vulnerability assessment should be enabled on your SQL servers
- Vulnerability assessment should be enabled on your SQL managed instances
- Vulnerability Assessment should be enabled on Virtual Machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities in container security configurations should be remediated
- Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports

1496 Security vulnerabilities in operating systems and firmware assessed as moderate or low risk are patched, updated or mitigated within one month of the security vulnerability being identified by vendors, independent third parties, system managers or users

- Vulnerabilities on your SQL databases should be remediated
- Vulnerability assessment should be enabled on your SQL servers
- Vulnerability assessment should be enabled on your SQL managed instances
- Vulnerability Assessment should be enabled on Virtual Machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities in container security configurations should be remediated
- Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports

Guidelines for System Management - Data backup and restoration

1511 Backups of important information, software and configuration settings are performed at least daily

- Audit virtual machines without disaster recovery configured

Guidelines for System Monitoring - Event logging and auditing

1405 A centralised logging facility is implemented and systems are configured to save event logs to the centralised logging facility as soon as possible after each event occurs

- Azure subscriptions should have a log profile for Activity Log

0582 The following events are logged for operating systems: access to important data and processes, application crashes and any error messages, attempts to use special privileges, changes to accounts, changes to security policy, changes to system configurations, Domain Name System (DNS) and Hypertext Transfer Protocol (HTTP) requests, failed attempts to access data and system resources, service failures and restarts, system startup and shutdown, transfer of data to external media, user or group management, use of special privileges

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics Agent Deployment in VMSS - VM Image (OS) unlisted
- Audit Log Analytics Workspace for VM - Report Mismatch
- Audit diagnostic setting

1537 The following events are logged for databases: access to particularly important information, addition of new users, especially privileged users, any query containing comments, any query containing multiple

embedded queries, any query or database alerts or failures, attempts to elevate privileges, attempted access that is successful or unsuccessful, changes to the database structure, changes to user roles or database permissions, database administrator actions, database logons and logoffs, modifications to data, use of executable commands

- Advanced data security should be enabled on your SQL servers
- Audit diagnostic setting
- Advanced data security should be enabled on your SQL managed instances

Guidelines for System Monitoring - Vulnerability management

0911 Vulnerability assessments and penetration tests are conducted by suitably skilled personnel before a system is deployed, after a significant change to a system, and at least annually or as specified by the system owner

- Vulnerabilities on your SQL databases should be remediated
- Vulnerability assessment should be enabled on your SQL servers
- Vulnerability assessment should be enabled on your SQL managed instances
- Vulnerability Assessment should be enabled on Virtual Machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities in container security configurations should be remediated

Guidelines for Database Systems Management - Database servers

1425 Hard disks of database servers are encrypted using full disk encryption

- Disk encryption should be applied on virtual machines
- Transparent Data Encryption on SQL databases should be enabled

1277 Information communicated between database servers and web applications is encrypted

- Only secure connections to your Redis Cache should be enabled
- Secure transfer to storage accounts should be enabled
- Show audit results from Windows web servers that are not using secure communication protocols
- Deploy prerequisites to audit Windows web servers that are not using secure communication protocols

Guidelines for Database Systems Management - Database management system software

1260 Default database administrator accounts are disabled, renamed or have their passphrases changed

- An Azure Active Directory administrator should be provisioned for SQL servers

1262 Database administrators have unique and identifiable accounts

- An Azure Active Directory administrator should be provisioned for SQL servers

1261 Database administrator accounts are not shared across different databases

- An Azure Active Directory administrator should be provisioned for SQL servers

1263 Database administrator accounts are used exclusively for administrative tasks, with standard database accounts used for general purpose interactions with database

- An Azure Active Directory administrator should be provisioned for SQL servers

1264 Database administrator access is restricted to defined roles rather than accounts with default administrative permissions, or all permissions

- An Azure Active Directory administrator should be provisioned for SQL servers

Guidelines for Using Cryptography - Cryptographic fundamentals

0459 Encryption software used for data at rest implements full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition

- Disk encryption should be applied on virtual machines

Guidelines for Using Cryptography - Transport Layer Security

1139 Only the latest version of TLS is used

- Latest TLS version should be used in your API App
- Latest TLS version should be used in your Web App
- Latest TLS version should be used in your Function App
- Deploy prerequisites to audit Windows web servers that are not using secure communication protocols
- Show audit results from Windows web servers that are not using secure communication protocols

Guidelines for Data Transfers and Content Filtering - Content filtering

1288 Antivirus scanning, using multiple different scanning engines, is performed on all content

- Microsoft IaaS Antimalware extension should be deployed on Windows servers
- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center

Guidelines for Data Transfers and Content Filtering - Web application development

1552 All web application content is offered exclusively using HTTPS

- Function App should only be accessible over HTTPS
- API App should only be accessible over HTTPS
- Web Application should only be accessible over HTTPS
- Only secure connections to your Redis Cache should be enabled

1424 Web browser-based security controls are implemented for web applications in order to help protect both web applications and their users

- CORS should not allow every resource to access your Web Applications

Guidelines for Network Management - Network design and configuration

0520 Network access controls are implemented on networks to prevent the connection of unauthorised network devices

- Audit unrestricted network access to storage accounts

1182 Network access controls are implemented to limit traffic within and between network segments to only those that are required for business purposes

- Internet-facing virtual machines should be protected with Network Security Groups
- Audit unrestricted network access to storage accounts
- Adaptive Network Hardening recommendations should be applied on internet facing virtual machines

Guidelines for Network Management - Service continuity for online services

1431 Denial-of-service attack prevention and mitigation strategies are discussed with service providers, specifically: their capacity to withstand denial-of-service attacks, any costs likely to be incurred by customers resulting from denial-of-service attacks, thresholds for notifying customers or turning off their online services during denial-of-service attacks, pre-approved actions that can be undertaken during denial-of-service attacks, denial-of-service attack prevention arrangements with upstream providers to block malicious traffic as far upstream as possible

- DDoS Protection Standard should be enabled

NOTE

Availability of specific Azure Policy definitions may vary in Azure Government and other national clouds.

Next steps

Additional articles about blueprints and how to use them:

[ISM PROTECTED blueprint - Overview](#) [ISM PROTECTED blueprint - Deploy steps](#)

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the Australian Government ISM PROTECTED blueprint sample

5/3/2021 • 24 minutes to read • [Edit Online](#)

To deploy the Azure Blueprints ISM PROTECTED blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **ISM PROTECTED** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the ISM PROTECTED blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with ISM PROTECTED controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the ISM PROTECTED blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - **Basics**
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - **Lock Assignment**

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - **Managed Identity**

Leave the default *system assigned* managed identity option.
 - **Artifact parameters**

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Log Analytics workspace ID that VMs should be configured for	This is the ID (GUID) of the Log Analytics workspace that the VMs should be configured for.
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor resource logs categories .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be excluded from Windows VM Administrators group	A semicolon-separated list of members that should be excluded in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be included in Windows VM Administrators group	A semicolon-separated list of members that should be included in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Linux VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Log Analytics workspace for Linux VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Windows VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Log Analytics workspace for Windows VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Advanced Threat Protection on Storage Accounts	Policy assignment	Effect	Information about policy effects can be found at Understand Azure Policy Effects .
Deploy Auditing on SQL servers	Policy assignment	The value in days of the retention period (0 indicates unlimited retention)	Retention days (optional, 180 days if unspecified)
Deploy Auditing on SQL servers	Policy assignment	Resource group name for storage account for SQL server auditing	Auditing writes database events to an audit log in your Azure Storage account (a storage account will be created in each region where a SQL Server is created that will be shared by all servers in that region). Important - for proper operation of Auditing do not delete or rename the resource group or the storage accounts.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Storage account prefix for network security group diagnostics	This prefix will be combined with the network security group location to form the created storage account name.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Deploy diagnostic settings for Network Security Groups	Policy assignment	Resource group name for storage account for network security group diagnostics (must exist)	The resource group that the storage account will be created in. This resource group must already exist.
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Allowed locations for resources and resource groups	List of Azure locations that your organization can specify when deploying resources. This provided value is also used by the 'Allowed locations' policy within the policy initiative.
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerability assessment should be enabled on your SQL managed instances	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerability assessment should be enabled on your SQL servers	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerability assessment should be enabled on Virtual Machines	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Geo-redundant storage should be enabled for Storage Accounts	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Geo-redundant backup should be enabled for Azure Database for MariaDB	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Geo-redundant backup should be enabled for Azure Database for MySQL	Information about policy effects can be found at Understand Azure Policy Effects .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Geo-redundant backup should be enabled for Azure Database for PostgreSQL	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Network Security Group rules for internet facing virtual machines should be hardened	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Web Application should only be accessible over HTTPS	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Function App should only be accessible over HTTPS	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	External accounts with write permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	External accounts with read permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	External accounts with owner permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Deprecated accounts with owner permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Deprecated accounts should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	CORS shouldn't allow every resource to access your Web Application	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	System updates on virtual machine scale sets should be installed	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	MFA should be enabled on accounts with read permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	MFA should be enabled on accounts with owner permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	MFA should be enabled on accounts with write permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Long-term geo-redundant backup should be enabled for Azure SQL Databases	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users excluded from Windows VM Administrators group	A semicolon-separated list of members that should be excluded in the Administrators local group. Ex: Administrator; myUser1; myUser2

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Log Analytics Workspace Id that VMs should be configured for	This is the ID (GUID) of the Log Analytics workspace that the VMs should be configured for.
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Adaptive Network Hardening recommendations should be applied on internet facing virtual machines	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	There should be more than one owner assigned to your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Disk encryption should be applied on virtual machines	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Remote debugging should be turned off for Function App	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Transparent Data Encryption on SQL databases should be enabled	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerability assessment should be enabled on your SQL managed instances	Information about policy effects can be found at Understand Azure Policy Effects .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	An Azure Active Directory administrator should be provisioned for SQL servers	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Only secure connections to your Redis Cache should be enabled	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Endpoint protection solution should be installed on virtual machine scale sets	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Audit unrestricted network access to storage accounts	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerabilities in security configuration on your virtual machine scale sets should be remediated	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Secure transfer to storage accounts should be enabled	Information about policy effects can be found at Understand Azure Policy Effects .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Adaptive Application Controls should be enabled on virtual machines	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	A maximum of 3 owners should be designated for your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	[Preview] Vulnerability Assessment should be enabled on Virtual Machines	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	CORS should not allow every resource to access your Web Application	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	External accounts with write permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Deprecated accounts should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Function App should only be accessible over HTTPS v2	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerabilities should be remediated by a Vulnerability Assessment solution	Information about policy effects can be found at Understand Azure Policy Effects .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Azure subscriptions should have a log profile for Activity Log	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor resource logs categories .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	System updates should be installed on your machines	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Latest TLS version should be used for App Service	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	MFA should be enabled accounts with write permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Microsoft IaaS Antimalware extension should be deployed on Windows servers	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Web Application should only be accessible over HTTPS v2	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	DDoS Protection Standard should be enabled	Information about policy effects can be found at Understand Azure Policy Effects .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	MFA should be enabled on accounts with owner permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Advanced data security should be enabled on your SQL servers	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Advanced data security should be enabled on your SQL managed instances	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Monitor missing endpoint protection in Azure Security Center	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Just-in-time network access control should be applied on virtual machines	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Service Fabric clusters should only use Azure Active Directory for client authentication	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	App Service should only be accessible over HTTPS v2	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	System updates on virtual machine scale sets should be installed	Information about policy effects can be found at Understand Azure Policy Effects .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Remote debugging should be turned off for Web Application	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerabilities in security configuration on your machines should be remediated	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	MFA should be enabled on accounts with read permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Enforce password history	Specifies limits on password reuse - how many times a new password must be created for a user account before the password can be repeated.
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Maximum password age	Specifies the maximum number of days that may elapse before a user account password must be changed. The format of the value is two integers separated by a comma, denoting an inclusive range.
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Minimum password age	Specifies the minimum number of days that must elapse before a user account password can be changed.
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Minimum password length	Specifies the minimum number of characters that a user account password may contain.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Password must meet complexity requirements	Specifies whether a user account password must be complex. If required, a complex password must not contain part of user's account name or full name; be at least 6 characters long; contain a mix of uppercase, lowercase, number, and non-alphabetic characters.
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerabilities in container security configurations should be remediated	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Remote debugging should be turned off for App Service	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Deprecated accounts with owner permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerability assessment should be enabled on your SQL servers	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Latest TLS version should be used in your Web App	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Internet-facing virtual machines should be protected with Network Security Groups	Information about policy effects can be found at Understand Azure Policy Effects .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	External accounts with owner permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Latest TLS version should be used in your Function App	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit Australian Government ISM PROTECTED controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerabilities on your SQL databases should be remediated	Information about policy effects can be found at Understand Azure Policy Effects .

Next steps

Now that you've reviewed the steps to deploy the Australian Government ISM PROTECTED blueprint sample, visit the following articles to learn about the blueprint and control mapping:

[ISM PROTECTED blueprint - Overview](#) [ISM PROTECTED blueprint - Control mapping](#)

Addition articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Canada Federal PBMM blueprint sample

5/4/2021 • 6 minutes to read • [Edit Online](#)

The Canada Federal PBMM blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific [Canada Federal PBMM](#) controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement controls for Canada Federal PBMM.

Control mapping

The [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **controls** in the Canada Federal PBMM framework. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints Canada Federal PBMM blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **Canada Federal PBMM** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the Canada Federal PBMM blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that are included in the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with Canada Federal PBMM controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.

2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the Canada Federal PBMM blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:

- Basics

- **Subscriptions:** Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
- **Assignment name:** The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
- **Location:** Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
- **Blueprint definition version:** Pick a **Published** version of your copy of the blueprint sample.

- Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *system assigned* managed identity option.

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Log Analytics workspace for Linux VMs	For more information, see Create a Log Analytics workspace in the Azure portal .
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: <code>[]</code>
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: <code>[]</code>
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Log Analytics workspace for Windows VMs	For more information, see Create a Log Analytics workspace in the Azure portal .
[Preview]: Audit Canada Federal PBMM controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Log Analytics workspace ID that VMs should be configured for	This is the ID (GUID) of the Log Analytics workspace that the VMs should be configured for.
[Preview]: Audit Canada Federal PBMM controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting isn't enabled. Acceptable values can be found at Azure Monitor diagnostic logs schemas .
[Preview]: Audit Canada Federal PBMM controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Administrators group	Group. Example: <code>Administrator; myUser1; myUser2</code>
[Preview]: Audit Canada Federal PBMM controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be included in Windows VM Administrators group	A semicolon-separated list of members that should be included in the Administrators local group. Example: <code>Administrator; myUser1; myUser2</code>
Deploy Advanced Threat Protection on Storage Accounts	Policy assignment	Effect	Information about policy effects can be found at Understand Azure Policy Effects .
Deploy Auditing on SQL servers	Policy assignment	The value in days of the retention period (0 indicates unlimited retention)	Retention days (optional, 180 days if unspecified)

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Deploy Auditing on SQL servers	Policy assignment	Resource group name for storage account for SQL server auditing	Auditing writes database events to an audit log in your Azure Storage account (a storage account is created in each region where a SQL Server is created that is shared by all servers in that region). Important - for proper operation of Auditing don't delete or rename the resource group or the storage accounts.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Storage account prefix for network security group diagnostics	This prefix is combined with the network security group location to form the created storage account name.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Resource group name for storage account for network security group diagnostics (must exist)	The resource group that the storage account is created in. This resource group must already exist.

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

CIS Microsoft Azure Foundations Benchmark v1.3.0 blueprint sample

5/3/2021 • 19 minutes to read • [Edit Online](#)

The CIS Microsoft Azure Foundations Benchmark v1.3.0 blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific CIS Microsoft Azure Foundations Benchmark v1.3.0 recommendations. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement CIS Microsoft Azure Foundations Benchmark v1.3.0 recommendations.

Recommendation mapping

The [Azure Policy recommendation mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **recommendations** in CIS Microsoft Azure Foundations Benchmark v1.3.0. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints CIS Microsoft Azure Foundations Benchmark v1.3.0 blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **CIS Microsoft Azure Foundations Benchmark v1.3.0** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the CIS Microsoft Azure Foundations Benchmark blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that are included in the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with CIS Microsoft Azure Foundations Benchmark v1.3.0 recommendations.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the CIS Microsoft Azure Foundations Benchmark blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - Managed Identity

Leave the default *system assigned* managed identity option.
 - Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are **priced by product**. Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	List of virtual machine extensions that are approved for use	A semicolon-separated list of virtual machine extensions; to see a complete list of extensions, use the Azure PowerShell command <code>Get-AzVMExtensionImage</code>
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: SQL managed instances should use customer-managed keys to encrypt data at rest	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in Azure Data Lake Store should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Disk encryption should be applied on virtual machines	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Key vault should have purge protection enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure API app has 'Client Certificates (Incoming client certificates)' set to 'On'	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: SQL servers should use customer-managed keys to encrypt data at rest	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Managed identity should be used in your Function App	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Azure Defender for Key Vault should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Custom subscription owner roles should not exist	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Keys should have expiration dates set	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Transparent Data Encryption on SQL databases should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Vulnerability assessment should be enabled on SQL Managed Instance	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'PHP version' is the latest, if used as a part of the API app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An Azure Active Directory administrator should be provisioned for SQL servers	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Azure Defender for App Service should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Storage accounts should restrict network access using virtual network rules	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Managed identity should be used in your Web App	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: SSH access from the Internet should be blocked	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Unattached disks should be encrypted	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Azure Defender for Storage should be enabled	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Storage accounts should restrict network access	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in Logic Apps should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in IoT Hub should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: FTPS only should be required in your Function App	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An activity log alert should exist for specific Security operations (Microsoft.Security/securitySolutions/delete)	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An activity log alert should exist for specific Security operations (Microsoft.Security/securitySolutions/write)	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Secure transfer to storage accounts should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in Batch accounts should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Auto provisioning of the Log Analytics agent should be enabled on your subscription	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'Java version' is the latest, if used as a part of the Web app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: FTPS should be required in your Web App	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Azure Defender for servers should be enabled	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Subscriptions should have a contact email address for security issues	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Storage account public access should be disallowed	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Azure Defender for Kubernetes should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Connection throttling should be enabled for PostgreSQL database servers	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure WEB app has 'Client Certificates (Incoming client certificates)' set to 'On'	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: External accounts with write permissions should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: External accounts with read permissions should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Azure Defender for SQL servers on machines should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Email notification for high severity alerts should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Storage account should use customer-managed key for encryption	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'Python version' is the latest, if used as a part of the Web app	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'Python version' is the latest, if used as a part of the Function app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'PHP version' is the latest, if used as a part of the WEB app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'Python version' is the latest, if used as a part of the API app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in Virtual Machine Scale Sets should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Azure Defender for Azure SQL Database servers should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in Event Hub should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: System updates should be installed on your machines	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'Java version' is the latest, if used as a part of the API app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: SQL servers should be configured with 90 days auditing retention or higher.	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'HTTP Version' is the latest, if used to run the Web app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Latest TLS version should be used in your API App	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: MFA should be enabled accounts with write permissions on your subscription	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Authentication should be enabled on your web app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Secrets should have expiration dates set	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'HTTP Version' is the latest, if used to run the API app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: FTPS only should be required in your API App	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'Java version' is the latest, if used as a part of the Function app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Web Application should only be accessible over HTTPS	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Auditing on SQL server should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: MFA should be enabled on accounts with owner permissions on your subscription	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Advanced data security should be enabled on your SQL servers	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Advanced data security should be enabled on SQL Managed Instance	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Role-Based Access Control (RBAC) should be used on Kubernetes Services	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Monitor missing Endpoint Protection in Azure Security Center	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in Search services should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in App Services should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.Network/network SecurityGroups/delete)	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.Network/network SecurityGroups/securityRules/delete)	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.Network/network SecurityGroups/securityRules/write)	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.Network/network SecurityGroups/write)	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.Sql/servers/firewallRules/delete)	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.Sql/servers/firewallRules/write)	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Only approved VM extensions should be installed	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Azure Defender for container registries should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Managed identity should be used in your API App	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Authentication should be enabled on your API app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An activity log alert should exist for specific Policy operations (Microsoft.Authorization/policyAssignments/delete)	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: An activity log alert should exist for specific Policy operations (Microsoft.Authorization/policyAssignments/write)	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Authentication should be enabled on your Function app	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in Data Lake Analytics should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Storage accounts should allow access from trusted Microsoft services	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in Key Vault should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Enforce SSL connection should be enabled for PostgreSQL database servers	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure that 'HTTP Version' is the latest, if used to run the Function app	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: MFA should be enabled on accounts with read permissions on your subscription	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: RDP access from the Internet should be blocked	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Enforce SSL connection should be enabled for MySQL database servers	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Ensure Function app has 'Client Certificates (Incoming client certificates)' set to 'On'	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Log checkpoints should be enabled for PostgreSQL database servers	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Log connections should be enabled for PostgreSQL database servers	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Disconnections should be logged for PostgreSQL database servers.	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Vulnerability assessment should be enabled on your SQL servers	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Latest TLS version should be used in your Web App	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: External accounts with owner permissions should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in Service Bus should be enabled	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Diagnostic logs in Azure Stream Analytics should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Latest TLS version should be used in your Function App	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Effect for policy: Storage account containing the container with activity logs must be encrypted with BYOK	For more information about effects, visit https://aka.ms/policyeffects
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Include AKS clusters when auditing if virtual machine scale set diagnostic logs are enabled	
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Latest Java version for App Services	Latest supported Java version for App Services
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Latest Python version for Linux for App Services	Latest supported Python version for App Services
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	List of regions where Network Watcher should be enabled	To see a complete list of regions, run the PowerShell command Get-AzLocation
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Latest PHP version for App Services	Latest supported PHP version for App Services
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Required retention period (days) for resource logs	For more information about resource logs, visit https://aka.ms/resourcelogs
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Name of the resource group for Network Watcher	Name of the resource group where Network Watchers are located
CIS Microsoft Azure Foundations Benchmark v1.3.0	Policy Assignment	Required auditing setting for SQL servers	

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).

- Learn how to [update existing assignments](#).

CIS Microsoft Azure Foundations Benchmark v1.1.0 blueprint sample

5/3/2021 • 5 minutes to read • [Edit Online](#)

The CIS Microsoft Azure Foundations Benchmark v1.1.0 blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific CIS Microsoft Azure Foundations Benchmark recommendations. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement CIS Microsoft Azure Foundations Benchmark v1.1.0 recommendations.

Recommendation mapping

The [Azure Policy recommendation mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **recommendations** in CIS Microsoft Azure Foundations Benchmark v1.1.0. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints CIS Microsoft Azure Foundations Benchmark v1.1.0 blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **CIS Microsoft Azure Foundations Benchmark v1.1.0** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the CIS Microsoft Azure Foundations Benchmark blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that are included in the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with CIS Microsoft Azure Foundations Benchmark v1.1.0 recommendations.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the CIS Microsoft Azure Foundations Benchmark blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - Managed Identity

Leave the default *system assigned* managed identity option.
 - Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are **priced by product**. Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Audit CIS Microsoft Azure Foundations Benchmark v1.1.0 recommendations and deploy specific supporting VM Extensions	Policy assignment	List of regions where Network Watcher should be enabled	A semicolon-separated list of regions. To see a complete list of regions use Get-AzLocation. Ex: eastus; eastus2
Audit CIS Microsoft Azure Foundations Benchmark v1.1.0 recommendations and deploy specific supporting VM Extensions	Policy assignment	List of virtual machine extensions that are approved for use	A semicolon-separated list of extensions. To see a complete list of virtual machine extensions, use Get-AzVMExtensionImage. Ex: AzureDiskEncryption; IaaSAntimalware

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

CMMC Level 3 blueprint sample

5/3/2021 • 34 minutes to read • [Edit Online](#)

The CMMC Level 3 blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific [Cybersecurity Maturity Model Certification \(CMMC\) framework](#) controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement controls for CMMC Level 3.

Control mapping

The [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **controls** in the CMMC framework. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints CMMC Level 3 blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **CMMC Level 3** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the CMMC Level 3 blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that are included in the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with CMMC Level 3 controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.

2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the CMMC Level 3 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:

- Basics

- **Subscriptions:** Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
- **Assignment name:** The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
- **Location:** Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
- **Blueprint definition version:** Pick a **Published** version of your copy of the blueprint sample.

- Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *system assigned* managed identity option.

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Include Arc-connected servers when evaluating guest configuration policies	By selecting 'true', you agree to be charged monthly per Arc connected machine; for more information, visit https://aka.ms/policy-pricing
CMMC Level 3	Policy Assignment	List of users that must be excluded from Windows VM Administrators group	A semicolon-separated list of users that should be excluded in the Administrators local group; Ex: Administrator; myUser1; myUser2
CMMC Level 3	Policy Assignment	List of users that must be included in Windows VM Administrators group	A semicolon-separated list of users that should be included in the Administrators local group; Ex: Administrator; myUser1; myUser2
CMMC Level 3	Policy Assignment	Log Analytics workspace ID for VM agent reporting	ID (GUID) of the Log Analytics workspace where VMs agents should report
CMMC Level 3	Policy Assignment	Allowed elliptic curve names	The list of allowed curve names for elliptic curve cryptography certificates.
CMMC Level 3	Policy Assignment	Allowed key types	The list of allowed key types
CMMC Level 3	Policy Assignment	Allow host network usage for Kubernetes cluster pods	Set this value to true if pod is allowed to use host network otherwise false.
CMMC Level 3	Policy Assignment	Audit Authentication Policy Change	Specifies whether audit events are generated when changes are made to authentication policy. This setting is useful for tracking changes in domain-level and forest-level trust and privileges that are granted to user accounts or groups.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Audit Authorization Policy Change	Specifies whether audit events are generated for assignment and removal of user rights in user right policies, changes in security token object permission, resource attributes changes and Central Access Policy changes for file system objects.
CMMC Level 3	Policy Assignment	Effect for policy: Azure Backup should be enabled for Virtual Machines	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Cognitive Services accounts should restrict network access	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: SQL managed instances should use customer-managed keys to encrypt data at rest	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure API for FHIR should use a customer-managed key (CMK) to encrypt data at rest	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Web Application Firewall (WAF) should be enabled for Azure Front Door Service	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Public network access should be disabled for Cognitive Services accounts	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: CORS should not allow every resource to access your Function Apps	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Adaptive network hardening recommendations should be applied on internet facing virtual machines	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: There should be more than one owner assigned to your subscription	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Disk encryption should be applied on virtual machines	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Email notification to subscription owner for high severity alerts should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Key vault should have purge protection enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: SQL servers should use customer-managed keys to encrypt data at rest	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Remote debugging should be turned off for Function Apps	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Defender for Key Vault should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Geo-redundant backup should be enabled for Azure Database for MariaDB	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: CORS should not allow every domain to access your API for FHIR	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Windows machines should meet requirements for 'Security Options - Network Security'	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Allowlist rules in your adaptive application control policy should be updated	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: Web Application Firewall (WAF) should use the specified mode for Application Gateway	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Keys should have expiration dates set	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Transparent Data Encryption on SQL databases should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Monitor log profile should collect logs for categories 'write,' 'delete,' and 'action'	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Vulnerability assessment should be enabled on SQL Managed Instance	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'PHP version' is the latest, if used as a part of the API app	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Key vault should have soft delete enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: An Azure Active Directory administrator should be provisioned for SQL servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Only secure connections to your Azure Cache for Redis should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Endpoint protection solution should be installed on virtual machine scale sets	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: Azure Defender for App Service should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Windows machines should meet requirements for 'System Audit Policies - Policy Change'	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Cognitive Services accounts should enable data encryption	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: SSH access from the Internet should be blocked	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Unattached disks should be encrypted	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Defender for Storage should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Storage accounts should restrict network access	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: CORS should not allow every resource to access your API App	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Deploy Advanced Threat Protection on Storage Accounts	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Automation account variables should be encrypted	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Diagnostic logs in IoT Hub should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Infrastructure encryption should be enabled for Azure Database for MySQL servers	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: An activity log alert should exist for specific Security operations (Microsoft.Security/securitySolutions/delete)	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Vulnerabilities in security configuration on your virtual machine scale sets should be remediated	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Windows machines should meet requirements for 'Security Options - Network Access'	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Secure transfer to storage accounts should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Monitor should collect activity logs from all regions	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Web Application Firewall (WAF) should use the specified mode for Azure Front Door Service	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Storage accounts should have infrastructure encryption	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Adaptive application controls for defining safe applications should be enabled on your machines	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Geo-redundant backup should be enabled for Azure Database for PostgreSQL	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Windows machines should meet requirements for 'Security Options - User Account Control'	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'Java version' is the latest, if used as a part of the Web app	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: Azure Defender for servers should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: A maximum of 3 owners should be designated for your subscription	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Subscriptions should have a contact email address for security issues	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Storage account public access should be disallowed	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: A vulnerability assessment solution should be enabled on your virtual machines	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Defender for Kubernetes should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Firewall should be enabled on Key Vault	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Web Application Firewall (WAF) should be enabled for Application Gateway	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: CORS should not allow every resource to access your Web Applications	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Audit Windows machines that allow re-use of the previous 24 passwords	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Container registries should be encrypted with a customer-managed key (CMK)	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: External accounts with write permissions should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: Public network access should be disabled for PostgreSQL flexible servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Vulnerabilities in Azure Container Registry images should be remediated	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: External accounts with read permissions should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Defender for SQL servers on machines should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Cognitive Services accounts should enable data encryption with customer-managed key	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Deprecated accounts should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Function App should only be accessible over HTTPS	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Email notification for high severity alerts should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Storage account should use customer-managed key for encryption	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'Python version' is the latest, if used as a part of the Web app	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'Python version' is the latest, if used as a part of the Function app	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'PHP version' is the latest, if used as a part of the WEB app	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'Python version' is the latest, if used as a part of the API app	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Keys should be the specified cryptographic type RSA or EC	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure subscriptions should have a log profile for Activity Log	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Defender for Azure SQL Database servers should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Data Explorer encryption at rest should use a customer-managed key	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Keys using RSA cryptography should have a specified minimum key size	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Geo-redundant backup should be enabled for Azure Database for MySQL	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Kubernetes cluster pods should only use approved host network and port range	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: System updates should be installed on your machines	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Windows machines should meet requirements for 'System Audit Policies - Privilege Use'	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Stream Analytics jobs should use customer-managed keys to encrypt data	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'Java version' is the latest, if used as a part of the API app	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'HTTP Version' is the latest, if used to run the Web app	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Latest TLS version should be used in your API App	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: MFA should be enabled accounts with write permissions on your subscription	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'HTTP Version' is the latest, if used to run the API app	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Microsoft IaaSAntimalware extension should be deployed on Windows servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'Java version' is the latest, if used as a part of the Function app	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: All network ports should be restricted on network security groups associated to your virtual machine	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: Security Center standard pricing tier should be selected	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Audit Windows machines that do not restrict the minimum password length to 14 characters	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Audit usage of custom RBAC rules	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Web Application should only be accessible over HTTPS	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Auditing on SQL server should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: The Log Analytics agent should be installed on virtual machines	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: MFA should be enabled on accounts with owner permissions on your subscription	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Advanced data security should be enabled on your SQL servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Advanced data security should be enabled on SQL Managed Instance	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Role-Based Access Control (RBAC) should be used on Kubernetes Services	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Virtual machines should have the Guest Configuration extension	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Monitor missing Endpoint Protection in Azure Security Center	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: Activity log should be retained for at least one year	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Management ports of virtual machines should be protected with just-in-time network access control	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Public network access should be disabled for PostgreSQL servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Deploy Advanced Threat Protection for Cosmos DB Accounts	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Diagnostic logs in App Services should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: API App should only be accessible over HTTPS	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.ClassicNetwork/networkSecurityGroups/delete)	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.ClassicNetwork/networkSecurityGroups/securityRules/delete)	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.Network/networkSecurityGroups/delete)	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.Network/networkSecurityGroups/securityRules/delete)	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: An activity log alert should exist for specific Administrative operations (Microsoft.Sql/servers/firewallRules/delete)	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Non-internet-facing virtual machines should be protected with network security groups	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Audit Windows machines that do not have the password complexity setting enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Defender for container registries should be enabled	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Data Box jobs should enable double encryption for data at rest on the device	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: System updates on virtual machine scale sets should be installed	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Microsoft Antimalware for Azure should be configured to automatically update protection signatures	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: An activity log alert should exist for specific Policy operations (Microsoft.Authorization/policyAssignments/delete)	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Public network access should be disabled for MySQL flexible servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Storage accounts should allow access from trusted Microsoft services	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: Remote debugging should be turned off for Web Applications	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Certificates using RSA cryptography should have the specified minimum key size	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Container registries should not allow unrestricted network access	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Enforce SSL connection should be enabled for PostgreSQL database servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Guest Configuration extension should be deployed to Azure virtual machines with system assigned managed identity	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Long-term geo-redundant backup should be enabled for Azure SQL Databases	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Public network access should be disabled for MySQL servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Audit Windows machines that do not store passwords using reversible encryption	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Windows machines should meet requirements for 'User Rights Assignment'	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Vulnerabilities in security configuration on your machines should be remediated	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Ensure that 'HTTP Version' is the latest, if used to run the Function app	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: MFA should be enabled on accounts with read permissions on your subscription	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: RDP access from the Internet should be blocked	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Audit Linux machines that do not have the passwd file permissions set to 0644	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Subnets should be associated with a Network Security Group	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Enforce SSL connection should be enabled for MySQL database servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Vulnerabilities in container security configurations should be remediated	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Remote debugging should be turned off for API Apps	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Audit Linux machines that allow remote connections from accounts without passwords	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Deprecated accounts with owner permissions should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Double encryption should be enabled on Azure Data Explorer	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Vulnerability assessment should be enabled on your SQL servers	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: The Log Analytics agent should be installed on Virtual Machine Scale Sets	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Latest TLS version should be used in your Web App	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Disk encryption should be enabled on Azure Data Explorer	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Internet-facing virtual machines should be protected with network security groups	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Audit Linux machines that have accounts without passwords	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Azure Synapse workspaces should use customer-managed keys to encrypt data at rest	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: External accounts with owner permissions should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Latest TLS version should be used in your Function App	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: All Internet traffic should be routed via your deployed Azure Firewall	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Linux machines should meet requirements for the Azure security baseline	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Effect for policy: Public network access should be disabled for MariaDB servers	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Vulnerabilities on your SQL databases should be remediated	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Effect for policy: Keys using elliptic curve cryptography should have the specified curve names	For more information about effects, visit https://aka.ms/policyeffects
CMMC Level 3	Policy Assignment	Namespaces excluded from evaluation of policy: Kubernetes cluster pods should only use approved host network and port range	List of Kubernetes namespaces to exclude from policy evaluation.
CMMC Level 3	Policy Assignment	Latest Java version for App Services	Latest supported Java version for App Services
CMMC Level 3	Policy Assignment	Latest Python version for Linux for App Services	Latest supported Python version for App Services
CMMC Level 3	Policy Assignment	Optional: List of VM images that have supported Linux OS to add to scope when auditing Log Analytics agent deployment	Example value: <code>'/subscriptions//resourceGroups/YourResourceGroup/providers/Microsoft.Compute/images/ContosoStdImage'</code>
CMMC Level 3	Policy Assignment	Optional: List of VM images that have supported Windows OS to add to scope when auditing Log Analytics agent deployment	Example value: <code>'/subscriptions//resourceGroups/YourResourceGroup/providers/Microsoft.Compute/images/ContosoStdImage'</code>
CMMC Level 3	Policy Assignment	List of regions where Network Watcher should be enabled	Audit if Network Watcher is not enabled for region(s).
CMMC Level 3	Policy Assignment	List of resource types that should have diagnostic logs enabled	
CMMC Level 3	Policy Assignment	Maximum value in the allowable host port range that pods can use in the host network namespace	The maximum value in the allowable host port range that pods can use in the host network namespace.
CMMC Level 3	Policy Assignment	Minimum RSA key size for keys	The minimum key size for RSA keys.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Minimum RSA key size certificates	The minimum key size for RSA certificates.
CMMC Level 3	Policy Assignment	Minimum TLS version for Windows web servers	Windows web servers with lower TLS versions will be assessed as non-compliant
CMMC Level 3	Policy Assignment	Minimum value in the allowable host port range that pods can use in the host network namespace	The minimum value in the allowable host port range that pods can use in the host network namespace.
CMMC Level 3	Policy Assignment	Mode Requirement	Mode required for all WAF policies
CMMC Level 3	Policy Assignment	Mode Requirement	Mode required for all WAF policies
CMMC Level 3	Policy Assignment	Allowed host paths for pod hostPath volumes to use	The host paths allowed for pod hostPath volumes to use. Provide an empty paths list to block all host paths.
CMMC Level 3	Policy Assignment	Network access: Remotely accessible registry paths	Specifies which registry paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the <code>winreg</code> registry key.
CMMC Level 3	Policy Assignment	Network access: Remotely accessible registry paths and sub-paths	Specifies which registry paths and sub-paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the <code>winreg</code> registry key.
CMMC Level 3	Policy Assignment	Network access: Shares that can be accessed anonymously	Specifies which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server.
CMMC Level 3	Policy Assignment	Network Security: Configure encryption types allowed for Kerberos	Specifies the encryption types that Kerberos is allowed to use.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Network security: LAN Manager authentication level	Specify which challenge-response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers.
CMMC Level 3	Policy Assignment	Network security: LDAP client signing requirements	Specify the level of data signing that is requested on behalf of clients that issue LDAP BIND requests.
CMMC Level 3	Policy Assignment	Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Specifies which behaviors are allowed by clients for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. See https://docs.microsoft.com/windows/security/threat-protection/security-policy-settings/network-security-minimum-session-security-for-ntlm-ssp-based-including-secure-rpc-servers for more information.
CMMC Level 3	Policy Assignment	Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Specifies which behaviors are allowed by servers for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services.
CMMC Level 3	Policy Assignment	Latest PHP version for App Services	Latest supported PHP version for App Services
CMMC Level 3	Policy Assignment	Required retention period (days) for IoT Hub diagnostic logs	
CMMC Level 3	Policy Assignment	Name of the resource group for Network Watcher	Name of the resource group of NetworkWatcher, such as NetworkWatcherRG. This is the resource group where the Network Watchers are located.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Required auditing setting for SQL servers	
CMMC Level 3	Policy Assignment	Azure Data Box SKUs that support software-based double encryption	The list of Azure Data Box SKUs that support software-based double encryption
CMMC Level 3	Policy Assignment	UAC: Admin Approval Mode for the Built-in Administrator account	Specifies the behavior of Admin Approval Mode for the built-in Administrator account.
CMMC Level 3	Policy Assignment	UAC: Behavior of the elevation prompt for administrators in Admin Approval Mode	Specifies the behavior of the elevation prompt for administrators.
CMMC Level 3	Policy Assignment	UAC: Detect application installations and prompt for elevation	Specifies the behavior of application installation detection for the computer.
CMMC Level 3	Policy Assignment	UAC: Run all administrators in Admin Approval Mode	Specifies the behavior of all User Account Control (UAC) policy settings for the computer.
CMMC Level 3	Policy Assignment	User and groups that may force shutdown from a remote system	Specifies which users and groups are permitted to shut down the computer from a remote location on the network.
CMMC Level 3	Policy Assignment	Users and groups that are denied access to this computer from the network	Specifies which users or groups are explicitly prohibited from connecting to the computer across the network.
CMMC Level 3	Policy Assignment	Users and groups that are denied local logon	Specifies which users and groups are explicitly not permitted to log on to the computer.
CMMC Level 3	Policy Assignment	Users and groups that are denied logging on as a batch job	Specifies which users and groups are explicitly not permitted to log on to the computer as a batch job (i.e. scheduled task).
CMMC Level 3	Policy Assignment	Users and groups that are denied logging on as a service	Specifies which service accounts are explicitly not permitted to register a process as a service.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Users and groups that are denied log on through Remote Desktop Services	Specifies which users and groups are explicitly not permitted to log on to the computer via Terminal Services/Remote Desktop Client.
CMMC Level 3	Policy Assignment	Users and groups that may restore files and directories	Specifies which users and groups are permitted to bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories.
CMMC Level 3	Policy Assignment	Users and groups that may shut down the system	Specifies which users and groups who are logged on locally to the computers in your environment are permitted to shut down the operating system with the Shut Down command.
CMMC Level 3	Policy Assignment	Users or groups that may log on locally	Specifies which remote users on the network are permitted to connect to the computer. This does not include Remote Desktop Connection.
CMMC Level 3	Policy Assignment	Users or groups that may back up files and directories	Specifies users and groups allowed to circumvent file and directory permissions to back up the system.
CMMC Level 3	Policy Assignment	Users or groups that may change the system time	Specifies which users and groups are permitted to change the time and date on the internal clock of the computer.
CMMC Level 3	Policy Assignment	Users or groups that may change the time zone	Specifies which users and groups are permitted to change the time zone of the computer.
CMMC Level 3	Policy Assignment	Users or groups that may create a token object	Specifies which users and groups are permitted to create an access token, which may provide elevated rights to access sensitive data.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
CMMC Level 3	Policy Assignment	Users or groups that may log on locally	Specifies which users or groups can interactively log on to the computer. Users who attempt to log on via Remote Desktop Connection or IIS also require this user right.
CMMC Level 3	Policy Assignment	Remote Desktop Users	Users or groups that may log on through Remote Desktop Services
CMMC Level 3	Policy Assignment	Users or groups that may manage auditing and security log	Specifies users and groups permitted to change the auditing options for files and directories and clear the Security log.
CMMC Level 3	Policy Assignment	Users or groups that may take ownership of files or other objects	Specifies which users and groups are permitted to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects to give ownership to the specified user.

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the DoD Impact Level 4 blueprint sample

5/3/2021 • 2 minutes to read • [Edit Online](#)

The Department of Defense Impact Level 4 (DoD IL4) blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific DoD Impact Level 4 controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement DoD Impact Level 4 controls. For latest information on which Azure Clouds and Services meet DoD Impact Level 4 authorization, see [Azure services by FedRAMP and DoD CC SRG audit scope](#).

NOTE

This blueprint sample is available in Azure Government.

Control mapping

The control mapping section provides details on policies included within this blueprint and how these policies address various controls in DoD Impact Level 4. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policies. For more information, see [Azure Policy](#).

Next steps

You've reviewed the overview of the DoD Impact Level 4 blueprint sample. Next, visit the following articles to learn about the control mapping and how to deploy this sample:

[DoD Impact Level 4 blueprint - Control mapping](#) [DoD Impact Level 4 blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Control mapping of the DoD Impact Level 4 blueprint sample

5/3/2021 • 25 minutes to read • [Edit Online](#)

The following article details how the Azure Blueprints Department of Defense Impact Level 4 (DoD IL4) blueprint sample maps to the DoD Impact Level 4 controls. For more information about the controls, see [DoD Cloud Computing Security Requirements Guide \(SRG\)](#). The Defense Information Systems Agency (DISA) is an agency of the US Department of Defense (DoD) that is responsible for developing and maintaining the DoD Cloud Computing Security Requirements Guide (SRG). The SRG defines the baseline security requirements for cloud service providers (CSPs) that host DoD information, systems, and applications, and for DoD's use of cloud services.

The following mappings are to the **DoD Impact Level 4** controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an [Azure Policy](#) initiative. To review the complete initiative, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **[Preview]: DoD Impact Level 4** built-in policy initiative.

IMPORTANT

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy definitions for this compliance blueprint sample may change over time. To view the change history, see the [GitHub Commit History](#).

AC-2 Account Management

This blueprint helps you review accounts that may not comply with your organization's account management requirements. This blueprint assigns [Azure Policy](#) definitions that audit external accounts with read, write, and owner permissions on a subscription and deprecated accounts. By reviewing the accounts audited by these policies, you can take appropriate action to ensure account management requirements are met.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription
- External accounts with owner permissions should be removed from your subscription
- External accounts with read permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription

AC-2 (7) Account Management | Role-Based Schemes

Azure implements [Azure role-based access control \(Azure RBAC\)](#) to help you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint also assigns [Azure Policy](#) definitions to audit use of Azure Active Directory authentication for SQL Servers and Service Fabric. Using Azure Active Directory authentication enables simplified permission management and centralized identity management of database users and other Microsoft services. Additionally, this blueprint assigns an Azure Policy definition to audit the use of custom Azure RBAC

rules. Understanding where custom Azure RBAC rules are implemented can help you verify need and proper implementation, as custom Azure RBAC rules are error prone.

- An Azure Active Directory administrator should be provisioned for SQL servers
- Audit usage of custom RBAC rules
- Service Fabric clusters should only use Azure Active Directory for client authentication

AC-2 (12) Account Management | Account Monitoring / Atypical Usage

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. All JIT requests to access virtual machines are logged in the Activity Log allowing you to monitor for atypical usage. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Just-In-Time network access control should be applied on virtual machines

AC-4 Information Flow Enforcement

Cross origin resource sharing (CORS) can allow App Services resources to be requested from an outside domain. Microsoft recommends that you allow only required domains to interact with your API, function, and web applications. This blueprint assigns an [Azure Policy](#) definition to help you monitor CORS resources access restrictions in Azure Security Center. Understanding CORS implementations can help you verify that information flow controls are implemented.

- CORS should not allow every resource to access your Web Application

AC-5 Separation of Duties

Having only one Azure subscription owner doesn't allow for administrative redundancy. Conversely, having too many Azure subscription owners can increase the potential for a breach via a compromised owner account. This blueprint helps you maintain an appropriate number of Azure subscription owners by assigning [Azure Policy](#) definitions that audit the number of owners for Azure subscriptions. This blueprint also assigns Azure Policy definitions that help you control membership of the Administrators group on Windows virtual machines. Managing subscription owner and virtual machine administrator permissions can help you implement appropriate separation of duties.

- A maximum of 3 owners should be designated for your subscription
- Audit Windows VMs in which the Administrators group contains any of the specified members
- Audit Windows VMs in which the Administrators group does not contain all of the specified members
- Deploy requirements to audit Windows VMs in which the Administrators group contains any of the specified members
- Deploy requirements to audit Windows VMs in which the Administrators group does not contain all of the specified members
- There should be more than one owner assigned to your subscription

AC-6 (7) Least Privilege | Review of User Privileges

Azure implements [Azure role-based access control \(Azure RBAC\)](#) to help you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint assigns [Azure Policy](#) definitions to audit accounts that should be prioritized for review. Reviewing these account indicators can help you ensure least privilege controls are implemented.

- A maximum of 3 owners should be designated for your subscription
- Audit Windows VMs in which the Administrators group contains any of the specified members
- Audit Windows VMs in which the Administrators group does not contain all of the specified members
- Deploy requirements to audit Windows VMs in which the Administrators group contains any of the specified members
- Deploy requirements to audit Windows VMs in which the Administrators group does not contain all of the specified members
- There should be more than one owner assigned to your subscription

AC-17 (1) Remote Access | Automated Monitoring / Control

This blueprint helps you monitor and control remote access by assigning [Azure Policy](#) definitions to monitors that remote debugging for Azure App Service application is turned off and policy definitions that audit Linux virtual machines that allow remote connections from accounts without passwords. This blueprint also assigns an Azure Policy definition that helps you monitor unrestricted access to storage accounts. Monitoring these indicators can help you ensure remote access methods comply with your security policy.

- [Preview]: Audit Linux VMs that allow remote connections from accounts without passwords
- [Preview]: Deploy requirements to audit Linux VMs that allow remote connections from accounts without passwords
- Audit unrestricted network access to storage accounts
- Remote debugging should be turned off for API App
- Remote debugging should be turned off for Function App
- Remote debugging should be turned off for Web Application

AC-23 Data Mining

This blueprint provides policy definitions that help you ensure data security notifications are properly enabled. In addition, this blueprint ensures that auditing and advanced data security are configured on SQL Servers.

- Advanced data security should be enabled on your SQL servers
- Advanced data security should be enabled on your SQL managed instances
- Advanced Threat Protection types should be set to 'All' in SQL server Advanced Data Security settings
- Advanced Threat Protection types should be set to 'All' in SQL managed instance Advanced Data Security settings
- Auditing should be enabled on advanced data security settings on SQL Server
- Email notifications to admins and subscription owners should be enabled in SQL server advanced data security settings
- Email notifications to admins and subscription owners should be enabled in SQL managed instance advanced data security settings
- Advanced data security settings for SQL server should contain an email address to receive security alerts
- Advanced data security settings for SQL managed instance should contain an email address to receive security alerts

AU-3 (2) Content of Audit Records | Centralized Management of Planned Audit Record Content

Log data collected by Azure Monitor is stored in a Log Analytics workspace enabling centralized configuration and management. This blueprint helps you ensure events are logged by assigning [Azure Policy](#) definitions that audit and enforce deployment of the Log Analytics agent on Azure virtual machines.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch
- Deploy Log Analytics agent for Linux virtual machine scale sets
- [Preview]: Deploy Log Analytics Agent for Linux VMs
- Deploy Log Analytics agent for Windows virtual machine scale sets
- [Preview]: Deploy Log Analytics Agent for Windows VMs

AU-5 Response to Audit Processing Failures

This blueprint assigns [Azure Policy](#) definitions that monitor audit and event logging configurations. Monitoring these configurations can provide an indicator of an audit system failure or misconfiguration and help you take corrective action.

- Audit diagnostic setting
- Auditing should be enabled on advanced data security settings on SQL Server
- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers

AU-6 (4) Audit Review, Analysis, and Reporting | Central Review and Analysis

Log data collected by Azure Monitor is stored in a Log Analytics workspace enabling centralized reporting and analysis. This blueprint helps you ensure events are logged by assigning [Azure Policy](#) definitions that audit and enforce deployment of the Log Analytics agent on Azure virtual machines.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch
- Deploy Log Analytics agent for Linux virtual machine scale sets
- [Preview]: Deploy Log Analytics Agent for Linux VMs
- Deploy Log Analytics agent for Windows virtual machine scale sets
- [Preview]: Deploy Log Analytics Agent for Windows VMs

AU-6 (5) Audit Review, Analysis, and Reporting | Integration / Scanning and Monitoring Capabilities

This blueprint provides policy definitions that audit records with analysis of vulnerability assessment on virtual machines, virtual machine scale sets, SQL Database servers, and SQL Managed Instance servers. These policy definitions also audit configuration of diagnostic logs to provide insight into operations that are performed within Azure resources. These insights provide real-time information about the security state of your deployed resources and can help you prioritize remediation actions. For detailed vulnerability scanning and monitoring, we recommend you use Azure Sentinel and Azure Security Center as well.

- [Preview]: Vulnerability Assessment should be enabled on Virtual Machines
- Vulnerability assessment should be enabled on your SQL servers
- Audit diagnostic setting
- Vulnerability assessment should be enabled on your SQL managed instances
- Vulnerability assessment should be enabled on your SQL servers
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities on your SQL databases should be remediated

- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted

AU-12 Audit Generation

This blueprint provides policy definitions that audit and enforce deployment of the Log Analytics agent on Azure virtual machines and configuration of audit settings for other Azure resource types. These policy definitions also audit configuration of diagnostic logs to provide insight into operations that are performed within Azure resources. Additionally, auditing and Advanced Data Security are configured on SQL servers.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch
- Deploy Log Analytics agent for Linux virtual machine scale sets
- [Preview]: Deploy Log Analytics Agent for Linux VMs
- Deploy Log Analytics agent for Windows virtual machine scale sets
- [Preview]: Deploy Log Analytics Agent for Windows VMs
- Audit diagnostic setting
- Auditing should be enabled on advanced data security settings on SQL Server
- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Deploy Auditing on SQL servers
- Deploy Diagnostic Settings for Network Security Groups

AU-12 (01) Audit Generation | System-Wide / Time-Correlated Audit Trail

This blueprint helps you ensure system events are logged by assigning [Azure Policy](#) definitions that audit log settings on Azure resources. This built-in policy requires you to specify an array of resource types to check whether diagnostic settings are enabled or not.

- Audit diagnostic setting

CM-7 (2) Least Functionality | Prevent Program Execution

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application allowlist solution that can block or prevent specific software from running on your virtual machines. Application control can run in an enforcement mode that prohibits non-approved application from running. This blueprint assigns an Azure Policy definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive application controls for defining safe applications should be enabled on your machines

CM-7 (5) Least Functionality | Authorized Software / Whitelisting

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application allowlist solution that can block or prevent specific software from running on your virtual machines. Application control helps you create approved application lists for your virtual machines. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines where an application allowlist is recommended but has

not yet been configured.

- Adaptive application controls for defining safe applications should be enabled on your machines

CM-11 User-Installed Software

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application allowlist solution that can block or prevent specific software from running on your virtual machines. Application control can help you enforce and monitor compliance with software restriction policies. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive application controls for defining safe applications should be enabled on your machines

CP-7 Alternate Processing Site

Azure Site Recovery replicates workloads running on virtual machines from a primary location to a secondary location. If an outage occurs at the primary site, the workload fails over the secondary location. This blueprint assigns an [Azure Policy](#) definition that audits virtual machines without disaster recovery configured. Monitoring this indicator can help you ensure necessary contingency controls are in place.

- Audit virtual machines without disaster recovery configured

CP-9 (05) Information System Backup | Transfer to Alternate Storage Site

This blueprint assigns Azure Policy definitions that audit the organization's system backup information to the alternate storage site electronically. For physical shipment of storage metadata, consider using Azure Data Box.

- Geo-redundant storage should be enabled for Storage Accounts
- Geo-redundant backup should be enabled for Azure Database for PostgreSQL
- Geo-redundant backup should be enabled for Azure Database for MySQL
- Geo-redundant backup should be enabled for Azure Database for MariaDB
- Long-term geo-redundant backup should be enabled for Azure SQL Databases

IA-2 (1) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts

This blueprint helps you restrict and control privileged access by assigning [Azure Policy](#) definitions to audit accounts with owner and/or write permissions that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled on accounts with write permissions on your subscription

IA-2 (2) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

This blueprint helps you restrict and control access by assigning an [Azure Policy](#) definition to audit accounts with read permissions that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be

compromised.

- MFA should be enabled on accounts with read permissions on your subscription

IA-5 Authenticator Management

This blueprint assigns [Azure Policy](#) definitions that audit Linux virtual machines that allow remote connections from accounts without passwords and/or have incorrect permissions set on the passwd file. This blueprint also assigns policy definitions that audit the configuration of the password encryption type for Windows virtual machines. Monitoring these indicators helps you ensure that system authenticators comply with your organization's identification and authentication policy.

- [Preview]: Audit Linux VMs that do not have the passwd file permissions set to 0644
- [Preview]: Audit Linux VMs that have accounts without passwords
- [Preview]: Audit Windows VMs that do not store passwords using reversible encryption
- [Preview]: Deploy requirements to audit Linux VMs that do not have the passwd file permissions set to 0644
- [Preview]: Deploy requirements to audit Linux VMs that have accounts without passwords
- [Preview]: Deploy requirements to audit Windows VMs that do not store passwords using reversible encryption

IA-5 (1) Authenticator Management | Password-Based Authentication

This blueprint helps you enforce strong passwords by assigning [Azure Policy](#) definitions that audit Windows virtual machines that don't enforce minimum strength and other password requirements. Awareness of virtual machines in violation of the password strength policy helps you take corrective actions to ensure passwords for all virtual machine user accounts comply with your organization's password policy.

- [Preview]: Audit Windows VMs that allow re-use of the previous 24 passwords
- [Preview]: Audit Windows VMs that do not have a maximum password age of 70 days
- [Preview]: Audit Windows VMs that do not have a minimum password age of 1 day
- [Preview]: Audit Windows VMs that do not have the password complexity setting enabled
- [Preview]: Audit Windows VMs that do not restrict the minimum password length to 14 characters
- [Preview]: Audit Windows VMs that do not store passwords using reversible encryption
- [Preview]: Deploy requirements to audit Windows VMs that allow re-use of the previous 24 passwords
- [Preview]: Deploy requirements to audit Windows VMs that do not have a maximum password age of 70 days
- [Preview]: Deploy requirements to audit Windows VMs that do not have a minimum password age of 1 day
- [Preview]: Deploy requirements to audit Windows VMs that do not have the password complexity setting enabled
- [Preview]: Deploy requirements to audit Windows VMs that do not restrict the minimum password length to 14 characters
- [Preview]: Deploy requirements to audit Windows VMs that do not store passwords using reversible encryption

IR-6 (2) Incident Reporting | Vulnerabilities Related to Incidents

This blueprint provides policy definitions that audit records with analysis of vulnerability assessment on virtual machines, virtual machine scale sets, and SQL servers. These insights provide real-time information about the security state of your deployed resources and can help you prioritize remediation actions.

- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities in container security configurations should be remediated
- Vulnerabilities on your SQL databases should be remediated

RA-5 Vulnerability Scanning

This blueprint helps you manage information system vulnerabilities by assigning [Azure Policy](#) definitions that monitor operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources. This blueprint also assigns policy definitions that audit and enforce Advanced Data Security on SQL servers. Advanced data security included vulnerability assessment and advanced threat protection capabilities to help you understand vulnerabilities in your deployed resources.

- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities in security configuration on your virtual machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

SC-5 Denial of Service Protection

Azure's distributed denial of service (DDoS) Standard tier provides additional features and mitigation capabilities over the basic service tier. These additional features include Azure Monitor integration and the ability to review post-attack mitigation reports. This blueprint assigns an [Azure Policy](#) definition that audits if the DDoS Standard tier is enabled. Understanding the capability difference between the service tiers can help you select the best solution to address denial of service protections for your Azure environment.

- DDoS Protection Standard should be enabled

SC-7 Boundary Protection

This blueprint helps you manage and control the system boundary by assigning an [Azure Policy](#) definition that monitors for network security group hardening recommendations in Azure Security Center. Azure Security Center analyzes traffic patterns of Internet facing virtual machines and provides network security group rule recommendations to reduce the potential attack surface. Additionally, this blueprint also assigns policy definitions that monitor unprotected endpoints, applications, and storage accounts. Endpoints and applications that aren't protected by a firewall, and storage accounts with unrestricted access can allow unintended access to information contained within the information system.

- Network Security Group Rules for Internet facing virtual machines should be hardened
- Access through Internet facing endpoint should be restricted
- The NSGs rules for web applications on IaaS should be hardened
- Audit unrestricted network access to storage accounts

SC-7 (3) Boundary Protection | Access Points

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT virtual machine access helps you limit the number of external connections to your resources in Azure. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Just-In-Time network access control should be applied on virtual machines

SC-7 (4) Boundary Protection | External Telecommunications Services

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT virtual machine access helps you manage exceptions to your traffic flow policy by facilitating the access request and approval processes. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Just-In-Time network access control should be applied on virtual machines

SC-8 (1) Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection

This blueprint helps you protect the confidential and integrity of transmitted information by assigning [Azure Policy](#) definitions that help you monitor cryptographic mechanism implemented for communications protocols. Ensuring communications are properly encrypted can help you meet your organization's requirements or protecting information from unauthorized disclosure and modification.

- API App should only be accessible over HTTPS
- Audit Windows web servers that are not using secure communication protocols
- Deploy requirements to audit Windows web servers that are not using secure communication protocols
- Function App should only be accessible over HTTPS
- Only secure connections to your Redis Cache should be enabled
- Secure transfer to storage accounts should be enabled
- Web Application should only be accessible over HTTPS

SC-28 (1) Protection of Information at Rest | Cryptographic Protection

This blueprint helps you enforce your policy on the use of cryptograph controls to protect information at rest by assigning [Azure Policy](#) definitions that enforce specific cryptograph controls and audit use of weak cryptographic settings. Understanding where your Azure resources may have non-optimal cryptographic configurations can help you take corrective actions to ensure resources are configured in accordance with your information security policy. Specifically, the policy definitions assigned by this blueprint require encryption for data lake storage accounts; require transparent data encryption on SQL databases; and audit missing encryption on SQL databases, virtual machine disks, and automation account variables.

- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Deploy SQL DB transparent data encryption
- Disk encryption should be applied on virtual machines
- Require encryption on Data Lake Store accounts
- Transparent Data Encryption on SQL databases should be enabled

SI-2 Flaw Remediation

This blueprint helps you manage information system flaws by assigning [Azure Policy](#) definitions that monitor missing system updates, operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources. This blueprint also assigns a policy

definition that ensures patching of the operating system for virtual machine scale sets.

- Require automatic OS image patching on Virtual Machine Scale Sets
- System updates on virtual machine scale sets should be installed
- System updates should be installed on your virtual machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities in security configuration on your virtual machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

SI-02 (06) Flaw Remediation | Removal of Previous Versions of Software / Firmware

This blueprint assigns policy definitions that help you ensure applications are using the latest version of HTTP, Java, PHP, Python, and TLS. This blueprint also assigns a policy definition that ensures that Kubernetes Services is upgraded to its non-vulnerable version.

- Ensure that 'HTTP Version' is the latest, if used to run the API app
- Ensure that 'HTTP Version' is the latest, if used to run the Function app
- Ensure that 'HTTP Version' is the latest, if used to run the Web app
- Ensure that 'Java version' is the latest, if used as a part of the API app
- Ensure that 'Java version' is the latest, if used as a part of the Function app
- Ensure that 'Java version' is the latest, if used as a part of the Web app
- Ensure that 'PHP version' is the latest, if used as a part of the API app
- Ensure that 'PHP version' is the latest, if used as a part of the WEB app
- Ensure that 'Python version' is the latest, if used as a part of the API app
- Ensure that 'Python version' is the latest, if used as a part of the Function app
- Ensure that 'Python version' is the latest, if used as a part of the Web app
- Latest TLS version should be used in your API App
- Latest TLS version should be used in your Function App
- Latest TLS version should be used in your Web App
- Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version

SI-3 Malicious Code Protection

This blueprint helps you manage endpoint protection, including malicious code protection, by assigning [Azure Policy](#) definitions that monitor for missing endpoint protection on virtual machines in Azure Security Center and enforce the Microsoft antimalware solution on Windows virtual machines.

- Deploy default Microsoft IaaS Antimalware extension for Windows Server
- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center

SI-3 (1) Malicious Code Protection | Central Management

This blueprint helps you manage endpoint protection, including malicious code protection, by assigning [Azure Policy](#) definitions that monitor for missing endpoint protection on virtual machines in Azure Security Center. Azure Security Center provides centralized management and reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources.

- Endpoint protection solution should be installed on virtual machine scale sets

- Monitor missing Endpoint Protection in Azure Security Center

SI-4 Information System Monitoring

This blueprint helps you monitor your system by auditing and enforcing logging and data security across Azure resources. Specifically, the policies assigned audit and enforce deployment of the Log Analytics agent, and enhanced security settings for SQL databases, storage accounts and network resources. These capabilities can help you detect anomalous behavior and indicators of attacks so you can take appropriate action.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch
- Deploy Log Analytics agent for Linux virtual machine scale sets
- [Preview]: Deploy Log Analytics Agent for Linux VMs
- Deploy Log Analytics agent for Windows virtual machine scale sets
- [Preview]: Deploy Log Analytics Agent for Windows VMs
- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Deploy Advanced Threat Protection on Storage Accounts
- Deploy Auditing on SQL servers
- Deploy network watcher when virtual networks are created
- Deploy Threat Detection on SQL servers
- Allowed locations
- Allowed locations for resource groups

SI-4 (12) Information System Monitoring | Automated Alerts

This blueprint provides policy definitions that help you ensure data security notifications are properly enabled. In addition, this blueprint ensures that the Standard pricing tier is enabled for Azure Security Center. Note that the Standard pricing tier enables threat detection for networks and virtual machines, providing threat intelligence, anomaly detection, and behavior analytics in Azure Security Center.

- Email notification to subscription owner for high severity alerts should be enabled
- A security contact email address should be provided for your subscription
- Email notifications to admins and subscription owners should be enabled in SQL managed instance advanced data security settings
- Email notifications to admins and subscription owners should be enabled in SQL server advanced data security settings
- A security contact phone number should be provided for your subscription
- Advanced data security settings for SQL server should contain an email address to receive security alerts
- Security Center standard pricing tier should be selected

SI-4 (18) Information System Monitoring | Analyze Traffic / Covert Exfiltration

Advanced Threat Protection for Azure Storage detects unusual and potentially harmful attempts to access or exploit storage accounts. Protection alerts include anomalous access patterns, anomalous extracts/uploads, and suspicious storage activity. These indicators can help you detect covert exfiltration of information.

- Deploy Advanced Threat Protection on Storage Accounts

NOTE

Availability of specific Azure Policy definitions may vary in Azure Government and other national clouds.

Next steps

Now that you've reviewed the control mapping of the DoD Impact Level 4 blueprint, visit the following articles to learn about the blueprint and how to deploy this sample:

[DoD Impact Level 4 blueprint - Overview](#) [DoD Impact Level 4 blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the DoD Impact Level 4 blueprint sample

5/3/2021 • 10 minutes to read • [Edit Online](#)

To deploy the Azure Blueprints Department of Defense Impact Level 4 (DoD IL4) blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure Government subscription, request a [trial subscription](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **DoD Impact Level 4** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the DoD Impact Level 4 blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with DoD Impact Level 4 controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the DoD IL4 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription

within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - **Basics**
 - **Subscriptions:** Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name:** The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location:** Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version:** Pick a **Published** version of your copy of the blueprint sample.
 - **Lock Assignment**

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - **Managed Identity**

Leave the default *system assigned* managed identity option.
 - **Artifact parameters**

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are **priced by product**. Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
---------------	---------------	----------------	-------------

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Allowed locations	Policy Assignment	Allowed Locations	This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements.
Allowed Locations for resource groups	Policy Assignment	Allowed Locations	This policy enables you to restrict the locations your organization can create resource groups in. Use to enforce your geo-compliance requirements.
Deploy Auditing on SQL servers	Policy assignment	The value in days of the retention period (0 indicates unlimited retention)	Retention days (optional, 180 days if unspecified)
Deploy Auditing on SQL servers	Policy assignment	Resource group name for storage account for SQL server auditing	Auditing writes database events to an audit log in your Azure Storage account (a storage account will be created in each region where a SQL Server is created that will be shared by all servers in that region). Important - for proper operation of Auditing do not delete or rename the resource group or the storage accounts.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Storage account prefix for network security group diagnostics	This prefix will be combined with the network security group location to form the created storage account name.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Resource group name for storage account for network security group diagnostics (must exist)	The resource group that the storage account will be created in. This resource group must already exist.
Deploy Log Analytics agent for Linux virtual machine scale sets	Policy assignment	Log Analytics workspace for Linux virtual machine scale sets	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics agent for Linux virtual machine scale sets	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Deploy Log Analytics Agent for Linux VMs	Policy assignment	Log Analytics workspace for Linux VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Log Analytics agent for Windows virtual machine scale sets	Policy assignment	Log Analytics workspace for Windows virtual machine scale sets	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics agent for Windows virtual machine scale sets	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Log Analytics Agent for Windows VMs	Policy assignment	Log Analytics workspace for Windows VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: DoD Impact Level 4	Policy assignment	Members to be included in the Administrators local group	A semicolon-separated list of members that should be excluded in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: DoD Impact Level 4	Policy assignment	Members that should be excluded in the Administrators local group	A semicolon-separated list of members that should be included in the Administrators local group. Ex: Administrator; myUser1; myUser2

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: DoD Impact Level 4	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor diagnostic logs schemas .
[Preview]: DoD Impact Level 4	Policy assignment	Log Analytics workspace ID that VMs should be configured for	This is the ID (GUID) of the Log Analytics workspace that the VMs should be configured for.
[Preview]: DoD Impact Level 4	Policy assignment	Long-term geo-redundant backup should be enabled for Azure SQL Databases	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	Vulnerability assessment should be enabled on your SQL managed instances	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	Vulnerability assessment should be enabled on your SQL servers	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	Geo-redundant storage should be enabled for Storage Accounts	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	Geo-redundant backup should be enabled for Azure Database for MySQL	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	Geo-redundant backup should be enabled for Azure Database for PostgreSQL	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	Web Application should only be accessible over HTTPS	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	Function App should only be accessible over HTTPS	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	External accounts with write permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: DoD Impact Level 4	Policy assignment	External accounts with read permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	External accounts with owner permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	Deprecated accounts with owner permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	Deprecated accounts should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	CORS shouldn't allow every resource to access your Web Application	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	System updates on virtual machine scale sets should be installed	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	MFA should be enabled on accounts with read permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	MFA should be enabled on accounts with owner permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: DoD Impact Level 4	Policy assignment	MFA should be enabled on accounts with write permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .

Next steps

Now that you've reviewed the steps to deploy the DoD Impact Level 4 blueprint sample, visit the following articles to learn about the blueprint and control mapping:

[DoD Impact Level 4 blueprint - Overview](#) [DoD Impact Level 4 blueprint - Control mapping](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).

- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the DoD Impact Level 5 blueprint sample

5/3/2021 • 2 minutes to read • [Edit Online](#)

The Department of Defense Impact Level 5 (DoD IL5) blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific DoD Impact Level 5 controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement DoD Impact Level 5 controls. For latest information on which Azure Clouds and Services meet DoD Impact Level 5 authorization, see [Azure services by FedRAMP and DoD CC SRG audit scope](#).

NOTE

This blueprint sample is available in Azure Government.

Control mapping

The control mapping section provides details on policies included within this blueprint and how these policies address various controls in DoD Impact Level 5. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policies. For more information, see [Azure Policy](#).

Next steps

You've reviewed the overview of the DoD Impact Level 5 blueprint sample. Next, visit the following articles to learn about the control mapping and how to deploy this sample:

[DoD Impact Level 5 blueprint - Control mapping](#) [DoD Impact Level 5 blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Control mapping of the DoD Impact Level 5 blueprint sample

5/3/2021 • 23 minutes to read • [Edit Online](#)

The following article details how the Azure Blueprints Department of Defense Impact Level 5 (DoD IL5) blueprint sample maps to the DoD Impact Level 5 controls. For more information about the controls, see [DoD Cloud Computing Security Requirements Guide \(SRG\)](#). The Defense Information Systems Agency (DISA) is an agency of the US Department of Defense (DoD) that is responsible for developing and maintaining the DoD Cloud Computing Security Requirements Guide (SRG). The SRG defines the baseline security requirements for cloud service providers (CSPs) that host DoD information, systems, and applications, and for DoD's use of cloud services.

The following mappings are to the **DoD Impact Level 5** controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an [Azure Policy](#) initiative. To review the complete initiative, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **[Preview]: DoD Impact Level 5** built-in policy initiative.

IMPORTANT

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy definitions for this compliance blueprint sample may change over time. To view the change history, see the [GitHub Commit History](#).

AC-2 Account Management

This blueprint helps you review accounts that may not comply with your organization's account management requirements. This blueprint assigns [Azure Policy](#) definitions that audit external accounts with read, write, and owner permissions on a subscription and deprecated accounts. By reviewing the accounts audited by these policies, you can take appropriate action to ensure account management requirements are met.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription
- External accounts with owner permissions should be removed from your subscription
- External accounts with read permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription

AC-2 (7) Account Management | Role-Based Schemes

Azure implements [Azure role-based access control \(Azure RBAC\)](#) to help you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint also assigns [Azure Policy](#) definitions to audit use of Azure Active Directory authentication for SQL Servers and Service Fabric. Using Azure Active Directory authentication enables simplified permission management and centralized identity management of database users and other Microsoft services. Additionally, this blueprint assigns an Azure Policy definition to audit the use of custom Azure RBAC

rules. Understanding where custom Azure RBAC rules are implemented can help you verify need and proper implementation, as custom Azure RBAC rules are error prone.

- An Azure Active Directory administrator should be provisioned for SQL servers
- Audit usage of custom RBAC rules
- Service Fabric clusters should only use Azure Active Directory for client authentication

AC-2 (12) Account Management | Account Monitoring / Atypical Usage

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. All JIT requests to access virtual machines are logged in the Activity Log allowing you to monitor for atypical usage. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Management ports of virtual machines should be protected with just-in-time network access control

AC-4 Information Flow Enforcement

Cross origin resource sharing (CORS) can allow App Services resources to be requested from an outside domain. Microsoft recommends that you allow only required domains to interact with your API, function, and web applications. This blueprint assigns an [Azure Policy](#) definition to help you monitor CORS resources access restrictions in Azure Security Center. Understanding CORS implementations can help you verify that information flow controls are implemented.

- CORS should not allow every resource to access your Web Applications

AC-5 Separation of Duties

Having only one Azure subscription owner doesn't allow for administrative redundancy. Conversely, having too many Azure subscription owners can increase the potential for a breach via a compromised owner account. This blueprint helps you maintain an appropriate number of Azure subscription owners by assigning [Azure Policy](#) definitions that audit the number of owners for Azure subscriptions. This blueprint also assigns Azure Policy definitions that help you control membership of the Administrators group on Windows virtual machines. Managing subscription owner and virtual machine administrator permissions can help you implement appropriate separation of duties.

- A maximum of 3 owners should be designated for your subscription
- Show audit results from Windows VMs in which the Administrators group contains any of the specified members
- Show audit results from Windows VMs in which the Administrators group does not contain all of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group contains any of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group does not contain all of the specified members
- There should be more than one owner assigned to your subscription

AC-6 (7) Least Privilege | Review of User Privileges

Azure implements [Azure role-based access control \(Azure RBAC\)](#) to help you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their

permissions. This blueprint assigns [Azure Policy](#) definitions to audit accounts that should be prioritized for review. Reviewing these account indicators can help you ensure least privilege controls are implemented.

- A maximum of 3 owners should be designated for your subscription
- Show audit results from Windows VMs in which the Administrators group contains any of the specified members
- Show audit results from Windows VMs in which the Administrators group does not contain all of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group contains any of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group does not contain all of the specified members
- There should be more than one owner assigned to your subscription

AC-17 (1) Remote Access | Automated Monitoring / Control

This blueprint helps you monitor and control remote access by assigning [Azure Policy](#) definitions to monitors that remote debugging for Azure App Service application is turned off and policy definitions that audit Linux virtual machines that allow remote connections from accounts without passwords. This blueprint also assigns an Azure Policy definition that helps you monitor unrestricted access to storage accounts. Monitoring these indicators can help you ensure remote access methods comply with your security policy.

- Show audit results from Linux VMs that allow remote connections from accounts without passwords
- Deploy prerequisites to audit Linux VMs that allow remote connections from accounts without passwords
- Storage accounts should restrict network access
- Remote debugging should be turned off for API Apps
- Remote debugging should be turned off for Function Apps
- Remote debugging should be turned off for Web Applications

AC-23 Data Mining

This blueprint ensures that auditing and advanced data security are configured on SQL Servers.

- Advanced data security should be enabled on your SQL servers
- Advanced data security should be enabled on SQL Managed Instance
- Auditing on SQL server should be enabled

AU-3 (2) Content of Audit Records | Centralized Management of Planned Audit Record Content

Log data collected by Azure Monitor is stored in a Log Analytics workspace enabling centralized configuration and management. This blueprint helps you ensure events are logged by assigning [Azure Policy](#) definitions that audit and enforce deployment of the Log Analytics agent on Azure virtual machines.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Audit Log Analytics workspace for VM - Report Mismatch
- The Log Analytics agent should be installed on Virtual Machine Scale Sets
- The Log Analytics agent should be installed on virtual machines

AU-5 Response to Audit Processing Failures

This blueprint assigns [Azure Policy](#) definitions that monitor audit and event logging configurations. Monitoring these configurations can provide an indicator of an audit system failure or misconfiguration and help you take corrective action.

- Audit diagnostic setting
- Auditing on SQL server should be enabled
- Advanced data security should be enabled on SQL Managed Instance
- Advanced data security should be enabled on your SQL servers

AU-6 (4) Audit Review, Analysis, and Reporting | Central Review and Analysis

Log data collected by Azure Monitor is stored in a Log Analytics workspace enabling centralized reporting and analysis. This blueprint helps you ensure events are logged by assigning [Azure Policy](#) definitions that audit and enforce deployment of the Log Analytics agent on Azure virtual machines.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Audit Log Analytics workspace for VM - Report Mismatch

AU-6 (5) Audit Review, Analysis, and Reporting | Integration / Scanning and Monitoring Capabilities

This blueprint provides policy definitions that audit records with analysis of vulnerability assessment on virtual machines, virtual machine scale sets, SQL Database servers, and SQL Managed Instance servers. These policy definitions also audit configuration of diagnostic logs to provide insight into operations that are performed within Azure resources. These insights provide real-time information about the security state of your deployed resources and can help you prioritize remediation actions. For detailed vulnerability scanning and monitoring, we recommend you use Azure Sentinel and Azure Security Center as well.

- Audit diagnostic setting
- Vulnerability assessment should be enabled on SQL Managed Instance
- Vulnerability assessment should be enabled on your SQL servers
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted

AU-12 Audit Generation

This blueprint provides policy definitions that audit and enforce deployment of the Log Analytics agent on Azure virtual machines and configuration of audit settings for other Azure resource types. These policy definitions also audit configuration of diagnostic logs to provide insight into operations that are performed within Azure resources. Additionally, auditing and Advanced Data Security are configured on SQL servers.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Audit Log Analytics workspace for VM - Report Mismatch
- Audit diagnostic setting
- Auditing on SQL server should be enabled

- Advanced data security should be enabled on SQL Managed Instance
- Advanced data security should be enabled on your SQL servers

AU-12 (01) Audit Generation | System-Wide / Time-Correlated Audit Trail

This blueprint helps you ensure system events are logged by assigning [Azure Policy](#) definitions that audit log settings on Azure resources. This built-in policy requires you to specify an array of resource types to check whether diagnostic settings are enabled or not.

- Audit diagnostic setting

CM-7 (2) Least Functionality | Prevent Program Execution

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application allowlist solution that can block or prevent specific software from running on your virtual machines. Application control can run in an enforcement mode that prohibits non-approved application from running. This blueprint assigns an Azure Policy definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive application controls for defining safe applications should be enabled on your machines

CM-7 (5) Least Functionality | Authorized Software / Whitelisting

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application allowlist solution that can block or prevent specific software from running on your virtual machines. Application control helps you create approved application lists for your virtual machines. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive application controls for defining safe applications should be enabled on your machines

CM-11 User-Installed Software

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application allowlist solution that can block or prevent specific software from running on your virtual machines. Application control can help you enforce and monitor compliance with software restriction policies. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive application controls for defining safe applications should be enabled on your machines

CP-7 Alternate Processing Site

Azure Site Recovery replicates workloads running on virtual machines from a primary location to a secondary location. If an outage occurs at the primary site, the workload fails over the secondary location. This blueprint assigns an [Azure Policy](#) definition that audits virtual machines without disaster recovery configured. Monitoring this indicator can help you ensure necessary contingency controls are in place.

- Audit virtual machines without disaster recovery configured

CP-9 (05) Information System Backup | Transfer to Alternate Storage Site

This blueprint assigns Azure Policy definitions that audit the organization's system backup information to the

alternate storage site electronically. For physical shipment of storage metadata, consider using Azure Data Box.

- Geo-redundant storage should be enabled for Storage Accounts
- Geo-redundant backup should be enabled for Azure Database for PostgreSQL
- Geo-redundant backup should be enabled for Azure Database for MySQL
- Long-term geo-redundant backup should be enabled for Azure SQL Databases

IA-2 (1) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts

This blueprint helps you restrict and control privileged access by assigning [Azure Policy](#) definitions to audit accounts with owner and/or write permissions that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription

IA-2 (2) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

This blueprint helps you restrict and control access by assigning an [Azure Policy](#) definition to audit accounts with read permissions that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with read permissions on your subscription

IA-5 Authenticator Management

This blueprint assigns [Azure Policy](#) definitions that audit Linux virtual machines that allow remote connections from accounts without passwords and/or have incorrect permissions set on the passwd file. This blueprint also assigns policy definitions that audit the configuration of the password encryption type for Windows virtual machines. Monitoring these indicators helps you ensure that system authenticators comply with your organization's identification and authentication policy.

- Show audit results from Linux VMs that do not have the passwd file permissions set to 0644
- Show audit results from Linux VMs that have accounts without passwords
- Show audit results from Windows VMs that do not store passwords using reversible encryption
- Deploy prerequisites to audit Linux VMs that do not have the passwd file permissions set to 0644
- Deploy prerequisites to audit Linux VMs that have accounts without passwords
- Deploy prerequisites to audit Windows VMs that do not store passwords using reversible encryption

IA-5 (1) Authenticator Management | Password-Based Authentication

This blueprint helps you enforce strong passwords by assigning [Azure Policy](#) definitions that audit Windows virtual machines that don't enforce minimum strength and other password requirements. Awareness of virtual machines in violation of the password strength policy helps you take corrective actions to ensure passwords for all virtual machine user accounts comply with your organization's password policy.

- Show audit results from Windows VMs that allow re-use of the previous 24 passwords

- Show audit results from Windows VMs that do not have a maximum password age of 70 days
- Show audit results from Windows VMs that do not have a minimum password age of 1 day
- Show audit results from Windows VMs that do not have the password complexity setting enabled
- Show audit results from Windows VMs that do not restrict the minimum password length to 14 characters
- Show audit results from Windows VMs that do not store passwords using reversible encryption
- Deploy prerequisites to audit Windows VMs that allow re-use of the previous 24 passwords
- Deploy prerequisites to audit Windows VMs that do not have a maximum password age of 70 days
- Deploy prerequisites to audit Windows VMs that do not have a minimum password age of 1 day
- Deploy prerequisites to audit Windows VMs that do not have the password complexity setting enabled
- Deploy prerequisites to audit Windows VMs that do not restrict the minimum password length to 14 characters
- Deploy prerequisites to audit Windows VMs that do not store passwords using reversible encryption

IR-6 (2) Incident Reporting | Vulnerabilities Related to Incidents

This blueprint provides policy definitions that audit records with analysis of vulnerability assessment on virtual machines, virtual machine scale sets, and SQL servers. These insights provide real-time information about the security state of your deployed resources and can help you prioritize remediation actions.

- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities in container security configurations should be remediated
- Vulnerabilities on your SQL databases should be remediated

RA-5 Vulnerability Scanning

This blueprint helps you manage information system vulnerabilities by assigning [Azure Policy](#) definitions that monitor operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources. This blueprint also assigns policy definitions that audit and enforce Advanced Data Security on SQL servers. Advanced data security included vulnerability assessment and advanced threat protection capabilities to help you understand vulnerabilities in your deployed resources.

- Advanced data security should be enabled on SQL Managed Instance
- Advanced data security should be enabled on your SQL servers
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

SC-5 Denial of Service Protection

Azure's distributed denial of service (DDoS) Standard tier provides additional features and mitigation capabilities over the basic service tier. These additional features include Azure Monitor integration and the ability to review post-attack mitigation reports. This blueprint assigns an [Azure Policy](#) definition that audits if the DDoS Standard tier is enabled. Understanding the capability difference between the service tiers can help you select the best solution to address denial of service protections for your Azure environment.

- Azure DDoS Protection Standard should be enabled

SC-7 Boundary Protection

This blueprint helps you manage and control the system boundary by assigning an [Azure Policy](#) definition that monitors for network security group hardening recommendations in Azure Security Center. Azure Security Center analyzes traffic patterns of Internet facing virtual machines and provides network security group rule recommendations to reduce the potential attack surface. Additionally, this blueprint also assigns policy definitions that monitor unprotected endpoints, applications, and storage accounts. Endpoints and applications that aren't protected by a firewall, and storage accounts with unrestricted access can allow unintended access to information contained within the information system.

- Access through Internet facing endpoint should be restricted
- Storage accounts should restrict network access

SC-7 (3) Boundary Protection | Access Points

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT virtual machine access helps you limit the number of external connections to your resources in Azure. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Management ports of virtual machines should be protected with just-in-time network access control

SC-7 (4) Boundary Protection | External Telecommunications Services

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT virtual machine access helps you manage exceptions to your traffic flow policy by facilitating the access request and approval processes. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Just-In-Time network access control should be applied on virtual machines

SC-8 (1) Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection

This blueprint helps you protect the confidentiality and integrity of transmitted information by assigning [Azure Policy](#) definitions that help you monitor cryptographic mechanism implemented for communications protocols. Ensuring communications are properly encrypted can help you meet your organization's requirements or protecting information from unauthorized disclosure and modification.

- API App should only be accessible over HTTPS
- Show audit results from Windows web servers that are not using secure communication protocols
- Deploy prerequisites to audit Windows web servers that are not using secure communication protocols
- Function App should only be accessible over HTTPS
- Only secure connections to your Azure Cache for Redis should be enabled
- Secure transfer to storage accounts should be enabled
- Web Application should only be accessible over HTTPS

SC-28 (1) Protection of Information at Rest | Cryptographic Protection

This blueprint helps you enforce your policy on the use of cryptograph controls to protect information at rest by assigning [Azure Policy](#) definitions that enforce specific cryptograph controls and audit use of weak

cryptographic settings. Understanding where your Azure resources may have non-optimal cryptographic configurations can help you take corrective actions to ensure resources are configured in accordance with your information security policy. Specifically, the policy definitions assigned by this blueprint require encryption for data lake storage accounts; require transparent data encryption on SQL databases; and audit missing encryption on SQL databases, virtual machine disks, and automation account variables.

- Advanced data security should be enabled on SQL Managed Instance
- Advanced data security should be enabled on your SQL servers
- Disk encryption should be applied on virtual machines
- Transparent Data Encryption on SQL databases should be enabled

SI-2 Flaw Remediation

This blueprint helps you manage information system flaws by assigning [Azure Policy](#) definitions that monitor missing system updates, operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources. This blueprint also assigns a policy definition that ensures patching of the operating system for virtual machine scale sets.

- System updates on virtual machine scale sets should be installed
- System updates should be installed on your machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

SI-02 (06) Flaw Remediation | Removal of Previous Versions of Software / Firmware

This blueprint assigns policy definitions that help you ensure applications are using the latest version of HTTP, Java, PHP, Python, and TLS. This blueprint also assigns a policy definition that ensures that Kubernetes Services is upgraded to its non-vulnerable version.

- Ensure that 'HTTP Version' is the latest, if used to run the API app
- Ensure that 'HTTP Version' is the latest, if used to run the Function app
- Ensure that 'HTTP Version' is the latest, if used to run the Web app
- Ensure that 'Java version' is the latest, if used as a part of the API app
- Ensure that 'Java version' is the latest, if used as a part of the Function app
- Ensure that 'Java version' is the latest, if used as a part of the Web app
- Ensure that 'PHP version' is the latest, if used as a part of the API app
- Ensure that 'PHP version' is the latest, if used as a part of the WEB app
- Ensure that 'Python version' is the latest, if used as a part of the API app
- Ensure that 'Python version' is the latest, if used as a part of the Function app
- Ensure that 'Python version' is the latest, if used as a part of the Web app
- Latest TLS version should be used in your API App
- Latest TLS version should be used in your Function App
- Latest TLS version should be used in your Web App
- Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version

SI-3 Malicious Code Protection

This blueprint helps you manage endpoint protection, including malicious code protection, by assigning [Azure Policy](#) definitions that monitor for missing endpoint protection on virtual machines in Azure Security Center and enforce the Microsoft antimalware solution on Windows virtual machines.

- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center
- Microsoft IaaS Antimalware extension should be deployed on Windows servers

SI-3 (1) Malicious Code Protection | Central Management

This blueprint helps you manage endpoint protection, including malicious code protection, by assigning [Azure Policy](#) definitions that monitor for missing endpoint protection on virtual machines in Azure Security Center. Azure Security Center provides centralized management and reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources.

- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center

SI-4 Information System Monitoring

This blueprint helps you monitor your system by auditing and enforcing logging and data security across Azure resources. Specifically, the policies assigned audit and enforce deployment of the Log Analytics agent, and enhanced security settings for SQL databases, storage accounts and network resources. These capabilities can help you detect anomalous behavior and indicators of attacks so you can take appropriate action.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Audit Log Analytics workspace for VM - Report Mismatch
- Advanced data security should be enabled on SQL Managed Instance
- Advanced data security should be enabled on your SQL servers
- Network Watcher should be enabled

SI-4 (12) Information System Monitoring | Automated Alerts

This blueprint provides policy definitions that help you ensure data security notifications are properly enabled. In addition, this blueprint ensures that the Standard pricing tier is enabled for Azure Security Center. Note that the Standard pricing tier enables threat detection for networks and virtual machines, providing threat intelligence, anomaly detection, and behavior analytics in Azure Security Center.

- Email notification to subscription owner for high severity alerts should be enabled
- A security contact email address should be provided for your subscription
- A security contact phone number should be provided for your subscription

NOTE

Availability of specific Azure Policy definitions may vary in Azure Government and other national clouds.

Next steps

Now that you've reviewed the control mapping of the DoD Impact Level 5 blueprint, visit the following articles to learn about the blueprint and how to deploy this sample:

[DoD Impact Level 5 blueprint - Overview](#) [DoD Impact Level 5 blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the DoD Impact Level 5 blueprint sample

5/3/2021 • 18 minutes to read • [Edit Online](#)

To deploy the Azure Blueprints Department of Defense Impact Level 5 (DoD IL5) blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure Government subscription, request a [trial subscription](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **DoD Impact Level 5** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the DoD Impact Level 5 blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with DoD Impact Level 5 controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the DoD IL5 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription

within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - **Basics**
 - **Subscriptions:** Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name:** The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location:** Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version:** Pick a **Published** version of your copy of the blueprint sample.
 - **Lock Assignment**

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - **Managed Identity**

Leave the default *system assigned* managed identity option.
 - **Artifact parameters**

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are **priced by product**. Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
---------------	---------------	----------------	-------------

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
DoD Impact Level 5	Policy Assignment	List of users that must be included in Windows VM Administrators group	A semicolon-separated list of users that should be included in the Administrators local group; Ex: Administrator; myUser1; myUser2
DoD Impact Level 5	Policy Assignment	List of users excluded from Windows VM Administrators group	A semicolon-separated list of users that should be excluded in the Administrators local group; Ex: Administrator; myUser1; myUser2
DoD Impact Level 5	Policy Assignment	List of resource types that should have diagnostic logs enabled	
DoD Impact Level 5	Policy Assignment	Log Analytics workspace ID for VM agent reporting	ID (GUID) of the Log Analytics workspace where VMs agents should report
DoD Impact Level 5	Policy Assignment	List of regions where Network Watcher should be enabled	To see a complete list of regions use Get-AzLocation,
DoD Impact Level 5	Policy Assignment	Minimum TLS version for Windows web servers	The minimum TLS protocol version that should be enabled on Windows web servers
DoD Impact Level 5	Policy Assignment	Latest PHP version	Latest supported PHP version for App Services
DoD Impact Level 5	Policy Assignment	Latest Java version	Latest supported Java version for App Services
DoD Impact Level 5	Policy Assignment	Latest Windows Python version	Latest supported Python version for App Services
DoD Impact Level 5	Policy Assignment	Latest Linux Python version	Latest supported Python version for App Services
DoD Impact Level 5	Policy Assignment	Optional: List of Windows VM images that support Log Analytics agent to add to audit scope	A semicolon-separated list of images; Ex: /subscriptions//resourceGroups/YourResourceGroup/providers/Microsoft.Compute/images/ContosoStdImage
DoD Impact Level 5	Policy Assignment	Optional: List of Linux VM images that support Log Analytics agent to add to audit scope	A semicolon-separated list of images; Ex: /subscriptions//resourceGroups/YourResourceGroup/providers/Microsoft.Compute/images/ContosoStdImage

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
DoD Impact Level 5	Policy Assignment	Effect for policy: There should be more than one owner assigned to your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Disk encryption should be applied on virtual machines	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Email notification to subscription owner for high severity alerts should be enabled	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Remote debugging should be turned off for Function Apps	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that '.NET Framework' version is the latest, if used as a part of the Function App	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Transparent Data Encryption on SQL databases should be enabled	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Vulnerability assessment should be enabled on your SQL managed instances	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'PHP version' is the latest, if used as a part of the API app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: An Azure Active Directory administrator should be provisioned for SQL servers	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Only secure connections to your Redis Cache should be enabled	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Endpoint protection solution should be installed on virtual machine scale sets	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
DoD Impact Level 5	Policy Assignment	Effect for policy: Audit unrestricted network access to storage accounts	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Advanced data security settings for SQL managed instance should contain an email address to receive security alerts	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Vulnerabilities in security configuration on your virtual machine scale sets should be remediated	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Secure transfer to storage accounts should be enabled	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Adaptive Application Controls should be enabled on virtual machines	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Geo-redundant backup should be enabled for Azure Database for PostgreSQL	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'Java version' is the latest, if used as a part of the Web app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: A maximum of 3 owners should be designated for your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: A security contact email address should be provided for your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: CORS should not allow every resource to access your Web Applications	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
DoD Impact Level 5	Policy Assignment	Effect for policy: External accounts with write permissions should be removed from your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: External accounts with read permissions should be removed from your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Deprecated accounts should be removed from your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Function App should only be accessible over HTTPS	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'Python version' is the latest, if used as a part of the Web app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'Python version' is the latest, if used as a part of the Function app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'PHP version' is the latest, if used as a part of the WEB app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'Python version' is the latest, if used as a part of the API app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Vulnerabilities should be remediated by a Vulnerability Assessment solution	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Geo-redundant backup should be enabled for Azure Database for MySQL	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that '.NET Framework' version is the latest, if used as a part of the Web app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
DoD Impact Level 5	Policy Assignment	Effect for policy: System updates should be installed on your machines	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'Java version' is the latest, if used as a part of the API app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'HTTP Version' is the latest, if used to run the Web app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Latest TLS version should be used in your API App	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: MFA should be enabled accounts with write permissions on your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Advanced data security settings for SQL server should contain an email address to receive security alerts	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'HTTP Version' is the latest, if used to run the API app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Microsoft IaaS Antimalware extension should be deployed on Windows servers	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'Java version' is the latest, if used as a part of the Function app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Access through Internet facing endpoint should be restricted	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Security Center standard pricing tier should be selected	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
DoD Impact Level 5	Policy Assignment	Effect for policy: Audit usage of custom RBAC rules	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Web Application should only be accessible over HTTPS	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Auditing on SQL server should be enabled	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: The Log Analytics agent should be installed on virtual machines	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: DDoS Protection Standard should be enabled	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: MFA should be enabled on accounts with owner permissions on your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'PHP version' is the latest, if used as a part of the Function app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Advanced data security should be enabled on your SQL servers	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Advanced data security should be enabled on your SQL managed instances	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Email notifications to admins and subscription owners should be enabled in SQL managed instance advanced data security settings	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Monitor missing Endpoint Protection in Azure Security Center	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
DoD Impact Level 5	Policy Assignment	Effect for policy: Just-In-Time network access control should be applied on virtual machines	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: A security contact phone number should be provided for your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Service Fabric clusters should only use Azure Active Directory for client authentication	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: API App should only be accessible over HTTPS	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Advanced Threat Protection types should be set to 'All' in SQL managed instance Advanced Data Security settings	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Geo-redundant storage should be enabled for Storage Accounts	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that '.NET Framework' version is the latest, if used as a part of the API app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: System updates on virtual machine scale sets should be installed	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Email notifications to admins and subscription owners should be enabled in SQL server advanced data security settings	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Remote debugging should be turned off for Web Applications	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
DoD Impact Level 5	Policy Assignment	Effect for policy: Long-term geo-redundant backup should be enabled for Azure SQL Databases	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Vulnerabilities in security configuration on your machines should be remediated	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Ensure that 'HTTP Version' is the latest, if used to run the Function app	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: MFA should be enabled on accounts with read permissions on your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Advanced Threat Protection types should be set to 'All' in SQL server Advanced Data Security settings	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Vulnerabilities in container security configurations should be remediated	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Remote debugging should be turned off for API Apps	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Deprecated accounts with owner permissions should be removed from your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Vulnerability assessment should be enabled on your SQL servers	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: The Log Analytics agent should be installed on Virtual Machine Scale Sets	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
DoD Impact Level 5	Policy Assignment	Effect for policy: Latest TLS version should be used in your Web App	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: External accounts with owner permissions should be removed from your subscription	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Latest TLS version should be used in your Function App	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: [Preview]: Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects
DoD Impact Level 5	Policy Assignment	Effect for policy: Vulnerabilities on your SQL databases should be remediated	Azure Policy effect for this policy; for more information about effects, visit https://aka.ms/policyeffects

Next steps

Now that you've reviewed the steps to deploy the DoD Impact Level 5 blueprint sample, visit the following articles to learn about the blueprint and control mapping:

[DoD Impact Level 5 blueprint - Overview](#) [DoD Impact Level 5 blueprint - Control mapping](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the FedRAMP Moderate blueprint sample

5/3/2021 • 2 minutes to read • [Edit Online](#)

The FedRAMP Moderate blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific FedRAMP Moderate controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement FedRAMP Moderate controls.

Control mapping

The control mapping section provides details on policies included within this blueprint and how these policies address various controls in FedRAMP Moderate. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policies. For more information, see [Azure Policy](#).

Next steps

You've reviewed the overview and of the FedRAMP Moderate blueprint sample. Next, visit the following articles to learn about the control mapping and how to deploy this sample:

[FedRAMP Moderate blueprint - Control mapping](#) [FedRAMP Moderate blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Control mapping of the FedRAMP Moderate blueprint sample

5/3/2021 • 17 minutes to read • [Edit Online](#)

The following article details how the Azure Blueprints FedRAMP Moderate blueprint sample maps to the FedRAMP Moderate controls. For more information about the controls, see [FedRAMP Security Controls Baseline](#).

The following mappings are to the **FedRAMP Moderate** controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an [Azure Policy](#) initiative. To review the complete initiative, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **[Preview]: Audit FedRAMP Moderate controls and deploy specific VM Extensions to support audit requirements** built-in policy initiative.

IMPORTANT

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy definitions for this compliance blueprint sample may change over time. To view the change history, see the [GitHub Commit History](#).

AC-2 Account Management

This blueprint helps you review accounts that may not comply with your organization's account management requirements. This blueprint assigns [Azure Policy](#) definitions that audit external accounts with read, write, and owner permissions on a subscription and deprecated accounts. By reviewing the accounts audited by these policies, you can take appropriate action to ensure account management requirements are met.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription
- External accounts with owner permissions should be removed from your subscription
- External accounts with read permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription

AC-2 (7) Account Management | Role-Based Schemes

[Azure role-based access control \(Azure RBAC\)](#) helps you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint also assigns [Azure Policy](#) definitions to audit use of Azure Active Directory authentication for SQL Servers and Service Fabric. Using Azure Active Directory authentication enables simplified permission management and centralized identity management of database users and other Microsoft services. Additionally, this blueprint assigns an Azure Policy definition to audit the use of custom Azure RBAC rules. Understanding where custom Azure RBAC rules are implemented can help you verify need and proper implementation, as custom Azure RBAC rules are error prone.

- An Azure Active Directory administrator should be provisioned for SQL servers
- Audit usage of custom RBAC rules

- Service Fabric clusters should only use Azure Active Directory for client authentication

AC-2 (12) Account Management | Account Monitoring / Atypical Usage

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. All JIT requests to access virtual machines are logged in the Activity Log allowing you to monitor for atypical usage. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Just-In-Time network access control should be applied on virtual machines

AC-4 Information Flow Enforcement

Cross origin resource sharing (CORS) can allow App Services resources to be requested from an outside domain. Microsoft recommends that you allow only required domains to interact with your API, function, and web applications. This blueprint assigns an [Azure Policy](#) definition to help you monitor CORS resources access restrictions in Azure Security Center. Understanding CORS implementations can help you verify that information flow controls are implemented.

- CORS should not allow every resource to access your Web Application

AC-5 Separation of Duties

Having only one Azure subscription owner doesn't allow for administrative redundancy. Conversely, having too many Azure subscription owners can increase the potential for a breach via a compromised owner account. This blueprint helps you maintain an appropriate number of Azure subscription owners by assigning [Azure Policy](#) definitions that audit the number of owners for Azure subscriptions. This blueprint also assigns Azure Policy definitions that help you control membership of the Administrators group on Windows virtual machines. Managing subscription owner and virtual machine administrator permissions can help you implement appropriate separation of duties.

- A maximum of 3 owners should be designated for your subscription
- Audit Windows VMs in which the Administrators group contains any of the specified members
- Audit Windows VMs in which the Administrators group does not contain all of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group contains any of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group does not contain all of the specified members
- There should be more than one owner assigned to your subscription

AC-17 (1) Remote Access | Automated Monitoring / Control

This blueprint helps you monitor and control remote access by assigning [Azure Policy](#) definitions to monitors that remote debugging for Azure App Service application is turned off and policy definitions that audit Linux virtual machines that allow remote connections from accounts without passwords. This blueprint also assigns an Azure Policy definition that helps you monitor unrestricted access to storage accounts. Monitoring these indicators can help you ensure remote access methods comply with your security policy.

- [Preview]: Audit Linux VMs that allow remote connections from accounts without passwords
- [Preview]: Deploy requirements to audit Linux VMs that allow remote connections from accounts without passwords

- Audit unrestricted network access to storage accounts
- Remote debugging should be turned off for API App
- Remote debugging should be turned off for Function App
- Remote debugging should be turned off for Web Application

AU-5 Response to Audit Processing Failures

This blueprint assigns [Azure Policy](#) definitions that monitor audit and event logging configurations. Monitoring these configurations can provide an indicator of an audit system failure or misconfiguration and help you take corrective action.

- Audit diagnostic setting
- Auditing on SQL server should be enabled
- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers

AU-12 Audit Generation

This blueprint helps you ensure system events are logged by assigning [Azure Policy](#) definitions that audit log settings on Azure resources. These policy definitions audit and enforce deployment of the Log Analytics agent on Azure virtual machines and configuration of audit settings for other Azure resource types. These policy definitions also audit configuration of diagnostic logs to provide insight into operations that are performed within Azure resources. Additionally, auditing and Advanced Data Security are configured on SQL servers.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment in VMSS - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch
- [Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Linux VMs
- [Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Windows VMs
- Audit diagnostic setting
- Auditing on SQL server should be enabled
- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Deploy Auditing on SQL servers
- Deploy Diagnostic Settings for Network Security Groups

CM-7 (2) Least Functionality | Prevent Program Execution

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application filtering solution that can block or prevent specific software from running on your virtual machines. Application control can run in an enforcement mode that prohibits non-approved application from running. This blueprint assigns an Azure Policy definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive Application Controls should be enabled on virtual machines

CM-7 (5) Least Functionality | Authorized Software / Whitelisting

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application

filtering solution that can block or prevent specific software from running on your virtual machines. Application control helps you create approved application lists for your virtual machines. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive Application Controls should be enabled on virtual machines

CM-11 User-Installed Software

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application filtering solution that can block or prevent specific software from running on your virtual machines. Application control can help you enforce and monitor compliance with software restriction policies. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive Application Controls should be enabled on virtual machines

CP-7 Alternate Processing Site

Azure Site Recovery replicates workloads running on virtual machines from a primary location to a secondary location. If an outage occurs at the primary site, the workload fails over the secondary location. This blueprint assigns an [Azure Policy](#) definition that audits virtual machines without disaster recovery configured. Monitoring this indicator can help you ensure necessary contingency controls are in place.

- Audit virtual machines without disaster recovery configured

IA-2 (1) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts

This blueprint helps you restrict and control privileged access by assigning [Azure Policy](#) definitions to audit accounts with owner and/or write permissions that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled on accounts with write permissions on your subscription

IA-2 (2) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

This blueprint helps you restrict and control access by assigning an [Azure Policy](#) definition to audit accounts with read permissions that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with read permissions on your subscription

IA-5 Authenticator Management

This blueprint assigns [Azure Policy](#) definitions that audit Linux virtual machines that allow remote connections from accounts without passwords and/or have incorrect permissions set on the passwd file. This blueprint also assigns policy definitions that audit the configuration of the password encryption type for Windows virtual

machines. Monitoring these indicators helps you ensure that system authenticators comply with your organization's identification and authentication policy.

- [Preview]: Audit Linux VMs that do not have the passwd file permissions set to 0644
- [Preview]: Audit Linux VMs that have accounts without passwords
- [Preview]: Audit Windows VMs that do not store passwords using reversible encryption
- [Preview]: Deploy requirements to audit Linux VMs that do not have the passwd file permissions set to 0644
- [Preview]: Deploy requirements to audit Linux VMs that have accounts without passwords
- [Preview]: Deploy requirements to audit Windows VMs that do not store passwords using reversible encryption

IA-5 (1) Authenticator Management | Password-Based Authentication

This blueprint helps you enforce strong passwords by assigning [Azure Policy](#) definitions that audit Windows virtual machines that don't enforce minimum strength and other password requirements. Awareness of virtual machines in violation of the password strength policy helps you take corrective actions to ensure passwords for all virtual machine user accounts comply with your organization's password policy.

- [Preview]: Audit Windows VMs that allow re-use of the previous 24 passwords
- [Preview]: Audit Windows VMs that do not have a maximum password age of 70 days
- [Preview]: Audit Windows VMs that do not have a minimum password age of 1 day
- [Preview]: Audit Windows VMs that do not have the password complexity setting enabled
- [Preview]: Audit Windows VMs that do not restrict the minimum password length to 14 characters
- [Preview]: Audit Windows VMs that do not store passwords using reversible encryption
- [Preview]: Deploy requirements to audit Windows VMs that allow re-use of the previous 24 passwords
- [Preview]: Deploy requirements to audit Windows VMs that do not have a maximum password age of 70 days
- [Preview]: Deploy requirements to audit Windows VMs that do not have a minimum password age of 1 day
- [Preview]: Deploy requirements to audit Windows VMs that do not have the password complexity setting enabled
- [Preview]: Deploy requirements to audit Windows VMs that do not restrict the minimum password length to 14 characters
- [Preview]: Deploy requirements to audit Windows VMs that do not store passwords using reversible encryption

RA-5 Vulnerability Scanning

This blueprint helps you manage information system vulnerabilities by assigning [Azure Policy](#) definitions that monitor operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources. This blueprint also assigns policy definitions that audit and enforce Advanced Data Security on SQL servers. Advanced data security included vulnerability assessment and advanced threat protection capabilities to help you understand vulnerabilities in your deployed resources.

- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities in security configuration on your virtual machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

SC-5 Denial of Service Protection

Azure's distributed denial of service (DDoS) Standard tier provides additional features and mitigation capabilities over the basic service tier. These additional features include Azure Monitor integration and the ability to review post-attack mitigation reports. This blueprint assigns an [Azure Policy](#) definition that audits if the DDoS Standard tier is enabled. Understanding the capability difference between the service tiers can help you select the best solution to address denial of service protections for your Azure environment.

- DDoS Protection Standard should be enabled

SC-7 Boundary Protection

This blueprint helps you manage and control the system boundary by assigning an [Azure Policy](#) definition that monitors for network security group hardening recommendations in Azure Security Center. Azure Security Center analyzes traffic patterns of Internet facing virtual machines and provides network security group rule recommendations to reduce the potential attack surface. Additionally, this blueprint also assigns policy definitions that monitor unprotected endpoints, applications, and storage accounts. Endpoints and applications that aren't protected by a firewall, and storage accounts with unrestricted access can allow unintended access to information contained within the information system.

- Network Security Group Rules for Internet facing virtual machines should be hardened
- Access through Internet facing endpoint should be restricted
- Web ports should be restricted on Network Security Groups associated to your VM
- Audit unrestricted network access to storage accounts

SC-7 (3) Boundary Protection | Access Points

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT virtual machine access helps you limit the number of external connections to your resources in Azure. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Just-In-Time network access control should be applied on virtual machines

SC-7 (4) Boundary Protection | External Telecommunications Services

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT virtual machine access helps you manage exceptions to your traffic flow policy by facilitating the access request and approval processes. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Just-In-Time network access control should be applied on virtual machines

SC-8 (1) Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection

This blueprint helps you protect the confidential and integrity of transmitted information by assigning [Azure Policy](#) definitions that help you monitor cryptographic mechanism implemented for communications protocols. Ensuring communications are properly encrypted can help you meet your organization's requirements or protecting information from unauthorized disclosure and modification.

- API App should only be accessible over HTTPS

- Audit Windows web servers that are not using secure communication protocols
- Deploy requirements to audit Windows web servers that are not using secure communication protocols
- Function App should only be accessible over HTTPS
- Only secure connections to your Redis Cache should be enabled
- Secure transfer to storage accounts should be enabled
- Web Application should only be accessible over HTTPS

SC-28 (1) Protection of Information at Rest | Cryptographic Protection

This blueprint helps you enforce your policy on the use of cryptograph controls to protect information at rest by assigning [Azure Policy](#) definitions that enforce specific cryptograph controls and audit use of weak cryptographic settings. Understanding where your Azure resources may have non-optimal cryptographic configurations can help you take corrective actions to ensure resources are configured in accordance with your information security policy. Specifically, the policy definitions assigned by this blueprint require encryption for data lake storage accounts; require transparent data encryption on SQL databases; and audit missing encryption on SQL databases, virtual machine disks, and automation account variables.

- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Deploy SQL DB transparent data encryption
- Disk encryption should be applied on virtual machines
- Require encryption on Data Lake Store accounts
- Transparent Data Encryption on SQL databases should be enabled

SI-2 Flaw Remediation

This blueprint helps you manage information system flaws by assigning [Azure Policy](#) definitions that monitor missing system updates, operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources. This blueprint also assigns a policy definition that ensures patching of the operating system for virtual machine scale sets.

- Require automatic OS image patching on Virtual Machine Scale Sets
- System updates on virtual machine scale sets should be installed
- System updates should be installed on your virtual machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities in security configuration on your virtual machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

SI-3 Malicious Code Protection

This blueprint helps you manage endpoint protection, including malicious code protection, by assigning [Azure Policy](#) definitions that monitor for missing endpoint protection on virtual machines in Azure Security Center and enforce the Microsoft antimalware solution on Windows virtual machines.

- Deploy default Microsoft IaaSAntimalware extension for Windows Server
- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center

SI-3 (1) Malicious Code Protection | Central Management

This blueprint helps you manage endpoint protection, including malicious code protection, by assigning [Azure Policy](#) definitions that monitor for missing endpoint protection on virtual machines in Azure Security Center. Azure Security Center provides centralized management and reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources.

- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center

SI-4 Information System Monitoring

This blueprint helps you monitor your system by auditing and enforcing logging and data security across Azure resources. Specifically, the policies assigned audit and enforce deployment of the Log Analytics agent, and enhanced security settings for SQL databases, storage accounts and network resources. These capabilities can help you detect anomalous behavior and indicators of attacks so you can take appropriate action.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment in VMSS - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch
- [Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Linux VMs
- [Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Windows VMs
- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Deploy Advanced Threat Protection on Storage Accounts
- Deploy Auditing on SQL servers
- Deploy network watcher when virtual networks are created
- Deploy Threat Detection on SQL servers

NOTE

Availability of specific Azure Policy definitions may vary in Azure Government and other national clouds.

Next steps

Now that you've reviewed the control mapping of the FedRAMP Moderate blueprint, visit the following articles to learn about the blueprint and how to deploy this sample:

[FedRAMP Moderate blueprint - Overview](#) [FedRAMP Moderate blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the FedRAMP Moderate blueprint sample

5/3/2021 • 7 minutes to read • [Edit Online](#)

To deploy the Azure Blueprints FedRAMP Moderate blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **FedRAMP Moderate** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the FedRAMP Moderate blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with FedRAMP Moderate controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the FedRAMP Moderate blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each

deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:

- Basics
 - **Subscriptions:** Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name:** The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location:** Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version:** Pick a **Published** version of your copy of the blueprint sample.

- Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *system assigned* managed identity option.

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit FedRAMP Moderate controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Log Analytics workspace ID that VMs should be configured for	This is the ID (GUID) of the Log Analytics workspace that the VMs should be configured for.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit FedRAMP Moderate controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor diagnostic logs schemas .
[Preview]: Audit FedRAMP Moderate controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be excluded from Windows VM Administrators group	A semicolon-separated list of members that should be excluded in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: Audit FedRAMP Moderate controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be included in Windows VM Administrators group	A semicolon-separated list of members that should be included in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Linux VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Log Analytics workspace for Linux VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Windows VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Log Analytics workspace for Windows VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Advanced Threat Protection on Storage Accounts	Policy assignment	Effect	Information about policy effects can be found at Understand Azure Policy Effects
Deploy Auditing on SQL servers	Policy assignment	The value in days of the retention period (0 indicates unlimited retention)	Retention days (optional, 180 days if unspecified)
Deploy Auditing on SQL servers	Policy assignment	Resource group name for storage account for SQL server auditing	Auditing writes database events to an audit log in your Azure Storage account (a storage account will be created in each region where a SQL Server is created that will be shared by all servers in that region). Important - for proper operation of Auditing do not delete or rename the resource group or the storage accounts.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Storage account prefix for network security group diagnostics	This prefix will be combined with the network security group location to form the created storage account name.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Resource group name for storage account for network security group diagnostics (must exist)	The resource group that the storage account will be created in. This resource group must already exist.

Next steps

Now that you've reviewed the steps to deploy the FedRAMP Moderate blueprint sample, visit the following articles to learn about the blueprint and control mapping:

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the FedRAMP High blueprint sample

5/3/2021 • 2 minutes to read • [Edit Online](#)

The FedRAMP High blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific FedRAMP High controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement FedRAMP High controls.

Control mapping

The control mapping section provides details on policies included within this blueprint and how these policies address various controls in FedRAMP High. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policies. For more information, see [Azure Policy](#).

Next steps

You've reviewed the overview and of the FedRAMP High blueprint sample. Next, visit the following articles to learn about the control mapping and how to deploy this sample:

[FedRAMP High blueprint - Control mapping](#) [FedRamp High blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Control mapping of the FedRAMP High blueprint sample

5/3/2021 • 22 minutes to read • [Edit Online](#)

The following article details how the Azure Blueprints FedRAMP High blueprint sample maps to the FedRAMP High controls. For more information about the controls, see [FedRAMP Security Controls Baseline](#).

The following mappings are to the **FedRAMP High** controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an [Azure Policy](#) initiative. To review the complete initiative, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements** built-in policy initiative.

IMPORTANT

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy definitions for this compliance blueprint sample may change over time. To view the change history, see the [GitHub Commit History](#).

AC-2 Account Management

This blueprint helps you review accounts that may not comply with your organization's account management requirements. This blueprint assigns [Azure Policy](#) definitions that audit external accounts with read, write, and owner permissions on a subscription and deprecated accounts. By reviewing the accounts audited by these policies, you can take appropriate action to ensure account management requirements are met.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription
- External accounts with owner permissions should be removed from your subscription
- External accounts with read permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription

AC-2 (7) Account Management | Role-Based Schemes

Azure implements [Azure role-based access control \(Azure RBAC\)](#) to help you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint also assigns [Azure Policy](#) definitions to audit use of Azure Active Directory authentication for SQL Servers and Service Fabric. Using Azure Active Directory authentication enables simplified permission management and centralized identity management of database users and other Microsoft services. Additionally, this blueprint assigns an Azure Policy definition to audit the use of custom Azure RBAC rules. Understanding where custom Azure RBAC rules are implemented can help you verify need and proper implementation, as custom Azure RBAC rules are error prone.

- An Azure Active Directory administrator should be provisioned for SQL servers
- Audit usage of custom RBAC rules

- Service Fabric clusters should only use Azure Active Directory for client authentication

AC-2 (12) Account Management | Account Monitoring / Atypical Usage

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. All JIT requests to access virtual machines are logged in the Activity Log allowing you to monitor for atypical usage. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Just-In-Time network access control should be applied on virtual machines

AC-4 Information Flow Enforcement

Cross origin resource sharing (CORS) can allow App Services resources to be requested from an outside domain. Microsoft recommends that you allow only required domains to interact with your API, function, and web applications. This blueprint assigns an [Azure Policy](#) definition to help you monitor CORS resources access restrictions in Azure Security Center. Understanding CORS implementations can help you verify that information flow controls are implemented.

- CORS should not allow every resource to access your Web Application

AC-5 Separation of Duties

Having only one Azure subscription owner doesn't allow for administrative redundancy. Conversely, having too many Azure subscription owners can increase the potential for a breach via a compromised owner account. This blueprint helps you maintain an appropriate number of Azure subscription owners by assigning [Azure Policy](#) definitions that audit the number of owners for Azure subscriptions. This blueprint also assigns Azure Policy definitions that help you control membership of the Administrators group on Windows virtual machines. Managing subscription owner and virtual machine administrator permissions can help you implement appropriate separation of duties.

- A maximum of 3 owners should be designated for your subscription
- Audit Windows VMs in which the Administrators group contains any of the specified members
- Audit Windows VMs in which the Administrators group does not contain all of the specified members
- Deploy requirements to audit Windows VMs in which the Administrators group contains any of the specified members
- Deploy requirements to audit Windows VMs in which the Administrators group does not contain all of the specified members
- There should be more than one owner assigned to your subscription

AC-6 (7) Least Privilege | Review of User Privileges

Azure implements [Azure role-based access control \(Azure RBAC\)](#) to help you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint assigns [Azure Policy](#) definitions to audit accounts that should be prioritized for review. Reviewing these account indicators can help you ensure least privilege controls are implemented.

- A maximum of 3 owners should be designated for your subscription
- Audit Windows VMs in which the Administrators group contains any of the specified members
- Audit Windows VMs in which the Administrators group does not contain all of the specified members
- Deploy requirements to audit Windows VMs in which the Administrators group contains any of the specified

members

- Deploy requirements to audit Windows VMs in which the Administrators group does not contain all of the specified members
- There should be more than one owner assigned to your subscription

AC-17 (1) Remote Access | Automated Monitoring / Control

This blueprint helps you monitor and control remote access by assigning [Azure Policy](#) definitions to monitors that remote debugging for Azure App Service application is turned off and policy definitions that audit Linux virtual machines that allow remote connections from accounts without passwords. This blueprint also assigns an Azure Policy definition that helps you monitor unrestricted access to storage accounts. Monitoring these indicators can help you ensure remote access methods comply with your security policy.

- [Preview]: Audit Linux VMs that allow remote connections from accounts without passwords
- [Preview]: Deploy requirements to audit Linux VMs that allow remote connections from accounts without passwords
- Audit unrestricted network access to storage accounts
- Remote debugging should be turned off for API App
- Remote debugging should be turned off for Function App
- Remote debugging should be turned off for Web Application

AU-3 (2) Content of Audit Records | Centralized Management of Planned Audit Record Content

Log data collected by Azure Monitor is stored in a Log Analytics workspace enabling centralized configuration and management. This blueprint helps you ensure events are logged by assigning [Azure Policy](#) definitions that audit and enforce deployment of the Log Analytics agent on Azure virtual machines.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment in VMSS - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch
- [Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Linux VMs
- [Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Windows VMs

AU-5 Response to Audit Processing Failures

This blueprint assigns [Azure Policy](#) definitions that monitor audit and event logging configurations. Monitoring these configurations can provide an indicator of an audit system failure or misconfiguration and help you take corrective action.

- Audit diagnostic setting
- Auditing should be enabled on advanced data security settings on SQL Server
- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers

AU-6 (4) Audit Review, Analysis, and Reporting | Central Review and Analysis

Log data collected by Azure Monitor is stored in a Log Analytics workspace enabling centralized reporting and analysis. This blueprint helps you ensure events are logged by assigning [Azure Policy](#) definitions that audit and

enforce deployment of the Log Analytics agent on Azure virtual machines.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment in VMSS - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch
- [Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Linux VMs
- [Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Windows VMs

AU-6 (5) Audit Review, Analysis, and Reporting | Integration / Scanning and Monitoring Capabilities

This blueprint provides policy definitions that audit records with analysis of vulnerability assessment on virtual machines, virtual machine scale sets, SQL Database servers, and SQL Managed Instance servers. These policy definitions also audit configuration of diagnostic logs to provide insight into operations that are performed within Azure resources. These insights provide real-time information about the security state of your deployed resources and can help you prioritize remediation actions. For detailed vulnerability scanning and monitoring, we recommend you use Azure Sentinel and Azure Security Center as well.

- [Preview]: Vulnerability Assessment should be enabled on Virtual Machines
- [Preview]: Enable Azure Monitor for VMs
- [Preview]: Enable Azure Monitor for VM Scale Sets (VMSS)
- Vulnerability assessment should be enabled on your SQL servers
- Audit diagnostic setting
- Vulnerability assessment should be enabled on your SQL managed instances
- Vulnerability assessment should be enabled on your SQL servers
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated

AU-12 Audit Generation

This blueprint provides policy definitions that audit and enforce deployment of the Log Analytics agent on Azure virtual machines and configuration of audit settings for other Azure resource types. These policy definitions also audit configuration of diagnostic logs to provide insight into operations that are performed within Azure resources. Additionally, auditing and Advanced Data Security are configured on SQL servers.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment in VMSS - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch
- [Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Linux VMs
- [Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Windows VMs
- Audit diagnostic setting
- Auditing should be enabled on advanced data security settings on SQL Server
- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers

- Deploy Advanced Data Security on SQL servers
- Deploy Auditing on SQL servers
- Deploy Diagnostic Settings for Network Security Groups

AU-12 (01) Audit Generation | System-Wide / Time-Correlated Audit Trail

This blueprint helps you ensure system events are logged by assigning [Azure Policy](#) definitions that audit log settings on Azure resources. This built-in policy requires you to specify an array of resource types to check whether diagnostic settings are enabled or not.

- Audit diagnostic setting

CM-7 (2) Least Functionality | Prevent Program Execution

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application filtering solution that can block or prevent specific software from running on your virtual machines. Application control can run in an enforcement mode that prohibits non-approved application from running. This blueprint assigns an Azure Policy definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive Application Controls should be enabled on virtual machines

CM-7 (5) Least Functionality | Authorized Software / Whitelisting

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application filtering solution that can block or prevent specific software from running on your virtual machines. Application control helps you create approved application lists for your virtual machines. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive Application Controls should be enabled on virtual machines

CM-11 User-Installed Software

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application filtering solution that can block or prevent specific software from running on your virtual machines. Application control can help you enforce and monitor compliance with software restriction policies. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive Application Controls should be enabled on virtual machines

CP-7 Alternate Processing Site

Azure Site Recovery replicates workloads running on virtual machines from a primary location to a secondary location. If an outage occurs at the primary site, the workload fails over the secondary location. This blueprint assigns an [Azure Policy](#) definition that audits virtual machines without disaster recovery configured. Monitoring this indicator can help you ensure necessary contingency controls are in place.

- Audit virtual machines without disaster recovery configured

CP-9 (05) Information System Backup | Transfer to Alternate Storage Site

This blueprint assigns Azure Policy definitions that audit the organization's system backup information to the alternate storage site electronically. For physical shipment of storage metadata, consider using Azure Data Box.

- Geo-redundant storage should be enabled for Storage Accounts
- Geo-redundant backup should be enabled for Azure Database for PostgreSQL
- Geo-redundant backup should be enabled for Azure Database for MySQL
- Geo-redundant backup should be enabled for Azure Database for MariaDB
- Long-term geo-redundant backup should be enabled for Azure SQL Databases

IA-2 (1) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts

This blueprint helps you restrict and control privileged access by assigning [Azure Policy](#) definitions to audit accounts with owner and/or write permissions that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled on accounts with write permissions on your subscription

IA-2 (2) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

This blueprint helps you restrict and control access by assigning an [Azure Policy](#) definition to audit accounts with read permissions that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with read permissions on your subscription

IA-5 Authenticator Management

This blueprint assigns [Azure Policy](#) definitions that audit Linux virtual machines that allow remote connections from accounts without passwords and/or have incorrect permissions set on the passwd file. This blueprint also assigns policy definitions that audit the configuration of the password encryption type for Windows virtual machines. Monitoring these indicators helps you ensure that system authenticators comply with your organization's identification and authentication policy.

- [Preview]: Audit Linux VMs that do not have the passwd file permissions set to 0644
- [Preview]: Audit Linux VMs that have accounts without passwords
- [Preview]: Audit Windows VMs that do not store passwords using reversible encryption
- [Preview]: Deploy requirements to audit Linux VMs that do not have the passwd file permissions set to 0644
- [Preview]: Deploy requirements to audit Linux VMs that have accounts without passwords
- [Preview]: Deploy requirements to audit Windows VMs that do not store passwords using reversible encryption

IA-5 (1) Authenticator Management | Password-Based Authentication

This blueprint helps you enforce strong passwords by assigning [Azure Policy](#) definitions that audit Windows virtual machines that don't enforce minimum strength and other password requirements. Awareness of virtual machines in violation of the password strength policy helps you take corrective actions to ensure passwords for

all virtual machine user accounts comply with your organization's password policy.

- [Preview]: Audit Windows VMs that allow re-use of the previous 24 passwords
- [Preview]: Audit Windows VMs that do not have a maximum password age of 70 days
- [Preview]: Audit Windows VMs that do not have a minimum password age of 1 day
- [Preview]: Audit Windows VMs that do not have the password complexity setting enabled
- [Preview]: Audit Windows VMs that do not restrict the minimum password length to 14 characters
- [Preview]: Audit Windows VMs that do not store passwords using reversible encryption
- [Preview]: Deploy requirements to audit Windows VMs that allow re-use of the previous 24 passwords
- [Preview]: Deploy requirements to audit Windows VMs that do not have a maximum password age of 70 days
- [Preview]: Deploy requirements to audit Windows VMs that do not have a minimum password age of 1 day
- [Preview]: Deploy requirements to audit Windows VMs that do not have the password complexity setting enabled
- [Preview]: Deploy requirements to audit Windows VMs that do not restrict the minimum password length to 14 characters
- [Preview]: Deploy requirements to audit Windows VMs that do not store passwords using reversible encryption

RA-5 Vulnerability Scanning

This blueprint helps you manage information system vulnerabilities by assigning [Azure Policy](#) definitions that monitor operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources. This blueprint also assigns policy definitions that audit and enforce Advanced Data Security on SQL servers. Advanced data security included vulnerability assessment and advanced threat protection capabilities to help you understand vulnerabilities in your deployed resources.

- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities in security configuration on your virtual machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

SC-5 Denial of Service Protection

Azure's distributed denial of service (DDoS) Standard tier provides additional features and mitigation capabilities over the basic service tier. These additional features include Azure Monitor integration and the ability to review post-attack mitigation reports. This blueprint assigns an [Azure Policy](#) definition that audits if the DDoS Standard tier is enabled. Understanding the capability difference between the service tiers can help you select the best solution to address denial of service protections for your Azure environment.

- DDoS Protection Standard should be enabled

SC-7 Boundary Protection

This blueprint helps you manage and control the system boundary by assigning an [Azure Policy](#) definition that monitors for network security group hardening recommendations in Azure Security Center. Azure Security Center analyzes traffic patterns of Internet facing virtual machines and provides network security group rule recommendations to reduce the potential attack surface. Additionally, this blueprint also assigns policy

definitions that monitor unprotected endpoints, applications, and storage accounts. Endpoints and applications that aren't protected by a firewall, and storage accounts with unrestricted access can allow unintended access to information contained within the information system.

- Network Security Group Rules for Internet facing virtual machines should be hardened
- Access through Internet facing endpoint should be restricted
- Web ports should be restricted on Network Security Groups associated to your VM
- Audit unrestricted network access to storage accounts

SC-7 (3) Boundary Protection | Access Points

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT virtual machine access helps you limit the number of external connections to your resources in Azure. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Just-In-Time network access control should be applied on virtual machines

SC-7 (4) Boundary Protection | External Telecommunications Services

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT virtual machine access helps you manage exceptions to your traffic flow policy by facilitating the access request and approval processes. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but haven't yet been configured.

- Just-In-Time network access control should be applied on virtual machines

SC-8 (1) Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection

This blueprint helps you protect the confidential and integrity of transmitted information by assigning [Azure Policy](#) definitions that help you monitor cryptographic mechanism implemented for communications protocols. Ensuring communications are properly encrypted can help you meet your organization's requirements or protecting information from unauthorized disclosure and modification.

- API App should only be accessible over HTTPS
- Audit Windows web servers that are not using secure communication protocols
- Deploy requirements to audit Windows web servers that are not using secure communication protocols
- Function App should only be accessible over HTTPS
- Only secure connections to your Redis Cache should be enabled
- Secure transfer to storage accounts should be enabled
- Web Application should only be accessible over HTTPS

SC-28 (1) Protection of Information at Rest | Cryptographic Protection

This blueprint helps you enforce your policy on the use of cryptograph controls to protect information at rest by assigning [Azure Policy](#) definitions that enforce specific cryptograph controls and audit use of weak cryptographic settings. Understanding where your Azure resources may have non-optimal cryptographic configurations can help you take corrective actions to ensure resources are configured in accordance with your information security policy. Specifically, the policy definitions assigned by this blueprint require encryption for data lake storage accounts; require transparent data encryption on SQL databases; and audit missing encryption

on SQL databases, virtual machine disks, and automation account variables.

- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Deploy SQL DB transparent data encryption
- Disk encryption should be applied on virtual machines
- Require encryption on Data Lake Store accounts
- Transparent Data Encryption on SQL databases should be enabled

SI-2 Flaw Remediation

This blueprint helps you manage information system flaws by assigning [Azure Policy](#) definitions that monitor missing system updates, operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources. This blueprint also assigns a policy definition that ensures patching of the operating system for virtual machine scale sets.

- Require automatic OS image patching on Virtual Machine Scale Sets
- System updates on virtual machine scale sets should be installed
- System updates should be installed on your virtual machines
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities in security configuration on your virtual machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

SI-3 Malicious Code Protection

This blueprint helps you manage endpoint protection, including malicious code protection, by assigning [Azure Policy](#) definitions that monitor for missing endpoint protection on virtual machines in Azure Security Center and enforce the Microsoft antimalware solution on Windows virtual machines.

- Deploy default Microsoft IaaS Antimalware extension for Windows Server
- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center

SI-3 (1) Malicious Code Protection | Central Management

This blueprint helps you manage endpoint protection, including malicious code protection, by assigning [Azure Policy](#) definitions that monitor for missing endpoint protection on virtual machines in Azure Security Center. Azure Security Center provides centralized management and reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources.

- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center

SI-4 Information System Monitoring

This blueprint helps you monitor your system by auditing and enforcing logging and data security across Azure resources. Specifically, the policies assigned audit and enforce deployment of the Log Analytics agent, and enhanced security settings for SQL databases, storage accounts and network resources. These capabilities can help you detect anomalous behavior and indicators of attacks so you can take appropriate action.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment in VMSS - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch
- [Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Linux VMs
- [Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)
- [Preview]: Deploy Log Analytics Agent for Windows VMs
- Advanced data security should be enabled on your managed instances
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Deploy Advanced Threat Protection on Storage Accounts
- Deploy Auditing on SQL servers
- Deploy network watcher when virtual networks are created
- Deploy Threat Detection on SQL servers
- Allowed locations
- Allowed locations for resource groups

SI-4 (18) Information System Monitoring | Analyze Traffic / Covert Exfiltration

Advanced Threat Protection for Azure Storage detects unusual and potentially harmful attempts to access or exploit storage accounts. Protection alerts include anomalous access patterns, anomalous extracts/uploads, and suspicious storage activity. These indicators can help you detect covert exfiltration of information.

- Deploy Advanced Threat Protection on Storage Accounts

NOTE

Availability of specific Azure Policy definitions may vary in Azure Government and other national clouds.

Next steps

Now that you've reviewed the control mapping of the FedRAMP High blueprint, visit the following articles to learn about the blueprint and how to deploy this sample:

[FedRAMP High blueprint - Overview](#) [FedRAMP High blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the FedRAMP High blueprint sample

5/3/2021 • 11 minutes to read • [Edit Online](#)

To deploy the Azure Blueprints FedRAMP High blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **FedRAMP High** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the FedRAMP High blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with FedRAMP High controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the FedRAMP High blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each

deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:

- Basics
 - **Subscriptions:** Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name:** The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location:** Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version:** Pick a **Published** version of your copy of the blueprint sample.

- Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *system assigned* managed identity option.

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Log Analytics workspace ID that VMs should be configured for	This is the ID (GUID) of the Log Analytics workspace that the VMs should be configured for.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor diagnostic logs schemas .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be excluded from Windows VM Administrators group	A semicolon-separated list of members that should be excluded in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be included in Windows VM Administrators group	A semicolon-separated list of members that should be included in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Linux VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Log Analytics workspace for Linux VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Windows VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Log Analytics workspace for Windows VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Advanced Threat Protection on Storage Accounts	Policy assignment	Effect	Information about policy effects can be found at Understand Azure Policy Effects .
Deploy Auditing on SQL servers	Policy assignment	The value in days of the retention period (0 indicates unlimited retention)	Retention days (optional, 180 days if unspecified)
Deploy Auditing on SQL servers	Policy assignment	Resource group name for storage account for SQL server auditing	Auditing writes database events to an audit log in your Azure Storage account (a storage account will be created in each region where a SQL Server is created that will be shared by all servers in that region). Important - for proper operation of Auditing do not delete or rename the resource group or the storage accounts.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Storage account prefix for network security group diagnostics	This prefix will be combined with the network security group location to form the created storage account name.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Resource group name for storage account for network security group diagnostics (must exist)	The resource group that the storage account will be created in. This resource group must already exist.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Allowed locations for resources and resource groups	List of Azure locations that your organization can specify when deploying resources. This provided value is also used by the 'Allowed locations' policy within the policy initiative.
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerability assessment should be enabled on your SQL managed instances	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerability assessment should be enabled on your SQL servers	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Vulnerability assessment should be enabled on Virtual Machines	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Geo-redundant storage should be enabled for Storage Accounts	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Geo-redundant backup should be enabled for Azure Database for MariaDB	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Geo-redundant backup should be enabled for Azure Database for MySQL	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Geo-redundant backup should be enabled for Azure Database for PostgreSQL	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Network Security Group rules for internet facing virtual machines should be hardened	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Web Application should only be accessible over HTTPS	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Function App should only be accessible over HTTPS	Information about policy effects can be found at Understand Azure Policy Effects .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	External accounts with write permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	External accounts with read permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	External accounts with owner permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Deprecated accounts with owner permissions should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Deprecated accounts should be removed from your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	CORS shouldn't allow every resource to access your Web Application	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	System updates on virtual machine scale sets should be installed	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	MFA should be enabled on accounts with read permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	MFA should be enabled on accounts with owner permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	MFA should be enabled on accounts with write permissions on your subscription	Information about policy effects can be found at Understand Azure Policy Effects .
[Preview]: Audit FedRAMP High controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Long-term geo-redundant backup should be enabled for Azure SQL Databases	Information about policy effects can be found at Understand Azure Policy Effects .

Next steps

Now that you've reviewed the steps to deploy the FedRAMP High blueprint sample, visit the following articles to learn about the blueprint and control mapping:

[FedRAMP High blueprint - Overview](#) [FedRAMP High blueprint - Control mapping](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

HIPAA HITRUST 9.2 blueprint sample

5/3/2021 • 16 minutes to read • [Edit Online](#)

The HIPAA HITRUST 9.2 blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific HIPAA HITRUST 9.2 controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement HIPAA HITRUST 9.2 controls.

Control mapping

The [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **compliance domains** and **controls** in HIPAA HITRUST 9.2. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints HIPAA HITRUST 9.2 blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **HIPAA HITRUST** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the HIPAA HITRUST 9.2 blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with HIPAA HITRUST 9.2 controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint

sample and then select it.

3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the HIPAA HITRUST 9.2 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - Managed Identity

Leave the default *system assigned* managed identity option.
 - Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	PARAMETER NAME	DESCRIPTION
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Access through Internet facing endpoint should be restricted	Enable or disable overly permissive inbound NSG rules monitoring
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Accounts: Guest account status	Specifies whether the local Guest account is disabled.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Adaptive Application Controls should be enabled on virtual machines	Enable or disable the monitoring of application whitelisting in Azure Security Center
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Allow simultaneous connections to the Internet or a Windows Domain	Specify whether to prevent computers from connecting to both a domain based network and a non-domain based network at the same time. A value of 0 allows simultaneous connections, and a value of 1 blocks them.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	API App should only be accessible over HTTPS V2	Enable or disable the monitoring of the use of HTTPS in API App V2
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Application names (supports wildcards)	A semicolon-separated list of the names of the applications that should be installed. e.g. 'Microsoft SQL Server 2014 (64-bit); Microsoft Visual Studio Code' or 'Microsoft SQL Server 2014*' (to match any application starting with 'Microsoft SQL Server 2014')
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Audit Process Termination	Specifies whether audit events are generated when a process has exited. Recommended for monitoring termination of critical processes.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Audit unrestricted network access to storage accounts	Enable or disable the monitoring of network access to storage account
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Audit: Shut down system immediately if unable to log security audits	Audits if the system will shut down when unable to log Security events.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Certificate thumbprints	A semicolon-separated list of certificate thumbprints that should exist under the Trusted Root certificate store (Cert:\LocalMachine\Root). e.g. THUMBPRINT1;THUMBPRINT2;THUMBPRINT3
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Diagnostic logs in Batch accounts should be enabled	Enable or disable the monitoring of diagnostic logs in Batch accounts

ARTIFACT NAME	PARAMETER NAME	DESCRIPTION
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Diagnostic logs in Event Hub should be enabled	Enable or disable the monitoring of diagnostic logs in Event Hub accounts
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Diagnostic logs in Search services should be enabled	Enable or disable the monitoring of diagnostic logs in Azure Search service
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Diagnostic logs in Virtual Machine Scale Sets should be enabled	Enable or disable the monitoring of diagnostic logs in Service Fabric
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Disk encryption should be applied on virtual machines	Enable or disable the monitoring for VM disk encryption
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Enable insecure guest logons	Specifies whether the SMB client will allow insecure guest logons to an SMB server.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Just-In-Time network access control should be applied on virtual machines	Enable or disable the monitoring of network just In time access
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Management ports should be closed on your virtual machines	Enable or disable the monitoring of open management ports on Virtual Machines
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	MFA should be enabled accounts with write permissions on your subscription	Enable or disable the monitoring of MFA for accounts with write permissions in subscription
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	MFA should be enabled on accounts with owner permissions on your subscription	Enable or disable the monitoring of MFA for accounts with owner permissions in subscription
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Network access: Remotely accessible registry paths	Specifies which registry paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the <code>winreg</code> registry key.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Network access: Remotely accessible registry paths and sub-paths	Specifies which registry paths and sub-paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the <code>winreg</code> registry key.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Network access: Shares that can be accessed anonymously	Specifies which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server.

ARTIFACT NAME	PARAMETER NAME	DESCRIPTION
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Recovery console: Allow floppy copy and access to all drives and all folders	Specifies whether to make the Recovery Console SET command available, which allows setting of recovery console environment variables.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Remote debugging should be turned off for API App	Enable or disable the monitoring of remote debugging for API App
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Remote debugging should be turned off for Web Application	Enable or disable the monitoring of remote debugging for Web App
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Required retention (in days) for logs in Batch accounts	The required diagnostic logs retention period in days
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Required retention (in days) of logs in Azure Search service	The required diagnostic logs retention period in days
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Required retention (in days) of logs in Event Hub accounts	The required diagnostic logs retention period in days
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Resource Group Name for Storage Account (must exist) to deploy diagnostic settings for Network Security Groups	The resource group that the storage account will be created in. This resource group must already exist.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Role-Based Access Control (RBAC) should be used on Kubernetes Services	Enable or disable the monitoring of Kubernetes Services without RBAC enabled
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	SQL managed instance TDE protector should be encrypted with your own key	Enable or disable the monitoring of Transparent Data Encryption (TDE) with your own key support. TDE with your own key support provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	SQL server TDE protector should be encrypted with your own key	Enable or disable the monitoring of Transparent Data Encryption (TDE) with your own key support. TDE with your own key support provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties.

ARTIFACT NAME	PARAMETER NAME	DESCRIPTION
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Storage Account Prefix for Regional Storage Account to deploy diagnostic settings for Network Security Groups	This prefix will be combined with the network security group location to form the created storage account name.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	System updates on virtual machine scale sets should be installed	Enable or disable virtual machine scale sets reporting of system updates
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	System updates on virtual machine scale sets should be installed	Enable or disable virtual machine scale sets reporting of system updates
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Turn off multicast name resolution	Specifies whether LLMNR, a secondary name resolution protocol that transmits using multicast over a local subnet link on a single subnet, is enabled.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Virtual machines should be migrated to new Azure Resource Manager resources	Enable or disable the monitoring of classic compute VMs
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Vulnerabilities in security configuration on your virtual machine scale sets should be remediated	Enable or disable virtual machine scale sets OS vulnerabilities monitoring
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Vulnerabilities should be remediated by a Vulnerability Assessment solution	Enable or disable the detection of VM vulnerabilities by a vulnerability assessment solution
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Vulnerability assessment should be enabled on your SQL managed instances	Audit SQL managed instances which do not have recurring vulnerability assessment scans enabled. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Domain): Apply local firewall rules	Specifies whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy for the Domain profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Domain): Behavior for outbound connections	Specifies the behavior for outbound connections for the Domain profile that do not match an outbound firewall rule. The default value of 0 means to allow connections, and a value of 1 means to block connections.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Domain): Behavior for outbound connections	Specifies the behavior for outbound connections for the Domain profile that do not match an outbound firewall rule. The default value of 0 means to allow connections, and a value of 1 means to block connections.

ARTIFACT NAME	PARAMETER NAME	DESCRIPTION
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Domain): Display notifications	Specifies whether Windows Firewall with Advanced Security displays notifications to the user when a program is blocked from receiving inbound connections, for the Domain profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Domain): Use profile settings	Specifies whether Windows Firewall with Advanced Security uses the settings for the Domain profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Private): Apply local connection security rules	Specifies whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy for the Private profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Private): Apply local firewall rules	Specifies whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy for the Private profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Private): Behavior for outbound connections	Specifies the behavior for outbound connections for the Private profile that do not match an outbound firewall rule. The default value of 0 means to allow connections, and a value of 1 means to block connections.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Private): Display notifications	Specifies whether Windows Firewall with Advanced Security displays notifications to the user when a program is blocked from receiving inbound connections, for the Private profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Private): Use profile settings	Specifies whether Windows Firewall with Advanced Security uses the settings for the Private profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Public): Apply local connection security rules	Specifies whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy for the Public profile.

ARTIFACT NAME	PARAMETER NAME	DESCRIPTION
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Public): Apply local firewall rules	Specifies whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy for the Public profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Public): Behavior for outbound connections	Specifies the behavior for outbound connections for the Public profile that do not match an outbound firewall rule. The default value of 0 means to allow connections, and a value of 1 means to block connections.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Public): Display notifications	Specifies whether Windows Firewall with Advanced Security displays notifications to the user when a program is blocked from receiving inbound connections, for the Public profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall (Public): Use profile settings	Specifies whether Windows Firewall with Advanced Security uses the settings for the Public profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall: Domain: Allow unicast response	Specifies whether Windows Firewall with Advanced Security permits the local computer to receive unicast responses to its outgoing multicast or broadcast messages; for the Domain profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall: Private: Allow unicast response	Specifies whether Windows Firewall with Advanced Security permits the local computer to receive unicast responses to its outgoing multicast or broadcast messages; for the Private profile.
Audit HITRUST/HIPAA controls and deploy specific VM Extensions to support audit requirements	Windows Firewall: Public: Allow unicast response	Specifies whether Windows Firewall with Advanced Security permits the local computer to receive unicast responses to its outgoing multicast or broadcast messages; for the Public profile.

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).

- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

IRS 1075 September 2016 blueprint sample

5/4/2021 • 8 minutes to read • [Edit Online](#)

The IRS 1075 September 2016 blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific [IRS 1075 September 2016](#) controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement controls for IRS 1075 September 2016.

Control mapping

The [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **controls** in the IRS 1075 September 2016 framework. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints IRS 1075 September 2016 blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **IRS 1075 September 2016** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the IRS 1075 September 2016 blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that are included in the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with IRS 1075 September 2016 controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.

2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the IRS 1075 September 2016 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:

- Basics

- **Subscriptions:** Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
- **Assignment name:** The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
- **Location:** Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
- **Blueprint definition version:** Pick a **Published** version of your copy of the blueprint sample.

- Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *system assigned* managed identity option.

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Audit IRS 1075 (Rev.11-2016) controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Log Analytics workspace ID that VMs should be configured for	This is the ID (GUID) of the Log Analytics workspace that the VMs should be configured for.
Audit IRS 1075 (Rev.11-2016) controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor diagnostic logs schemas .
Audit IRS 1075 (Rev.11-2016) controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be excluded from Windows VM Administrators group	A semicolon-separated list of members that should be excluded in the Administrators local group. Ex: Administrator; myUser1; myUser2
Audit IRS 1075 (Rev.11-2016) controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be included in Windows VM Administrators group	A semicolon-separated list of members that should be included in the Administrators local group. Ex: Administrator; myUser1; myUser2
Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Linux VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Log Analytics Agent for Linux VMs	Policy assignment	Log Analytics workspace for Linux VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Windows VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Log Analytics Agent for Windows VMs	Policy assignment	Log Analytics workspace for Windows VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Advanced Threat Protection on Storage Accounts	Policy assignment	Effect	Information about policy effects can be found at Understand Azure Policy Effects
Deploy Auditing on SQL servers	Policy assignment	The value in days of the retention period (0 indicates unlimited retention)	Retention days (optional, 180 days if unspecified)
Deploy Auditing on SQL servers	Policy assignment	Resource group name for storage account for SQL server auditing	Auditing writes database events to an audit log in your Azure Storage account (a storage account will be created in each region where a SQL Server is created that will be shared by all servers in that region). Important - for proper operation of Auditing do not delete or rename the resource group or the storage accounts.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Storage account prefix for network security group diagnostics	This prefix will be combined with the network security group location to form the created storage account name.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Deploy diagnostic settings for Network Security Groups	Policy assignment	Resource group name for storage account for network security group diagnostics (must exist)	The resource group that the storage account will be created in. This resource group must already exist.

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

ISO 27001 blueprint sample

5/3/2021 • 6 minutes to read • [Edit Online](#)

The ISO 27001 blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific ISO 27001 controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement ISO 27001 controls.

Control mapping

The [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **compliance domains** and **controls** in ISO 27001. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints ISO 27001 blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **ISO 27001** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the ISO 27001 blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with ISO 27001 controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint

sample and then select it.

3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the ISO 27001 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - Managed Identity

Leave the default *system assigned* managed identity option.
 - Blueprint parameters

The parameters defined in this section are used by many of the artifacts in the blueprint definition to provide consistency.
 - **Allowed location for resources and resource groups**: Value that indicates the allowed locations for resource groups and resources.
 - Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are **priced by product**. Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Linux VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Log Analytics workspace for Linux VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Windows VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Log Analytics workspace for Windows VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
Allowed storage account SKUs	Policy assignment	List of allowed storage SKUs	The list of SKUs that can be specified for storage accounts.
Allowed virtual machine SKUs	Policy assignment	List of allowed virtual machine SKUs	The list of SKUs that can be specified for virtual machines.
Blueprint initiative for ISO 27001	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor diagnostic logs schemas .

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the ISO 27001 Shared Services blueprint sample

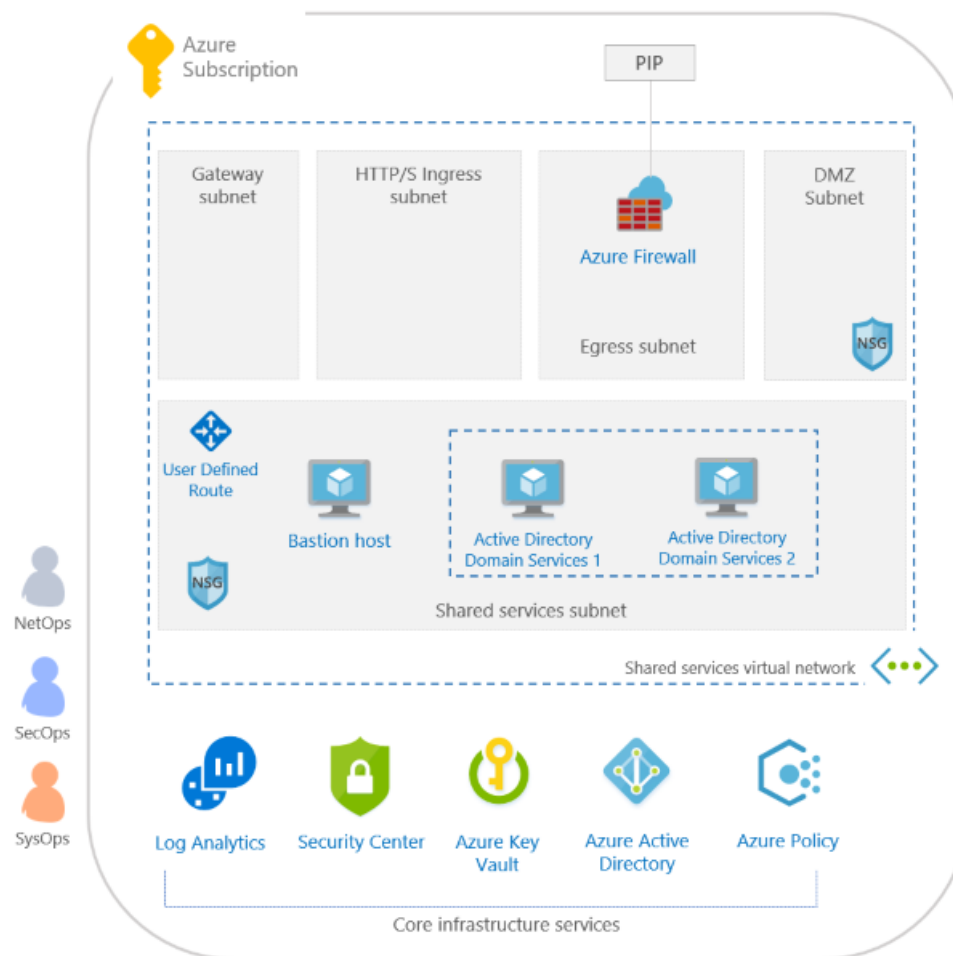
5/3/2021 • 2 minutes to read • [Edit Online](#)

The ISO 27001 Shared Services blueprint sample provides a set of compliant infrastructure patterns and policy guardrails that help toward ISO 27001 attestation. This blueprint helps customers deploy cloud-based architectures that offer solutions to scenarios that have accreditation or compliance requirements.

The [ISO 27001 App Service Environment/SQL Database workload](#) blueprint sample extends this sample.

Architecture

The ISO 27001 Shared Services blueprint sample deploys a foundation infrastructure in Azure that can be used by organizations to host multiple workloads based on the Virtual Datacenter (VDC) approach. VDC is a proven set of reference architectures, automation tooling, and engagement model used by Microsoft with its largest enterprise customers. The Shared Services blueprint sample is based on a fully native Azure VDC environment shown below.



This environment is composed of several Azure services used to provide a secure, fully monitored, enterprise-ready shared services infrastructure based on ISO 27001 standards. This environment is composed of:

- **Azure roles** used for segregation of duties from a control plane perspective. Three roles are defined before deployment of any infrastructure:
 - **NetOps** role has the rights to manage the network environment, including firewall settings, NSG

- settings, routing, and other networking functionality
- SecOps role has the necessary rights to deploy and manage [Azure Security Center](#), define [Azure Policy](#) definitions, and other security-related rights
- SysOps role has the necessary rights to define [Azure Policy](#) definitions within the subscription, manage [Log Analytics](#) for the entire environment, among other operational rights
- [Log Analytics](#) is deployed as the first Azure service to ensure all actions and services log to a central location from the moment you start your secure deployment
- A virtual network supporting subnets for connectivity back to an on-premises datacenter, an ingress and egress stack for Internet connectivity, and a shared service subnet using NSGs and ASGs for full micro-segmentation containing:
 - A jumpbox or bastion host used for management purposes, which can only be accessed over an [Azure Firewall](#) deployed in the ingress stack subnet
 - Two virtual machines running Azure Active Directory Domain Services (Azure AD DS) and DNS only accessible through the jumpbox, and can be configured only to replicate AD over a VPN or [ExpressRoute](#) connection (not deployed by the blueprint)
 - Use of [Azure Net Watcher](#) and standard DDoS protection
- An [Azure Key Vault](#) instance used to host secrets used for the VMs deployed in the shared services environment

All these elements abide to the proven practices published in the [Azure Architecture Center - Reference Architectures](#).

NOTE

The ISO 27001 Shared Services infrastructure lays out a foundational architecture for workloads. You still need to deploy workloads behind this foundational architecture.

For more information, see the [Virtual Datacenter documentation](#).

Next steps

You've reviewed the overview and architecture of the ISO 27001 Shared Services blueprint sample. Next, visit the following articles to learn about the control mapping and how to deploy this sample:

[ISO 27001 Shared Services blueprint - Control mapping](#) [ISO 27001 Shared Services blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Control mapping of the ISO 27001 Shared Services blueprint sample

5/3/2021 • 11 minutes to read • [Edit Online](#)

The following article details how the Azure Blueprints ISO 27001 Shared Services blueprint sample maps to the ISO 27001 controls. For more information about the controls, see [ISO 27001](#).

The following mappings are to the **ISO 27001:2013** controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an [Azure Policy](#) initiative. To review the complete initiative, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **[Preview] Audit ISO 27001:2013 controls and deploy specific VM Extensions to support audit requirements** built-in policy initiative.

IMPORTANT

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy definitions for this compliance blueprint sample may change over time. To view the change history, see the [GitHub Commit History](#).

A.6.1.2 Segregation of duties

Having only one Azure subscription owner doesn't allow for administrative redundancy. Conversely, having too many Azure subscription owners can increase the potential for a breach via a compromised owner account. This blueprint helps you maintain an appropriate number of Azure subscription owners by assigning two [Azure Policy](#) definitions that audit the number of owners for Azure subscriptions. Managing subscription owner permissions can help you implement appropriate separation of duties.

- A maximum of 3 owners should be designated for your subscription
- There should be more than one owner assigned to your subscription

A.8.2.1 Classification of information

Azure's [SQL Vulnerability Assessment service](#) can help you discover sensitive data stored in your databases and includes recommendations to classify that data. This blueprint assigns an [Azure Policy](#) definition to audit that vulnerabilities identified during SQL Vulnerability Assessment scan are remediated.

- Vulnerabilities on your SQL databases should be remediated

A.9.1.2 Access to networks and network services

[Azure role-based access control \(Azure RBAC\)](#) helps to manage who has access to Azure resources. This blueprint helps you control access to Azure resources by assigning seven [Azure Policy](#) definitions. These policies audit use of resource types and configurations that may allow more permissive access to resources. Understanding resources that are in violation of these policies can help you take corrective actions to ensure access Azure resources is restricted to authorized users.

- Show audit results from Linux VMs that have accounts without passwords
- Show audit results from Linux VMs that allow remote connections from accounts without passwords
- Storage accounts should be migrated to new Azure Resource Manager resources
- Virtual machines should be migrated to new Azure Resource Manager resources
- Audit VMs that do not use managed disks

A.9.2.3 Management of privileged access rights

This blueprint helps you restrict and control privileged access rights by assigning four [Azure Policy](#) definitions to audit external accounts with owner and/or write permissions and accounts with owner and/or write permissions that don't have multi-factor authentication enabled. Azure role-based access control (Azure RBAC) helps to manage who has access to Azure resources. This blueprint also assigns three Azure Policy definitions to audit use of Azure Active Directory authentication for SQL Servers and Service Fabric. Using Azure Active Directory authentication enables simplified permission management and centralized identity management of database users and other Microsoft services. This blueprint also assigns an Azure Policy definition to audit the use of custom Azure RBAC rules. Understanding where custom Azure RBAC rules are implemented can help you verify need and proper implementation, as custom Azure RBAC rules are error prone.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription
- External accounts with owner permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription
- An Azure Active Directory administrator should be provisioned for SQL servers
- Service Fabric clusters should only use Azure Active Directory for client authentication
- Audit usage of custom RBAC rules

A.9.2.4 Management of secret authentication information of users

This blueprint assigns three [Azure Policy](#) definitions to audit accounts that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised. This blueprint also assigns two Azure Policy definitions that audit Linux VM password file permissions to alert if they're set incorrectly. This setup enables you to take corrective action to ensure authenticators aren't compromised.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled on accounts with read permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription
- Show audit results from Linux VMs that do not have the passwd file permissions set to 0644

A.9.2.5 Review of user access rights

[Azure role-based access control \(Azure RBAC\)](#) helps you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint assigns four [Azure Policy](#) definitions to audit accounts that should be prioritized for review, including deprecated accounts and external accounts with elevated permissions.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription
- External accounts with owner permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription

A.9.2.6 Removal or adjustment of access rights

[Azure role-based access control \(Azure RBAC\)](#) helps you manage who has access to resources in Azure. Using [Azure Active Directory](#) and Azure RBAC, you can update user roles to reflect organizational changes. When needed, accounts can be blocked from signing in (or removed), which immediately removes access rights to Azure resources. This blueprint assigns two [Azure Policy](#) definitions to audit deprecated account that should be considered for removal.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription

A.9.4.2 Secure log-on procedures

This blueprint assigns three Azure Policy definitions to audit accounts that don't have multi-factor authentication enabled. Azure AD Multi-Factor Authentication provides additional security by requiring a second form of authentication and delivers strong authentication. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled on accounts with read permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription

A.9.4.3 Password management system

This blueprint helps you enforce strong passwords by assigning 10 [Azure Policy](#) definitions that audit Windows VMs that don't enforce minimum strength and other password requirements. Awareness of VMs in violation of the password strength policy helps you take corrective actions to ensure passwords for all VM user accounts are compliant with policy.

- Show audit results from Windows VMs that do not have the password complexity setting enabled
- Show audit results from Windows VMs that do not have a maximum password age of 70 days
- Show audit results from Windows VMs that do not have a minimum password age of 1 day
- Show audit results from Windows VMs that do not restrict the minimum password length to 14 characters
- Show audit results from Windows VMs that allow re-use of the previous 24 passwords

A.10.1.1 Policy on the use of cryptographic controls

This blueprint helps you enforce your policy on the use of cryptograph controls by assigning 13 [Azure Policy](#) definitions that enforce specific cryptograph controls and audit use of weak cryptographic settings. Understanding where your Azure resources may have non-optimal cryptographic configurations can help you take corrective actions to ensure resources are configured in accordance with your information security policy. Specifically, the policies assigned by this blueprint require encryption for blob storage accounts and Data Lake storage accounts; require transparent data encryption on SQL databases; audit missing encryption on storage accounts, SQL databases, virtual machine disks, and automation account variables; audit insecure connections to storage accounts, Function Apps, Web App, API Apps, and Redis Cache; audit weak virtual machine password encryption; and audit unencrypted Service Fabric communication.

- Function App should only be accessible over HTTPS
- Web Application should only be accessible over HTTPS
- API App should only be accessible over HTTPS
- Show audit results from Windows VMs that do not store passwords using reversible encryption
- Disk encryption should be applied on virtual machines
- Automation account variables should be encrypted

- Only secure connections to your Azure Cache for Redis should be enabled
- Secure transfer to storage accounts should be enabled
- Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign
- Transparent Data Encryption on SQL databases should be enabled

A.12.4.1 Event logging

This blueprint helps you ensure system events are logged by assigning seven [Azure Policy](#) definitions that audit log settings on Azure resources. Diagnostic logs provide insight into operations that were performed within Azure resources.

- Audit Dependency agent deployment - VM Image (OS) unlisted
- Audit Dependency agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Audit diagnostic setting
- Auditing on SQL server should be enabled

A.12.4.3 Administrator and operator logs

This blueprint helps you ensure system events are logged by assigning seven Azure Policy definitions that audit log settings on Azure resources. Diagnostic logs provide insight into operations that were performed within Azure resources.

- Audit Dependency agent deployment - VM Image (OS) unlisted
- Audit Dependency agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Audit diagnostic setting
- Auditing on SQL server should be enabled

A.12.4.4 Clock synchronization

This blueprint helps you ensure system events are logged by assigning seven Azure Policy definitions that audit log settings on Azure resources. Azure logs rely on synchronized internal clocks to create a time-correlated record of events across resources.

- Audit Dependency agent deployment - VM Image (OS) unlisted
- Audit Dependency agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Audit diagnostic setting
- Auditing on SQL server should be enabled

A.12.5.1 Installation of software on operational systems

Adaptive application control is solution from Azure Security Center that helps you control which applications can run on your VMs located in Azure. This blueprint assigns an Azure Policy definition that monitors changes to the set of allowed applications. This capability helps you control installation of software and applications on Azure VMs.

- Adaptive application controls for defining safe applications should be enabled on your machines

A.12.6.1 Management of technical vulnerabilities

This blueprint helps you manage information system vulnerabilities by assigning five [Azure Policy](#) definitions that monitor missing system updates, operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources.

- Monitor missing Endpoint Protection in Azure Security Center
- System updates should be installed on your machines
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

A.12.6.2 Restrictions on software installation

Adaptive application control is solution from Azure Security Center that helps you control which applications can run on your VMs located in Azure. This blueprint assigns an Azure Policy definition that monitors changes to the set of allowed applications. Restrictions on software installation can help you reduce the likelihood of introduction of software vulnerabilities.

- Adaptive application controls for defining safe applications should be enabled on your machines

A.13.1.1 Network controls

This blueprint helps you manage and control networks by assigning an [Azure Policy](#) definition that monitors network security groups with permissive rules. Rules that are too permissive may allow unintended network access and should be reviewed. This blueprint also assigns three Azure Policy definitions that monitor unprotected endpoints, applications, and storage accounts. Endpoints and applications that aren't protected by a firewall, and storage accounts with unrestricted access can allow unintended access to information contained within the information system.

- Access through Internet facing endpoint should be restricted
- Storage accounts should restrict network access

A.13.2.1 Information transfer policies and procedures

The blueprint helps you ensure information transfer with Azure services is secure by assigning two [Azure Policy](#) definitions to audit insecure connections to storage accounts and Azure Cache for Redis.

- Only secure connections to your Azure Cache for Redis should be enabled
- Secure transfer to storage accounts should be enabled

Next steps

Now that you've reviewed the control mapping of the ISO 27001 Shared Services blueprint, visit the following articles to learn about the architecture and how to deploy this sample:

[ISO 27001 Shared Services blueprint - Overview](#) [ISO 27001 Shared Services blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).

- Learn how to [update existing assignments](#).

Deploy the ISO 27001 Shared Services blueprint sample

5/2/2021 • 11 minutes to read • [Edit Online](#)

To deploy the Azure Blueprints ISO 27001 Shared Services blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **ISO 27001: Shared Services** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the ISO 27001 Shared Services blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from the ISO 27001 standard.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the ISO 27001 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *system assigned* managed identity option.

- Blueprint parameters

The parameters defined in this section are used by many of the artifacts in the blueprint definition to provide consistency.

- **Organization name**: Enter a short-name for your organization. This property is primarily used for naming resources.
- **Shared services subnet address prefix**: Provide the CIDR notation value for networking the deployed resources together.
- **Shared services location**: Determines what location the artifacts are deployed to. Not all services are available in all locations. Artifacts deploying such services provide a parameter option for the location to deploy that artifact to.
- **Allowed location (Policy: Blueprint initiative for ISO 27001)**: Value that indicates the allowed locations for resource groups and resources.
- **Log Analytics workspace for VM agents (Policy: Blueprint initiative for ISO 27001)**: Specifies the Resource ID of a workspace. This parameter uses a `concat` function to construct the Resource ID.

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint

assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	(Optional) Default value is <i>["none"]</i> .
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	(Optional) Default value is <i>["none"]</i> .
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	(Optional) Default value is <i>["none"]</i> .
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	(Optional) Default value is <i>["none"]</i> .
Allowed resource types	Policy assignment	Allowed resource types	List of resource types allowed to be deployed. This list is composed of all the resource types deployed in Shared Services.
Allowed storage account SKUs	Policy assignment	Allowed storage SKUs	List of diagnostic logs storage account SKUs allowed. Default value is <i>["Standard_LRS"]</i> .
Allowed virtual machine SKUs	Policy assignment	List of virtual machine SKUs allowed to be deployed. Default value is <i>["Standard_DS1_v2", "Standard_DS2_v2"]</i> .	
Blueprint initiative for ISO 27001	Policy assignment	Resource types to audit diagnostic logs	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor diagnostic logs schemas .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Log Analytics resource group	Resource group	Name	Locked - Concatenates the Organization name with <code>-sharedsvsc-log-rg</code> to make the resource group unique.
Log Analytics resource group	Resource group	Location	Locked - Uses the blueprint parameter.
Log Analytics template	Resource Manager template	Service tier	Sets the tier of the Log Analytics workspace. Default value is <i>PerNode</i> .
Log Analytics template	Resource Manager template	Log retention in days	Data retention in days. Default value is <i>365</i> .
Log Analytics template	Resource Manager template	Location	Region used for creating the Log Analytics workspace. Default value is <i>West US 2</i> .
Network resource group	Resource group	Name	Locked - Concatenates the Organization name with <code>-sharedsvcs-net-rg</code> to make the resource group unique.
Network resource group	Resource group	Location	Locked - Uses the blueprint parameter.
Azure Firewall template	Resource Manager template	Azure firewall private IP	Configures the private IP of the Azure firewall . This value is also used as default route table on shared services subnet. Should be part of the CIDR notation defined in Azure Firewall subnet address prefix . Default value is <i>10.0.4.4</i> .
Azure Firewall template	Resource Manager template	Log retention in days	Data retention in days. Default value is <i>365</i> .
Network Security Group template	Resource Manager template	Log retention in days	Data retention in days. Default value is <i>365</i> .
Virtual Network and Route Table template	Resource Manager template	Virtual Network address prefix	The CIDR notation for the virtual network. Default value is <i>10.0.0.0/16</i> .
Virtual Network and Route Table template	Resource Manager template	Enable Virtual Network DDoS protection	Configures DDoS protection for the virtual network. Default value is <i>true</i> .
Virtual Network and Route Table template	Resource Manager template	Shared Services subnet address prefix	The CIDR notation for the Shared Services subnet. Default value is <i>10.0.0.0/24</i> .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Virtual Network and Route Table template	Resource Manager template	DMZ subnet address prefix	The CIDR notation for the DMZ subnet. Default value is <i>10.0.1.0/24</i> .
Virtual Network and Route Table template	Resource Manager template	Application Gateway subnet address prefix	The CIDR notation for the application gateway subnet. Default value is <i>10.0.2.0/24</i> .
Virtual Network and Route Table template	Resource Manager template	Virtual Network Gateway subnet address prefix	The CIDR notation for the virtual network gateway subnet. Default value is <i>10.0.3.0/24</i> .
Virtual Network and Route Table template	Resource Manager template	Azure Firewall subnet address prefix	The CIDR notation for the Azure firewall subnet. Should include the Azure firewall private IP parameter.
Key Vault resource group	Resource group	Name	Locked - Concatenates the Organization name with <code>-sharedsvcs-kv-rg</code> to make the resource group unique.
Key Vault resource group	Resource group	Location	Locked - Uses the blueprint parameter.
Key Vault template	Resource Manager template	Jumpbox admin username	Username for the jumpbox. Must match same property value in Jumpbox template . Default value is <i>jb-admin-user</i> .
Key Vault template	Resource Manager template	Jumpbox admin ssh key or password	Key or password for the account on the jumpbox. Must match same property value in Jumpbox template . No default value and can't be left blank.
Key Vault template	Resource Manager template	Domain admin username	Username used to access Active Directory VM and to join other VMs to a domain. Must match Domain admin user property value in Active Directory Domain Services template . Default value is <i>domain-admin-user</i> .
Key Vault template	Resource Manager template	Domain admin password	Domain admin user's password. No default value and can't be left blank.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Key Vault template	Resource Manager template	AAD object ID	The AAD object identifier of the account that requires access to the Key Vault instance. No default value and can't be left blank. To locate this value from the Azure portal, search for and select "Users" under <i>Services</i> . Use the <i>Name</i> box to filter for the account name and select that account. On the <i>User profile</i> page, select the "Click to copy" icon next to the <i>Object ID</i> .
Key Vault template	Resource Manager template	Log retention in days	Data retention in days. Default value is <i>365</i> .
Key Vault template	Resource Manager template	Key Vault SKU	Specifies the SKU of the Key Vault that is created. Default value is <i>Premium</i> .
Jumpbox resource group	Resource group	Name	Locked - Concatenates the Organization name with <code>-sharedsvcs-jb-rg</code> to make the resource group unique.
Jumpbox resource group	Resource group	Location	Locked - Uses the blueprint parameter.
Jumpbox template	Resource Manager template	Jumpbox admin username	The username used to access jumpbox VMs. Must match same property value in Key Vault template . Default value is <i>jb-admin-user</i> .
Jumpbox template	Resource Manager template	Jumpbox admin password (Key Vault Resource ID)	The Resource ID of the Key Vault. Use <code>"/subscriptions/{subscriptionId}/resourceGroups/{orgName}-sharedsvcs-kv-rg/providers/Microsoft.KeyVault/vaults/{orgName}-sharedsvcs-kv"</code> and replace <code>{subscriptionId}</code> with your Subscription ID and <code>{orgName}</code> with the Organization name blueprint parameter.
Jumpbox template	Resource Manager template	Jumpbox admin password (Key Vault Secret Name)	Username of the jumpbox admin. Must match value in Key Vault template property Jumpbox admin username .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Jumpbox template	Resource Manager template	Jumpbox Operating System	Determines the operating system of the jumpbox VM. Default value is <i>Windows</i> .
Active Directory Domain Services resource group	Resource group	Name	Locked - Concatenates the Organization name with <code>-sharedsvcs-adds-rg</code> to make the resource group unique.
Active Directory Domain Services resource group	Resource group	Location	Locked - Uses the blueprint parameter.
Active Directory Domain Services template	Resource Manager template	Domain admin username	Username for the ADDS jumpbox. Must match same property value in Key Vault template . Default value is <i>adds-admin-user</i> .
Active Directory Domain Services template	Resource Manager template	Domain admin password (Key Vault Resource ID)	The Resource ID of the Key Vault. Use <code>"/subscriptions/{subscriptionId}/resourceGroups/{orgName}-sharedsvcs-kv-rg/providers/Microsoft.KeyVault/vaults/{orgName}-sharedsvcs-kv"</code> and replace <code>{subscriptionId}</code> with your Subscription ID and <code>{orgName}</code> with the Organization name blueprint parameter.
Active Directory Domain Services template	Resource Manager template	Domain admin password (Key Vault Secret Name)	Username of the domain admin. Must match value in Key Vault template property Domain admin username .
Active Directory Domain Services template	Resource Manager template	Domain name	Name of the Active Directory created by the sample. Default value is <i>contoso.com</i> .
Active Directory Domain Services template	Resource Manager template	Domain admin user	Username for the admin AD account and for joining devices to the AD domain. Must match AD admin username property value in Key Vault template . Default value is <i>domain-admin-user</i> .
Active Directory Domain Services template	Resource Manager template	Domain admin password	Set the Key Vault details for storing the password. No default value and can't be left blank.

Next steps

Now that you've reviewed the steps to deploy the ISO 27001 Shared Services blueprint sample, visit the following articles to learn about the architecture and control mapping:

[ISO 27001 Shared Services blueprint - Overview](#) [ISO 27001 Shared Services blueprint - Control mapping](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the ISO 27001 App Service Environment/SQL Database workload blueprint sample

5/3/2021 • 2 minutes to read • [Edit Online](#)

The ISO 27001 App Service Environment/SQL Database workload blueprint sample provides additional infrastructure to the [ISO 27001 Shared Services](#) blueprint sample. This blueprint helps customers deploy cloud-based architectures that offer solutions to scenarios that have accreditation or compliance requirements.

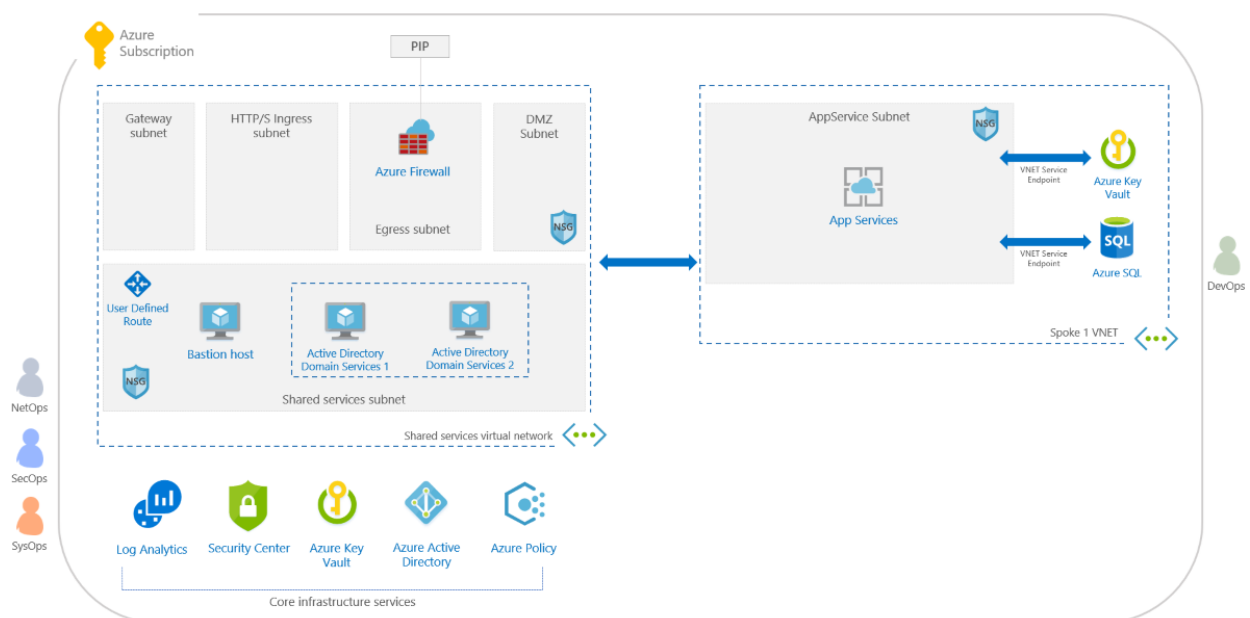
There are two ISO 27001 blueprint samples, this sample and the [ISO 27001 Shared Services](#) blueprint sample.

IMPORTANT

This sample is dependent on infrastructure deployed by the [ISO 27001 Shared Services](#) blueprint sample. It must be deployed first.

Architecture

The ISO 27001 App Service Environment/SQL Database workload blueprint sample deploys a platform as a service-based web environment. The environment can be used to host multiple web applications, web APIs, and SQL Database instances that follow the ISO 27001 standards. This blueprint sample depends on the [ISO 27001 Shared Services](#) blueprint sample.



This environment is composed of several Azure services used to provide a secure, fully monitored, enterprise-ready workload infrastructure based on ISO 27001 standards. This environment is composed of:

- [Azure role](#) named DevOps that has rights to deploy and manage resources in an [Azure App Service Environments](#) deployed by the blueprint sample
- [Azure Policy](#) definitions to lock down what services can be deployed to the environment and denying the creation of any public IP address (PIP) resource
- A virtual network containing a single subnet and peered back to a pre-existing [shared services](#) environment

and forcing all traffic to pass by the [shared services](#) firewall. The virtual network hosts the following resources:

- An [Azure App Service Environment](#) that can be used to host one or more web applications, web APIs, or functions
- An [Azure Key Vault](#) instance using a VNet service endpoint, for storing secrets used by applications running in the workload environment
- An [Azure SQL Database](#) server instance using a VNet service endpoint, for hosting databases used for applications in the workload environment

Next steps

You've reviewed the overview and architecture of the ISO 27001 App Service Environment/SQL Database workload blueprint sample. Next, visit the following articles to learn about the control mapping and how to deploy this sample:

[ISO 27001 App Service Environment/SQL Database workload blueprint - Control mapping](#) [ISO 27001 App Service Environment/SQL Database workload blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Control mapping of the ISO 27001 ASE/SQL workload blueprint sample

5/3/2021 • 11 minutes to read • [Edit Online](#)

The following article details how the Azure Blueprints ISO 27001 ASE/SQL Workload blueprint sample maps to the ISO 27001 controls. For more information about the controls, see [ISO 27001](#).

The following mappings are to the **ISO 27001:2013** controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an [Azure Policy](#) initiative. To review the complete initiative, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **[Preview] Audit ISO 27001:2013 controls and deploy specific VM Extensions to support audit requirements** built-in policy initiative.

IMPORTANT

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy definitions for this compliance blueprint sample may change over time. To view the change history, see the [GitHub Commit History](#).

A.6.1.2 Segregation of duties

Having only one Azure subscription owner doesn't allow for administrative redundancy. Conversely, having too many Azure subscription owners can increase the potential for a breach via a compromised owner account. This blueprint helps you maintain an appropriate number of Azure subscription owners by assigning two [Azure Policy](#) definitions that audit the number of owners for Azure subscriptions. Managing subscription owner permissions can help you implement appropriate separation of duties.

- A maximum of 3 owners should be designated for your subscription
- There should be more than one owner assigned to your subscription

A.8.2.1 Classification of information

Azure's [SQL Vulnerability Assessment service](#) can help you discover sensitive data stored in your databases and includes recommendations to classify that data. This blueprint assigns an [Azure Policy](#) definition to audit that vulnerabilities identified during SQL Vulnerability Assessment scan are remediated.

- Vulnerabilities on your SQL databases should be remediated

A.9.1.2 Access to networks and network services

Azure implements [Azure role-based access control \(Azure RBAC\)](#) to manage who has access to Azure resources. This blueprint helps you control access to Azure resources by assigning seven [Azure Policy](#) definitions. These policies audit use of resource types and configurations that may allow more permissive access to resources. Understanding resources that are in violation of these policies can help you take corrective actions to ensure access Azure resources is restricted to authorized users.

- Show audit results from Linux VMs that have accounts without passwords
- Show audit results from Linux VMs that allow remote connections from accounts without passwords
- Storage accounts should be migrated to new Azure Resource Manager resources
- Virtual machines should be migrated to new Azure Resource Manager resources
- Audit VMs that do not use managed disks

A.9.2.3 Management of privileged access rights

This blueprint helps you restrict and control privileged access rights by assigning four [Azure Policy](#) definitions to audit external accounts with owner and/or write permissions and accounts with owner and/or write permissions that don't have multi-factor authentication enabled. Azure role-based access control (Azure RBAC) helps to manage who has access to Azure resources. This blueprint also assigns three Azure Policy definitions to audit use of Azure Active Directory authentication for SQL Servers and Service Fabric. Using Azure Active Directory authentication enables simplified permission management and centralized identity management of database users and other Microsoft services. This blueprint also assigns an Azure Policy definition to audit the use of custom Azure RBAC rules. Understanding where custom Azure RBAC rules are implemented can help you verify need and proper implementation, as custom Azure RBAC rules are error prone.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription
- External accounts with owner permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription
- An Azure Active Directory administrator should be provisioned for SQL servers
- Service Fabric clusters should only use Azure Active Directory for client authentication
- Audit usage of custom RBAC rules

A.9.2.4 Management of secret authentication information of users

This blueprint assigns three [Azure Policy](#) definitions to audit accounts that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised. This blueprint also assigns two Azure Policy definitions that audit Linux VM password file permissions to alert if they're set incorrectly. This setup enables you to take corrective action to ensure authenticators aren't compromised.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled on accounts with read permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription
- Show audit results from Linux VMs that do not have the passwd file permissions set to 0644

A.9.2.5 Review of user access rights

Azure implements [Azure role-based access control \(Azure RBAC\)](#) to help you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint assigns four [Azure Policy](#) definitions to audit accounts that should be prioritized for review, including deprecated accounts and external accounts with elevated permissions.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription
- External accounts with owner permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription

A.9.2.6 Removal or adjustment of access rights

Azure implements [Azure role-based access control \(Azure RBAC\)](#) to help you manage who has access to resources in Azure. Using [Azure Active Directory](#) and Azure RBAC, you can update user roles to reflect organizational changes. When needed, accounts can be blocked from signing in (or removed), which immediately removes access rights to Azure resources. This blueprint assigns two [Azure Policy](#) definitions to audit deprecated account that should be considered for removal.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription

A.9.4.2 Secure log-on procedures

This blueprint assigns three Azure Policy definitions to audit accounts that don't have multi-factor authentication enabled. Azure AD Multi-Factor Authentication provides additional security by requiring a second form of authentication and delivers strong authentication. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled on accounts with read permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription

A.9.4.3 Password management system

This blueprint helps you enforce strong passwords by assigning 10 [Azure Policy](#) definitions that audit Windows VMs that don't enforce minimum strength and other password requirements. Awareness of VMs in violation of the password strength policy helps you take corrective actions to ensure passwords for all VM user accounts are compliant with policy.

- Show audit results from Windows VMs that do not have the password complexity setting enabled
- Show audit results from Windows VMs that do not have a maximum password age of 70 days
- Show audit results from Windows VMs that do not have a minimum password age of 1 day
- Show audit results from Windows VMs that do not restrict the minimum password length to 14 characters
- Show audit results from Windows VMs that allow re-use of the previous 24 passwords

A.10.1.1 Policy on the use of cryptographic controls

This blueprint helps you enforce your policy on the use of cryptograph controls by assigning 13 [Azure Policy](#) definitions that enforce specific cryptograph controls and audit use of weak cryptographic settings. Understanding where your Azure resources may have non-optimal cryptographic configurations can help you take corrective actions to ensure resources are configured in accordance with your information security policy. Specifically, the policies assigned by this blueprint require encryption for blob storage accounts and data lake storage accounts; require transparent data encryption on SQL databases; audit missing encryption on storage accounts, SQL databases, virtual machine disks, and automation account variables; audit insecure connections to storage accounts, Function Apps, Web App, API Apps, and Redis Cache; audit weak virtual machine password encryption; and audit unencrypted Service Fabric communication.

- Function App should only be accessible over HTTPS
- Web Application should only be accessible over HTTPS
- API App should only be accessible over HTTPS
- Show audit results from Windows VMs that do not store passwords using reversible encryption
- Disk encryption should be applied on virtual machines
- Automation account variables should be encrypted

- Only secure connections to your Azure Cache for Redis should be enabled
- Secure transfer to storage accounts should be enabled
- Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign
- Transparent Data Encryption on SQL databases should be enabled

A.12.4.1 Event logging

This blueprint helps you ensure system events are logged by assigning seven [Azure Policy](#) definitions that audit log settings on Azure resources. Diagnostic logs provide insight into operations that were performed within Azure resources.

- Audit Dependency agent deployment - VM Image (OS) unlisted
- Audit Dependency agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Audit diagnostic setting
- Auditing on SQL server should be enabled

A.12.4.3 Administrator and operator logs

This blueprint helps you ensure system events are logged by assigning seven Azure Policy definitions that audit log settings on Azure resources. Diagnostic logs provide insight into operations that were performed within Azure resources.

- Audit Dependency agent deployment - VM Image (OS) unlisted
- Audit Dependency agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Audit diagnostic setting
- Auditing on SQL server should be enabled

A.12.4.4 Clock synchronization

This blueprint helps you ensure system events are logged by assigning seven Azure Policy definitions that audit log settings on Azure resources. Azure logs rely on synchronized internal clocks to create a time-correlated record of events across resources.

- Audit Dependency agent deployment - VM Image (OS) unlisted
- Audit Dependency agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Audit Log Analytics agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Audit diagnostic setting
- Auditing on SQL server should be enabled

A.12.5.1 Installation of software on operational systems

Adaptive application control is solution from Azure Security Center that helps you control which applications can run on your VMs located in Azure. This blueprint assigns an Azure Policy definition that monitors changes to the set of allowed applications. This capability helps you control installation of software and applications on Azure VMs.

- Adaptive application controls for defining safe applications should be enabled on your machines

A.12.6.1 Management of technical vulnerabilities

This blueprint helps you manage information system vulnerabilities by assigning five [Azure Policy](#) definitions that monitor missing system updates, operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources.

- Monitor missing Endpoint Protection in Azure Security Center
- System updates should be installed on your machines
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

A.12.6.2 Restrictions on software installation

Adaptive application control is solution from Azure Security Center that helps you control which applications can run on your VMs located in Azure. This blueprint assigns an Azure Policy definition that monitors changes to the set of allowed applications. Restrictions on software installation can help you reduce the likelihood of introduction of software vulnerabilities.

- Adaptive application controls for defining safe applications should be enabled on your machines

A.13.1.1 Network controls

This blueprint helps you manage and control networks by assigning an [Azure Policy](#) definition that monitors network security groups with permissive rules. Rules that are too permissive may allow unintended network access and should be reviewed. This blueprint also assigns three Azure Policy definitions that monitor unprotected endpoints, applications, and storage accounts. Endpoints and applications that aren't protected by a firewall, and storage accounts with unrestricted access can allow unintended access to information contained within the information system.

- Access through Internet facing endpoint should be restricted
- Storage accounts should restrict network access

A.13.2.1 Information transfer policies and procedures

The blueprint helps you ensure information transfer with Azure services is secure by assigning two [Azure Policy](#) definitions to audit insecure connections to storage accounts and Azure Cache for Redis.

- Only secure connections to your Azure Cache for Redis should be enabled
- Secure transfer to storage accounts should be enabled

Next steps

Now that you've reviewed the control mapping of the ISO 27001 App Service Environment/SQL Database workload blueprint sample, visit the following articles to learn about the architecture and how to deploy this sample:

[ISO 27001 App Service Environment/SQL Database workload blueprint - Overview](#) [ISO 27001 App Service Environment/SQL Database workload blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).

- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the ISO 27001 App Service Environment/SQL Database workload blueprint sample

5/2/2021 • 9 minutes to read • [Edit Online](#)

To deploy the Azure Blueprints ISO 27001 App Service Environment/SQL Database workload blueprint sample, the following steps must be taken:

- Deploy the [ISO 27001 Shared Services](#) blueprint sample
- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Deploy the ISO 27001 Shared Services blueprint sample

Before this blueprint sample can be deployed, the [ISO 27001 Shared Services](#) blueprint sample must be deployed to the target subscription. Without a successful deployment of the ISO 27001 Shared Services blueprint sample, this blueprint sample will be missing infrastructure dependencies and fail during deployment.

IMPORTANT

This blueprint sample must be assigned in the same subscription as the [ISO 27001 Shared Services](#) blueprint sample.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **ISO 27001: ASE/SQL Workload** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the ISO 27001 ASE/SQL workload blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from the ISO 27001 standard.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the ISO 27001 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:

- Basics

- **Subscriptions:** Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
- **Assignment name:** The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
- **Location:** Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
- **Blueprint definition version:** Pick a **Published** version of your copy of the blueprint sample.

- Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *system assigned* managed identity option.

- Blueprint parameters

The parameters defined in this section are used by many of the artifacts in the blueprint definition to provide consistency.

- **Organization name:** Enter a short-name for your organization. This property is primarily used for naming resources.
- **Shared Service Subscription ID:** Subscription ID where the [ISO 27001 Shared Services](#)

blueprint sample is assigned.

- **Default subnet address prefix:** The CIDR notation for the virtual network default subnet. Default value is *10.1.0.0/24*.
- **Workload location:** Determines what location the artifacts are deployed to. Not all services are available in all locations. Artifacts deploying such services provide a parameter option for the location to deploy that artifact to.
- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Log Analytics resource group	Resource group	Name	Locked - Concatenates the Organization name with <code>-workload-log-rg</code> to make the resource group unique.
Log Analytics resource group	Resource group	Location	Locked - Uses the blueprint parameter.
Log Analytics template	Resource Manager template	Service tier	Sets the tier of the Log Analytics workspace. Default value is <i>PerNode</i> .
Log Analytics template	Resource Manager template	Log retention in days	Data retention in days. Default value is <i>365</i> .
Log Analytics template	Resource Manager template	Location	Region used for creating the Log Analytics workspace. Default value is <i>West US 2</i> .
Network resource group	Resource group	Name	Locked - Concatenates the Organization name with <code>-workload-net-rg</code> to make the resource group unique.
Network resource group	Resource group	Location	Locked - Uses the blueprint parameter.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Network Security Group template	Resource Manager template	Log retention in days	Data retention in days. Default value is <i>365</i> .
Virtual Network and Route Table template	Resource Manager template	Azure firewall private IP	Configures the private IP of the Azure firewall . Should be part of the CIDR notation defined in <i>ISO 27001: Shared Services</i> artifact parameter Azure Firewall subnet address prefix . Default value is <i>10.0.4.4</i> .
Virtual Network and Route Table template	Resource Manager template	Virtual Network address prefix	The CIDR notation for the virtual network. Default value is <i>10.1.0.0/16</i> .
Virtual Network and Route Table template	Resource Manager template	ADDS IP address	IP address of the first ADDS VM. This value is used as custom VNET DNS.
Virtual Network and Route Table template	Resource Manager template	Log retention in days	Data retention in days. Default value is <i>365</i> .
Virtual Network and Route Table template	Resource Manager template	Virtual Network Peering name	Value used to enable VNET peering between a Workload and Shared Services.
Key Vault resource group	Resource group	Name	Locked - Concatenates the Organization name with <code>-workload-kv-rg</code> to make the resource group unique.
Key Vault resource group	Resource group	Location	Locked - Uses the blueprint parameter.
Key Vault template	Resource Manager template	AAD object ID	The AAD object identifier of the account that requires access to the Key Vault instance. No default value and can't be left blank. To locate this value from the Azure portal, search for and select "Users" under <i>Services</i> . Use the <i>Name</i> box to filter for the account name and select that account. On the <i>User profile</i> page, select the "Click to copy" icon next to the <i>Object ID</i> .
Key Vault template	Resource Manager template	Log retention in days	Data retention in days. Default value is <i>365</i> .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Key Vault template	Resource Manager template	Key Vault SKU	Specifies the SKU of the Key Vault that is created. Default value is <i>Premium</i> .
Key Vault template	Resource Manager template	Azure SQL Server admin username	The username used to access Azure SQL Server. Must match same property value in Azure SQL Database template . Default value is <i>sql-admin-user</i> .
Key Vault template	Resource Manager template	Azure SQL Server admin password	The password for the Azure SQL Server admin username
Azure SQL Database resource group	Resource group	Name	Locked - Concatenates the Organization name with <code>-workload-azsql-rg</code> to make the resource group unique.
Azure SQL Database resource group	Resource group	Location	Locked - Uses the blueprint parameter.
Azure SQL Database template	Resource Manager template	Azure SQL Server admin username	Username for the Azure SQL Server. Must match same property value in Key Vault template . Default value is <i>sql-admin-user</i> .
Azure SQL Database template	Resource Manager template	Azure SQL Server admin password (Key vault resource ID)	The Resource ID of the Key Vault. Use <code>"/subscriptions/{subscriptionId}/resourceGroups/{orgName}-workload-kv-rg/providers/Microsoft.KeyVault/vaults/{orgName}-workload-kv"</code> and replace <code>{subscriptionId}</code> with your Subscription ID and <code>{orgName}</code> with the Organization name blueprint parameter.
Azure SQL Database template	Resource Manager template	Azure SQL Server admin password (Key vault secret name)	Username of the SQL Server admin. Must match value in Key Vault template property Azure SQL Server admin username .
Azure SQL Database template	Resource Manager template	Azure SQL Server admin password (Key vault secret version)	Key vault secret version (leave empty for new deployments)

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Azure SQL Database template	Resource Manager template	Log retention in days	Data retention in days. Default value is <i>365</i> .
Azure SQL Database template	Resource Manager template	AAD admin object ID	AAD object ID of the user that will get assigned as an Active Directory admin. No default value and can't be left blank. To locate this value from the Azure portal, search for and select "Users" under <i>Services</i> . Use the <i>Name</i> box to filter for the account name and select that account. On the <i>User profile</i> page, select the "Click to copy" icon next to the <i>Object ID</i> .
Azure SQL Database template	Resource Manager template	AAD admin login	Currently, Microsoft accounts (such as live.com or outlook.com) can't be set as admin. Only users and security groups within your organization can be set as admin. No default value and can't be left blank. To locate this value from the Azure portal, search for and select "Users" under <i>Services</i> . Use the <i>Name</i> box to filter for the account name and select that account. On the <i>User profile</i> page, copy the <i>User name</i> .
App Service Environment resource group	Resource group	Name	Locked - Concatenates the Organization name with <code>-workload-ase-rg</code> to make the resource group unique.
App Service Environment resource group	Resource group	Location	Locked - Uses the blueprint parameter.
App Service Environment template	Resource Manager template	Domain name	Name of the Active Directory created by the sample. Default value is <i>contoso.com</i> .
App Service Environment template	Resource Manager template	ASE location	App Service Environment location. Default value is <i>West US 2</i> .
App Service Environment template	Resource Manager template	Application Gateway log retention in days	Data retention in days. Default value is <i>365</i> .

Next steps

Now that you've reviewed the steps to deploy the ISO 27001 App Service Environment/SQL Database workload blueprint sample, visit the following articles to learn about the architecture and control mapping:

[ISO 27001 App Service Environment/SQL Database workload blueprint - Overview](#) [ISO 27001 App Service Environment/SQL Database workload blueprint - Control mapping](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the Media blueprint sample

5/3/2021 • 2 minutes to read • [Edit Online](#)

Media blueprint sample provides a set of governance guardrails using [Azure Policy](#) that help toward [Media](#) attestation.

Blueprint sample

The blueprint sample helps customers deploy a core set of policies for any Azure-deployed architecture requiring accreditation or compliance with the Media framework. The [control mapping](#) section provides details on policies included within this initiative and how these policies help meet various controls defined by Media framework. When assigned to an architecture, resources are evaluated by Azure Policy for compliance with assigned policies.

Next steps

You've reviewed the overview of the Media blueprint sample. Next, visit the following articles to learn about the control mapping and how to deploy this sample:

[Media blueprint - Control mapping](#) [Media blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Control mapping of the Media blueprint sample

4/28/2021 • 8 minutes to read • [Edit Online](#)

The following article details how the Azure Blueprints Media blueprint sample maps to the Media controls. For more information about the controls, see [Media](#).

The following mappings are to the **Media** controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an [Azure Policy](#) initiative. To review the complete initiative, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **[Preview]: Audit Media controls** built-in policy initiative.

IMPORTANT

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy definitions for this compliance blueprint sample may change over time. To view the change history, see the [GitHub Commit History](#).

Access Control

AC-1.1- Ensure no root access key exists

- [Preview]: Deploy prerequisites to audit Windows VMs that do not contain the specified certificates in Trusted Root

AC-1.2 - Passwords, PINs, and Tokens must be protected

- [Preview]: Deploy prerequisites to audit Windows VMs that do not restrict the minimum password length to 14 characters

AC-1.8 - Shared account access is prohibited

- All authorization rules except RootManageSharedAccessKey should be removed from Service Bus namespace

AC-1.9 -System must restrict access to authorized users.

- Audit unrestricted network access to storage accounts

AC- 1.14 -System must enforce access rights.

- [Preview]: Deploy prerequisites to audit Windows VMs configurations in 'User Rights Assignment'

AC- 1.15 -Prevent unauthorized access to security relevant information or functions.

- [Preview]: Show audit results from Windows VMs configurations in 'Security Options - System settings'

AC-1-21 - Separation of duties must be enforced through appropriate assignment of role.

- [Preview]: Role-Based Access Control (RBAC) should be used on Kubernetes Services

AC-1.40- Ensure that systems are not connecting trusted network and untrusted networks at the same time.

- [Preview]: Deploy prerequisites to audit Windows VMs configurations in 'Security Options - Network Access'

AC-1.42 & AC- 1.43 - Remote access for non-employees must be restricted to allow access only to specifically

approved information systems

- [Preview]: Show audit results from Linux VMs that allow remote connections from accounts without passwords

AC-1.50- Log security related events for all information system components.

- Diagnostic logs in Logic Apps should be enabled

AC-1.54- Ensure multi-factor authentication (MFA) is enabled for all cloud console users.

- MFA should be enabled accounts with write permissions on your subscription
- Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.

Auditing & Logging

AL-2.1- Successful and unsuccessful events must be logged.

- Diagnostic logs in Search services should be enabled

AL -2.16 - Network devices/instances must log any event classified as a critical security event by that network device/instance (ELBs, web application firewalls, etc.)

- [Preview]: Show audit results from Windows VMs configurations in 'Security Options - Accounts'

AL-2.17- Servers/instances must log any event classified as a critical security event by that server/instance

- [Preview]: Show audit results from Windows VMs configurations in 'Security Options - Accounts'

AL-2.19 - Domain events must log any event classified as a critical or high security event by the domain management software

- [Preview]: Show audit results from Windows VMs configurations in 'Security Options - Accounts'
- [Preview]: Deploy prerequisites to audit Windows VMs configurations in 'Security Options - Microsoft Network Client'

AL-2.20- Domain events must log any event classified as a critical security event by domain security controls

- [Preview]: Show audit results from Windows VMs configurations in 'Security Options - Accounts'

AL-2.21- Domain events must log any access or changes to the domain log

- [Preview]: Show audit results from Windows VMs configurations in 'Security Options - Recovery console'

Cryptographic Controls

CC-4.2- Applications and systems must use current cryptographic solutions for protecting data.

- Transparent Data Encryption on SQL databases should be enabled
- Transparent data encryption should be enabled to protect data-at-rest and meet compliance requirements

CC-4.5- Digital Certificates must be signed by an approved Certificate Authority.

- [Preview]: Show audit results from Windows VMs that contain certificates expiring within the specified number of days

CC-4.6- Digital Certificates must be uniquely assigned to a user or device.

- [Preview]: Deploy prerequisites to audit Windows VMs that contain certificates expiring within the specified number of days

CC-4.7- Cryptographic material must be stored to enable decryption of the records for the length of time the records are retained.

- Disk encryption should be applied on virtual machines
- VMs without an enabled disk encryption will be monitored by Azure Security Center as recommendations

CC-4.8- Secret and private keys must be stored securely.

- Transparent Data Encryption on SQL databases should be enabled
- Transparent data encryption should be enabled to protect data-at-rest and meet compliance requirements

Change & Config Management

CM-5.2- Only authorized users may implement approved changes on the system.

- System updates should be installed on your machines
- Missing security system updates on your servers will be monitored by Azure Security Center as recommendations

CM-5.12- Maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

- System updates should be installed on your machines
- Missing security system updates on your servers will be monitored by Azure Security Center as recommendations

CM-5.13- Employ automated tools to maintain a baseline configuration of the information system.

- System updates should be installed on your machines
- Missing security system updates on your servers will be monitored by Azure Security Center as recommendations

CM-5.14- Identify and disable unnecessary and/or non-secure functions, ports, protocols and services.

- Network interfaces should disable IP forwarding
- [Preview]: IP Forwarding on your virtual machine should be disabled

CM-5.19- Monitor changes to the security configuration settings.

- Deploy Diagnostic Settings for Network Security Groups

CM-5.22- Ensure that only authorized software and updates are installed on Company systems.

- System updates should be installed on your machines
- Missing security system updates on your servers will be monitored by Azure Security Center as recommendations

Identity & Authentication

IA-7.1- User accounts must be uniquely assigned to individuals for access to information that is not classified as Public. Account IDs must be constructed using a standardized logical format.

- External accounts with owner permissions should be removed from your subscription
- External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.

Network Security

NS-9.2- Access to network device management functionality is restricted to authorized users.

- [Preview]: Deploy prerequisites to audit Windows VMs configurations in 'Security Options - Network Access'

NS-9.3- All network devices must be configured using their most secure configurations.

- [Preview]: Deploy prerequisites to audit Windows VMs configurations in 'Security Options - Network Access'

NS-9.5- All network connections to a system through a firewall must be approved and audited on a regular basis.

- [Preview]: Show audit results from Windows VMs configurations in 'Windows Firewall Properties'

NS-9.7- Appropriate controls must be present at any boundary between a trusted network and any untrusted or public network.

- [Preview]: Deploy prerequisites to audit Windows VMs configurations in 'Windows Firewall Properties'

Security Planning

SP-11.3- Threats must be identified that could negatively impact the confidentiality, integrity, or availability of Company information and content along with the likelihood of their occurrence.

- Advanced Threat Protection types should be set to 'All' in SQL managed instance Advanced Data Security settings

Security Continuity

SC-12.5- Data in long-term storage must be accessible throughout the retention period and protected against media degradation and technology changes.

- SQL servers should be configured with auditing retention days greater than 90 days.
- Audit SQL servers configured with an auditing retention period of less than 90 days.

System Integrity

SI-14.3- Only authorized personnel may monitor network and user activities.

- Vulnerabilities on your SQL databases should be remediated
- Monitor Vulnerability Assessment scan results and recommendations for how to remediate database vulnerabilities.

SI-14.4- Internet facing systems must have intrusion detection.

- Deploy Threat Detection on SQL servers

SI-14.13- Standardized centrally managed anti-malware software should be implemented across the company.

- Deploy default Microsoft IaaSAntimalware extension for Windows Server

SI-14.14- Anti-malware software must scan computers and media weekly at a minimum.

- Deploy default Microsoft IaaSAntimalware extension for Windows Server

Vulnerability Management

VM-15.4- Ensure that applications are scanned for vulnerabilities on a monthly basis.

- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.

VM-15.5- Ensure that vulnerabilities are identified, paired to threats, and evaluated for risk.

- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.

VM-15.6- Ensure that identified vulnerabilities have been remediated within a mutually agreed upon timeline.

- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.

VM-15.7- Access to and use of vulnerability management systems must be restricted to authorized personnel.

- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.

NOTE

Availability of specific Azure Policy definitions may vary in Azure Government and other national clouds.

Next steps

You've reviewed the control mapping of the Media blueprint sample. Next, visit the following articles to learn about the overview and how to deploy this sample:

[Media blueprint - Overview](#) [Media blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the Media blueprint sample

4/5/2021 • 6 minutes to read • [Edit Online](#)

To deploy the Media blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** and search for and select **Policy** in the left pane. On the **Policy** page, select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **Media** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from the standard.

1. Select **All services** and search for and select **Policy** in the left pane. On the **Policy** page, select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the Media blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription

within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** and search for and select **Policy** in the left pane. On the **Policy** page, select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - **Basics**
 - **Subscriptions:** Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name:** The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location:** Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version:** Pick a **Published** version of your copy of the blueprint sample.
 - **Lock Assignment**

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - **Managed Identity**

Leave the default *system assigned* managed identity option.
 - **Artifact parameters**

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
---------------	---------------	----------------	-------------

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Log Analytics workspace for Linux VMs	For more information, see Create a Log Analytics workspace in the Azure portal .
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: <code>[]</code>
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: <code>[]</code>
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Log Analytics workspace for Windows VMs	For more information, see Create a Log Analytics workspace in the Azure portal .
[Preview]: Audit Media controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Log Analytics workspace ID that VMs should be configured for	This is the ID (GUID) of the Log Analytics workspace that the VMs should be configured for.
[Preview]: Audit Media controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting isn't enabled. Acceptable values can be found at Azure Monitor diagnostic logs schemas .
[Preview]: Audit Media controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Administrators group	Group. Example: <code>Administrator; myUser1; myUser2</code>
[Preview]: Audit Media controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be included in Windows VM Administrators group	A semicolon-separated list of members that should be included in the Administrators local group. Example: <code>Administrator; myUser1; myUser2</code>
Deploy Advanced Threat Protection on Storage Accounts	Policy assignment	Effect	Information about policy effects can be found at Understand Azure Policy Effects .
Deploy Auditing on SQL servers	Policy assignment	The value in days of the retention period (0 indicates unlimited retention)	Retention days (optional, <i>180</i> days if unspecified)

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Deploy Auditing on SQL servers	Policy assignment	Resource group name for storage account for SQL server auditing	Auditing writes database events to an audit log in your Azure Storage account (a storage account is created in each region where a SQL Server is created that is shared by all servers in that region). Important - for proper operation of Auditing don't delete or rename the resource group or the storage accounts.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Storage account prefix for network security group diagnostics	This prefix is combined with the network security group location to form the created storage account name.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Resource group name for storage account for network security group diagnostics (must exist)	The resource group that the storage account is created in. This resource group must already exist.

Next steps

Now that you've reviewed the steps to deploy the Media sample, visit the following articles to learn about the overview and control mapping:

[Media blueprints - Overview](#) [Media blueprints - Control mapping](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

New Zealand ISM Restricted blueprint sample

5/3/2021 • 17 minutes to read • [Edit Online](#)

The New Zealand ISM Restricted blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific [New Zealand Information Security Manual](#) controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement controls for New Zealand ISM Restricted.

Control mapping

The [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **controls** in the New Zealand Information Security Manual. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints New Zealand ISM Restricted blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **New Zealand ISM Restricted** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the New Zealand ISM Restricted blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that are included in the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with New Zealand ISM Restricted controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the New Zealand ISM Restricted blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - Managed Identity

Leave the default *system assigned* managed identity option.
 - Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are **priced by product**. Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
New Zealand ISM Restricted	Policy Assignment	List of users that must be included in Windows VM Administrators group	A semicolon-separated list of users that should be included in the Administrators local group; Ex: Administrator; myUser1; myUser2
New Zealand ISM Restricted	Policy Assignment	List of users that must be excluded from Windows VM Administrators group	A semicolon-separated list of users that should be excluded in the Administrators local group; Ex: Administrator; myUser1; myUser2
New Zealand ISM Restricted	Policy Assignment	List of users that Windows VM Administrators group must only include	A semicolon-separated list of all the expected members of the Administrators local group; Ex: Administrator; myUser1; myUser2
New Zealand ISM Restricted	Policy Assignment	Log Analytics workspace ID for VM agent reporting	ID (GUID) of the Log Analytics workspace where VMs agents should report
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Web Application Firewall (WAF) should be enabled for Azure Front Door Service	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Adaptive network hardening recommendations should be applied on internet facing virtual machines	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: There should be more than one owner assigned to your subscription	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Disk encryption should be applied on virtual machines	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Remote debugging should be turned off for Function Apps	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Web Application Firewall (WAF) should use the specified mode for Application Gateway	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	WAF mode requirement for Application Gateway	The Prevention or Detection mode must be enabled on the Application Gateway service
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Transparent Data Encryption on SQL databases should be enabled	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Vulnerability assessment should be enabled on SQL Managed Instance	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Optional: List of custom VM images that have supported Windows OS to add to scope additional to the images in the gallery for policy: Deploy - Configure Dependency agent to be enabled on Windows virtual machines	For more information on Guest Configuration, visit https://aka.ms/gcpol
New Zealand ISM Restricted	Policy Assignment	Effect for policy: An Azure Active Directory administrator should be provisioned for SQL servers	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Only secure connections to your Azure Cache for Redis should be enabled	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Endpoint protection solution should be installed on virtual machine scale sets	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
New Zealand ISM Restricted	Policy Assignment	Include Arc-connected servers when evaluating policy: Audit Windows machines missing any of specified members in the Administrators group	By selecting 'true', you agree to be charged monthly per Arc connected machine
New Zealand ISM Restricted	Policy Assignment	Optional: List of custom VM images that have supported Windows OS to add to scope additional to the images in the gallery for policy: [Preview]: Log Analytics Agent should be enabled for listed virtual machine images	For more information on Guest Configuration, visit https://aka.ms/gcpol
New Zealand ISM Restricted	Policy Assignment	Optional: List of custom VM images that have supported Linux OS to add to scope additional to the images in the gallery for policy: [Preview]: Log Analytics Agent should be enabled for listed virtual machine images	For more information on Guest Configuration, visit https://aka.ms/gcpol
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Storage accounts should restrict network access	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Optional: List of custom VM images that have supported Windows OS to add to scope additional to the images in the gallery for policy: Deploy - Configure Dependency agent to be enabled on Windows virtual machine scale sets	For more information on Guest Configuration, visit https://aka.ms/gcpol
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Vulnerabilities in security configuration on your virtual machine scale sets should be remediated	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Include Arc-connected servers when evaluating policy: Audit Windows machines that have extra accounts in the Administrators group	By selecting 'true', you agree to be charged monthly per Arc connected machine
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Secure transfer to storage accounts should be enabled	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Web Application Firewall (WAF) should use the specified mode for Azure Front Door Service	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	WAF mode requirement for Azure Front Door Service	The Prevention or Detection mode must be enabled on the Azure Front Door service
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Adaptive application controls for defining safe applications should be enabled on your machines	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: A maximum of 3 owners should be designated for your subscription	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: [Preview]: Storage account public access should be disallowed	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: A vulnerability assessment solution should be enabled on your virtual machines	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Web Application Firewall (WAF) should be enabled for Application Gateway	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: CORS should not allow every resource to access your Web Applications	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Include Arc-connected servers when evaluating policy: Audit Windows web servers that are not using secure communication protocols	By selecting 'true', you agree to be charged monthly per Arc connected machine
New Zealand ISM Restricted	Policy Assignment	Minimum TLS version for Windows web servers	Windows web servers with lower TLS versions will be assessed as non-compliant

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
New Zealand ISM Restricted	Policy Assignment	Optional: List of custom VM images that have supported Linux OS to add to scope additional to the images in the gallery for policy: Log Analytics agent should be enabled in virtual machine scale sets for listed virtual machine images	For more information on Guest Configuration, visit https://aka.ms/gcpol
New Zealand ISM Restricted	Policy Assignment	Optional: List of custom VM images that have supported Windows OS to add to scope additional to the images in the gallery for policy: Log Analytics agent should be enabled in virtual machine scale sets for listed virtual machine images	For more information on Guest Configuration, visit https://aka.ms/gcpol
New Zealand ISM Restricted	Policy Assignment	Effect for policy: External accounts with write permissions should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Include Arc-connected servers when evaluating policy: Audit Windows machines that have the specified members in the Administrators group	By selecting 'true', you agree to be charged monthly per Arc connected machine
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Deprecated accounts should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Function App should only be accessible over HTTPS	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Azure subscriptions should have a log profile for Activity Log	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	List of resource types that should have diagnostic logs enabled	
New Zealand ISM Restricted	Policy Assignment	Effect for policy: System updates should be installed on your machines	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Latest TLS version should be used in your API App	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
New Zealand ISM Restricted	Policy Assignment	Effect for policy: MFA should be enabled accounts with write permissions on your subscription	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Microsoft IaaS Antimalware extension should be deployed on Windows servers	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Web Application should only be accessible over HTTPS	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Azure DDoS Protection Standard should be enabled	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: MFA should be enabled on accounts with owner permissions on your subscription	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Advanced data security should be enabled on your SQL servers	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Advanced data security should be enabled on SQL Managed Instance	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Monitor missing Endpoint Protection in Azure Security Center	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Activity log should be retained for at least one year	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Management ports of virtual machines should be protected with just-in-time network access control	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Service Fabric clusters should only use Azure Active Directory for client authentication	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: API App should only be accessible over HTTPS	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Audit Windows machines on which Windows Defender Exploit Guard is not enabled	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Include Arc-connected servers when evaluating policy: Audit Windows machines on which Windows Defender Exploit Guard is not enabled	By selecting 'true', you agree to be charged monthly per Arc connected machine
New Zealand ISM Restricted	Policy Assignment	Compliance state to report for Windows machines on which Windows Defender Exploit Guard is not available	Windows Defender Exploit Guard is only available starting with Windows 10/Windows Server with update 1709. Setting this value to 'Non-Compliant' shows machines with older versions on which Windows Defender Exploit Guard is not available (such as Windows Server 2012 R2) as non-compliant. Setting this value to 'Compliant' shows these machines as compliant.
New Zealand ISM Restricted	Policy Assignment	Effect for policy: System updates on virtual machine scale sets should be installed	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Remote debugging should be turned off for Web Applications	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Vulnerabilities in security configuration on your machines should be remediated	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: MFA should be enabled on accounts with read permissions on your subscription	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Vulnerabilities in container security configurations should be remediated	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Remote debugging should be turned off for API Apps	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Audit Linux machines that allow remote connections from accounts without passwords	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Include Arc-connected servers when evaluating policy: Audit Linux machines that allow remote connections from accounts without passwords	By selecting 'true', you agree to be charged monthly per Arc connected machine
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Deprecated accounts with owner permissions should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Vulnerability assessment should be enabled on your SQL servers	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Latest TLS version should be used in your Web App	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Windows machines should meet requirements for 'Security Settings - Account Policies'	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Enforce password history for Windows VM local accounts	Specifies limits on password reuse - how many times a new password must be created for a user account before the password can be repeated
New Zealand ISM Restricted	Policy Assignment	Include Arc-connected servers when evaluating policy: Windows machines should meet requirements for 'Security Settings - Account Policies'	By selecting 'true', you agree to be charged monthly per Arc connected machine
New Zealand ISM Restricted	Policy Assignment	Maximum password age for Windows VM local accounts	Specifies the maximum number of days that may elapse before a user account password must be changed; the format of the value is two integers separated by a comma, denoting an inclusive range

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
New Zealand ISM Restricted	Policy Assignment	Minimum password age for Windows VM local accounts	Specifies the minimum number of days that must elapse before a user account password can be changed
New Zealand ISM Restricted	Policy Assignment	Minimum password length for Windows VM local accounts	Specifies the minimum number of characters that a user account password may contain
New Zealand ISM Restricted	Policy Assignment	Password must meet complexity requirements for Windows VM local accounts	Specifies whether a user account password must be complex; if required, a complex password must not contain part of the user's account name or full name; be at least 6 characters long; contain a mix of uppercase, lowercase, number, and non-alphabetic characters
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Internet-facing virtual machines should be protected with network security groups	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Audit Linux machines that have accounts without passwords	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Include Arc-connected servers when evaluating policy: Audit Linux machines that have accounts without passwords	By selecting 'true', you agree to be charged monthly per Arc connected machine
New Zealand ISM Restricted	Policy Assignment	Effect for policy: External accounts with owner permissions should be removed from your subscription	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Latest TLS version should be used in your Function App	For more information about effects, visit https://aka.ms/policyeffects
New Zealand ISM Restricted	Policy Assignment	Effect for policy: [Preview]: All Internet traffic should be routed via your deployed Azure Firewall	For more information about effects, visit https://aka.ms/policyeffects

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
New Zealand ISM Restricted	Policy Assignment	Effect for policy: Vulnerabilities on your SQL databases should be remediated	For more information about effects, visit https://aka.ms/policyeffects

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

NIST SP 800-53 R4 blueprint sample

5/3/2021 • 8 minutes to read • [Edit Online](#)

The NIST SP 800-53 R4 blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific NIST SP 800-53 R4 controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement NIST SP 800-53 R4 controls.

Control mapping

The [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **compliance domains** and **controls** in NIST SP 800-53 R4. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints NIST SP 800-53 R4 blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **NIST SP 800-53 R4** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the NIST SP 800-53 R4 blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with NIST SP 800-53 controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint

sample and then select it.

3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the NIST SP 800-53 R4 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - Managed Identity

Leave the default *system assigned* managed identity option.
 - Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are **priced by product**. Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit NIST SP 800-53 R4 controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Log Analytics workspace ID that VMs should be configured for	This is the ID (GUID) of the Log Analytics workspace that the VMs should be configured for.
[Preview]: Audit NIST SP 800-53 R4 controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor diagnostic logs schemas .
[Preview]: Audit NIST SP 800-53 R4 controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be excluded from Windows VM Administrators group	A semicolon-separated list of members that should be excluded in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: Audit NIST SP 800-53 R4 controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be included in Windows VM Administrators group	A semicolon-separated list of members that should be included in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Linux VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Log Analytics workspace for Linux VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Windows VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Log Analytics workspace for Windows VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Advanced Threat Protection on Storage Accounts	Policy assignment	Effect	Information about policy effects can be found at Understand Azure Policy Effects
Deploy Auditing on SQL servers	Policy assignment	The value in days of the retention period (0 indicates unlimited retention)	Retention days (optional, 180 days if unspecified)
Deploy Auditing on SQL servers	Policy assignment	Resource group name for storage account for SQL server auditing	Auditing writes database events to an audit log in your Azure Storage account (a storage account will be created in each region where a SQL Server is created that will be shared by all servers in that region). Important - for proper operation of Auditing do not delete or rename the resource group or the storage accounts.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Storage account prefix for network security group diagnostics	This prefix will be combined with the network security group location to form the created storage account name.

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Deploy diagnostic settings for Network Security Groups	Policy assignment	Resource group name for storage account for network security group diagnostics (must exist)	The resource group that the storage account will be created in. This resource group must already exist.

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

NIST SP 800-171 R2 blueprint sample

5/3/2021 • 6 minutes to read • [Edit Online](#)

The NIST SP 800-171 R2 blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific NIST SP 800-171 R2 requirements or controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement NIST SP 800-171 R2 requirements or controls.

Control mapping

The [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **compliance domains** and **requirements** in NIST SP 800-171 R2. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints NIST SP 800-171 R2 blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **NIST SP 800-171 R2** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the NIST SP 800-171 R2 blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that are included in the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with NIST SP 800-171 requirements.

1. Select **All services** in the left pane. Search for and select **Blueprints**.

2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the NIST SP 800-171 R2 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:

- Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.

- Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *system assigned* managed identity option.

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: NIST SP 800-171 R2	Policy assignment	List of users that should be excluded from Windows VM Administrators group	A semicolon-separated list of members that should be excluded in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: NIST SP 800-171 R2	Policy assignment	List of users that should be included in Windows VM Administrators group	A semicolon-separated list of members that should be included in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: NIST SP 800-171 R2	Policy assignment	List of regions where Network Watcher should be enabled	A semicolon-separated list of regions. To see a complete list of regions use Get-AzLocation. Ex: East US; East US2
[Preview]: NIST SP 800-171 R2	Policy assignment	Log Analytics workspace ID that VMs should be configured for	This is the ID (GUID) of the Log Analytics workspace that the VMs should be configured for.
[Preview]: NIST SP 800-171 R2	Policy assignment	Optional: List of Windows VM images that support Log Analytics agent to add to audit scope	A semicolon-separated list of images
[Preview]: NIST SP 800-171 R2	Policy assignment	Optional: List of Linux VM images that support Log Analytics agent to add to audit scope	A semicolon-separated list of images
[Preview]: NIST SP 800-171 R2	Policy assignment	Latest PHP version	Latest supported PHP version for App Services
[Preview]: NIST SP 800-171 R2	Policy assignment	Latest Java version	Latest supported Java version for App Services
[Preview]: NIST SP 800-171 R2	Policy assignment	Latest Windows Python version	Latest supported Python version for App Services
[Preview]: NIST SP 800-171 R2	Policy assignment	Latest Linux Python version	Latest supported Python version for App Services
[Preview]: NIST SP 800-171 R2	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor diagnostic logs schemas .

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: NIST SP 800-171 R2	Policy assignment	Minimum TLS version for Windows Web servers	The minimum TLS protocol version that should be enabled on Windows web servers.

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the PCI-DSS v3.2.1 blueprint sample

5/3/2021 • 2 minutes to read • [Edit Online](#)

The PCI-DSS v3.2.1 blueprint sample is a set of policies which aides in achieving PCI-DSS v3.2.1 compliance. This blueprint helps customers govern cloud-based environments with PCI-DSS workloads. The PCI-DSS blueprint deploys a core set of policies for any Azure-deployed architecture requiring this accreditation.

Control mapping

The control mapping section provides details on policies included within this initiative and how these policies help meet various controls defined by PCI-DSS v3.2.1. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policies.

After assigning this blueprint, view your Azure environments level of compliance in the Azure Policy Compliance Dashboard.

Next steps

You've reviewed the overview of the PCI-DSS v3.2.1 blueprint sample. Next, visit the following articles to learn about the control mapping and how to deploy this sample:

[PCI-DSS v3.2.1 blueprint - Control mapping](#) [PCI-DSS v3.2.1 blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Control mapping of the PCI-DSS v3.2.1 blueprint sample

5/3/2021 • 7 minutes to read • [Edit Online](#)

The following article details how the Azure Blueprints PCI-DSS v3.2.1 blueprint sample maps to the PCI-DSS v3.2.1 controls. For more information about the controls, see [PCI-DSS v3.2.1](#).

The following mappings are to the **PCI-DSS v3.2.1:2018** controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an [Azure Policy](#) initiative. To review the complete initiative, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **PCI v3.2.1:2018** built-in policy initiative.

IMPORTANT

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy definitions for this compliance blueprint sample may change over time. To view the change history, see the [GitHub Commit History](#).

1.3.2 and 1.3.4 Boundary Protection

This blueprint helps you manage and control networks by assigning [Azure Policy](#) definitions that monitors network security groups with permissive rules. Rules that are too permissive may allow unintended network access and should be reviewed. This blueprint assigns one Azure Policy definitions that monitor unprotected endpoints, applications, and storage accounts. Endpoints and applications that aren't protected by a firewall, and storage accounts with unrestricted access can allow unintended access to information contained within the information system.

- Audit unrestricted network access to storage accounts
- Access through Internet facing endpoint should be restricted

3.4.a, 4.1, 4.1.g, 4.1.h and 6.5.3 Cryptographic Protection

This blueprint helps you enforce your policy with the use of cryptograph controls by assigning [Azure Policy](#) definitions which enforce specific cryptograph controls and audit use of weak cryptographic settings. Understanding where your Azure resources may have non-optimal cryptographic configurations can help you take corrective actions to ensure resources are configured in accordance with your information security policy. Specifically, the policies assigned by this blueprint require transparent data encryption on SQL databases; audit missing encryption on storage accounts, and automation account variables. There are also policies which address audit insecure connections to storage accounts, Function Apps, WebApp, API Apps, and Redis Cache, and audit unencrypted Service Fabric communication.

- Function App should only be accessible over HTTPS
- Web Application should only be accessible over HTTPS
- API App should only be accessible over HTTPS
- Transparent Data Encryption on SQL databases should be enabled

- Disk encryption should be applied on virtual machines
- Automation account variables should be encrypted
- Only secure connections to your Redis Cache should be enabled
- Secure transfer to storage accounts should be enabled
- Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign
- Transparent Data Encryption on SQL databases should be enabled
- Deploy SQL DB transparent data encryption

5.1, 6.2, 6.6 and 11.2.1 Vulnerability Scanning and System Updates

This blueprint helps you manage information system vulnerabilities by assigning [Azure Policy](#) definitions that monitor missing system updates, operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources.

- Monitor missing Endpoint Protection in Azure Security Center
- Deploy default Microsoft IaaS Antimalware extension for Windows Server
- Deploy Threat Detection on SQL Servers
- System updates should be installed on your machines
- Vulnerabilities in security configuration on your machines should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities should be remediated by a Vulnerability Assessment solution

7.1.1, 7.1.2 and 7.1.3 Separation of Duties

Having only one Azure subscription owner doesn't allow for administrative redundancy. Conversely, having too many Azure subscription owners can increase the potential for a breach via a compromised owner account. This blueprint helps you maintain an appropriate number of Azure subscription owners by assigning [Azure Policy](#) definitions which audit the number of owners for Azure subscriptions. Managing subscription owner permissions can help you implement appropriate separation of duties.

- There should be more than one owner assigned to your subscription
- A maximum of 3 owners should be designated for your subscription

3.2, 7.2.1, 8.3.1.a and 8.3.1.b Management of Privileged Access Rights

This blueprint helps you restrict and control privileged access rights by assigning [Azure Policy](#) definitions to audit external accounts with owner, write and/or read permissions and employee accounts with owner and/or write permissions that don't have multi-factor authentication enabled. Azure role-based access control (Azure RBAC) helps to manage who has access to Azure resources. Understanding where custom Azure RBAC rules are implemented can help you verify need and proper implementation, as custom Azure RBAC rules are error prone. This blueprint also assigns [Azure Policy](#) definitions to audit use of Azure Active Directory authentication for SQL Servers. Using Azure Active Directory authentication simplifies permission management and centralizes identity management of database users and other Microsoft services.

- External accounts with owner permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription
- External accounts with read permissions should be removed from your subscription
- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled accounts with write permissions on your subscription
- MFA should be enabled on accounts with read permissions on your subscription
- An Azure Active Directory administrator should be provisioned for SQL servers

- Audit usage of custom RBAC rules

8.1.2 and 8.1.5 Least Privilege and Review of User Access Rights

Azure role-based access control (Azure RBAC) helps you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint assigns [Azure Policy](#) definitions to audit accounts that should be prioritized for review, including deprecated accounts and external accounts with elevated permissions.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription
- External accounts with owner permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription
- External accounts with read permissions should be removed from your subscription

8.1.3 Removal or Adjustment of Access Rights

Azure role-based access control (Azure RBAC) helps you manage who has access to resources in Azure. Using Azure Active Directory and Azure RBAC, you can update user roles to reflect organizational changes. When needed, accounts can be blocked from signing in (or removed), which immediately removes access rights to Azure resources. This blueprint assigns [Azure Policy](#) definitions to audit deprecated account that should be considered for removal.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription

8.2.3.a,b, 8.2.4.a,b and 8.2.5 Password-based Authentication

This blueprint helps you enforce strong passwords by assigning [Azure Policy](#) definitions that audit Windows VMs that don't enforce minimum strength and other password requirements. Awareness of VMs in violation of the password strength policy helps you take corrective actions to ensure passwords for all VM user accounts are compliant with policy.

- [Preview]: Audit Windows VMs that do not have a maximum password age of 70 days
- [Preview]: Deploy requirements to audit Windows VMs that do not have a maximum password age of 70 days
- [Preview]: Audit Windows VMs that do not restrict the minimum password length to 14 characters
- [Preview]: Deploy requirements to audit Windows VMs that do not restrict the minimum password length to 14 characters
- [Preview]: Audit Windows VMs that allow re-use of the previous 24 passwords
- [Preview]: Deploy requirements to audit Windows VMs that allow re-use of the previous 24 passwords

10.3 and 10.5.4 Audit Generation

This blueprint helps you ensure system events are logged by assigning [Azure Policy](#) definitions that audit log settings on Azure resources. Diagnostic logs provide insight into operations that were performed within Azure resources. Azure logs rely on synchronized internal clocks to create a time-correlated record of events across resources.

- Auditing should be enabled on advanced data security settings on SQL Server
- Audit diagnostic setting
- Audit SQL server level Auditing settings
- Deploy Auditing on SQL servers

- Storage accounts should be migrated to new Azure Resource Manager resources
- Virtual machines should be migrated to new Azure Resource Manager resources

12.3.6 and 12.3.7 Information Security

This blueprint helps you manage and control your network by assigning [Azure Policy](#) definitions that audit the acceptable network locations and the approved company products allowed for the environment. These are customizable by each company through the policy parameters within each of these policies.

- Allowed locations
- Allowed locations for resource groups

Next steps

Now that you've reviewed the control mapping of the PCI-DSS v3.2.1 blueprint, visit the following articles to learn about the overview and how to deploy this sample:

[PCI-DSS v3.2.1 blueprint - Overview](#) [PCI-DSS v3.2.1 blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the PCI-DSS v3.2.1 blueprint sample

5/2/2021 • 4 minutes to read • [Edit Online](#)

To deploy the Azure Blueprints PCI-DSS v3.2.1 blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **PCI-DSS v3.2.1** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the PCI-DSS v3.2.1 blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from the PCI-DSS v3.2.1 standard.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the PCI-DSS v3.2.1 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each

deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:

- Basics
 - **Subscriptions:** Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name:** The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location:** Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version:** Pick a **Published** version of your copy of the blueprint sample.

- Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *system assigned* managed identity option.

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
PCI v3.2.1:2018	Policy Assignment	List of Resource Types	Audit diagnostic setting for selected resource types. Default value is all resources are selected

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Allowed locations	Policy Assignment	List Of Allowed Locations	List of data center locations allowed for any resource to be deployed into. This list is customizable to the desired Azure locations globally. Select locations you wish to allow.
Allowed Locations for resource groups	Policy Assignment	Allowed Location	This policy enables you to restrict the locations your organization can create resource groups in. Use to enforce your geo-compliance requirements.
Deploy Auditing on SQL servers	Policy Assignment	Retention days	Data retention in number of days. Default value is 180 but PCI requires 365.
Deploy Auditing on SQL servers	Policy Assignment	Resource group name for storage account	Auditing writes database events to an audit log in your Azure Storage account (a storage account will be created in each region where a SQL Server is created that will be shared by all servers in that region).

Next steps

Now that you've reviewed the steps to deploy the PCI-DSS v3.2.1 blueprint sample, visit the following articles to learn about the overview and control mapping:

[PCI-DSS v3.2.1 blueprint - Overview](#) [PCI-DSS v3.2.1 blueprint - Control mapping](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the SWIFT CSP-CSCF v2020 blueprint sample

5/3/2021 • 2 minutes to read • [Edit Online](#)

The SWIFT CSP-CSCF v2020 blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific SWIFT CSP controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement SWIFT CSP controls.

Control mapping

The control mapping section provides details on policies included within this blueprint and how these policies address various controls in the latest SWIFT CSP-CSCF. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policies. For more information, see [Azure Policy](#).

Next steps

You've reviewed the overview and of the SWIFT CSP-CSCF v2020 blueprint sample. Next, visit the following articles to learn about the control mapping and how to deploy this sample:

[SWIFT CSP-CSCF v2020 blueprint - Control mapping](#) [SWIFT CSP-CSCF v2020 blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Control mapping of the SWIFT CSP-CSCF v2020 blueprint sample

5/3/2021 • 19 minutes to read • [Edit Online](#)

The following article details how the Azure Blueprints SWIFT CSP-CSCF v2020 blueprint sample maps to the SWIFT CSP-CSCF v2020 controls. For more information about the controls, see [SWIFT CSP-CSCF v2020](#).

The following mappings are to the **SWIFT CSP-CSCF v2020** controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an [Azure Policy](#) initiative. To review the complete initiative, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **[Preview]: Audit SWIFT CSP-CSCF v2020 controls and deploy specific VM Extensions to support audit requirements** built-in policy initiative.

IMPORTANT

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy definitions for this compliance blueprint sample may change over time. To view the change history, see the [GitHub Commit History](#).

1.2 and 5.1 Account Management

This blueprint helps you review accounts that may not comply with your organization's account management requirements. This blueprint assigns [Azure Policy](#) definitions that audit external accounts with read, write and owner permissions on a subscription and deprecated accounts. By reviewing the accounts audited by these policies, you can take appropriate action to ensure account management requirements are met.

- Deprecated accounts should be removed from your subscription
- Deprecated accounts with owner permissions should be removed from your subscription
- External accounts with owner permissions should be removed from your subscription
- External accounts with read permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription

2.6, 5.1, 6.4, and 6.5A Account Management | Role-Based Schemes

[Azure role-based access control](#) (Azure RBAC) to help you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint also assigns [Azure Policy](#) definitions to audit use of Azure Active Directory authentication for SQL Servers and Service Fabric. Using Azure Active Directory authentication enables simplified permission management and centralized identity management of database users and other Microsoft services. Additionally, this blueprint assigns an Azure Policy definition to audit the use of custom Azure RBAC rules. Understanding where custom Azure RBAC rules are implement can help you verify need and proper implementation, as custom Azure RBAC rules are error prone.

- An Azure Active Directory administrator should be provisioned for SQL servers
- Audit VMs that do not use managed disks

- Service Fabric clusters should only use Azure Active Directory for client authentication

2.9A Account Management | Account Monitoring / Atypical Usage

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. All JIT requests to access virtual machines are logged in the Activity Log allowing you to monitor for atypical usage. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but have not yet been configured.

- Management ports of virtual machines should be protected with just-in-time network access control

1.3, 5.1, and 6.4 Separation of Duties

Having only one Azure subscription owner doesn't allow for administrative redundancy. Conversely, having too many Azure subscription owners can increase the potential for a breach via a compromised owner account. This blueprint helps you maintain an appropriate number of Azure subscription owners by assigning [Azure Policy](#) definitions that audit the number of owners for Azure subscriptions. This blueprint also assigns Azure Policy definitions that help you control membership of the Administrators group on Windows virtual machines. Managing subscription owner and virtual machine administrator permissions can help you implement appropriate separation of duties.

- A maximum of 3 owners should be designated for your subscription
- Show audit results from Windows VMs in which the Administrators group does not contain all of the specified members
- Deploy prerequisites to audit Windows VMs in which the Administrators group does not contain all of the specified members
- There should be more than one owner assigned to your subscription

1.3, 5.1, and 6.4 Least Privilege | Review of User Privileges

[Azure role-based access control \(Azure RBAC\)](#) helps you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint assigns [Azure Policy](#) definitions to audit accounts that should be prioritized for review. Reviewing these account indicators can help you ensure least privilege controls are implemented.

- A maximum of 3 owners should be designated for your subscription
- Show audit results from Windows VMs that are not joined to the specified domain
- Deploy prerequisites to audit Windows VMs that are not joined to the specified domain
- There should be more than one owner assigned to your subscription

2.2 and 2.7 Security Attributes

The data discovery and classification capability of advanced data security for Azure SQL Database provides capabilities for discovering, classifying, labeling, and protecting the sensitive data in your databases. It can be used to provide visibility into your database classification state, and to track the access to sensitive data within the database and beyond its borders. Advanced data security can help you ensure information as associated with the appropriate security attributes for your organization. This blueprint assigns [Azure Policy](#) definitions to monitor and enforce use of advanced data security on SQL server.

- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers

2.2, 2.7, 4.1, and 6.1 Remote Access | Automated Monitoring / Control

This blueprint helps you monitor and control remote access by assigning [Azure Policy](#) definitions to monitors that remote debugging for Azure App Service application is turned off and policy definitions that audit Linux virtual machines that allow remote connections from accounts without passwords. This blueprint also assigns an Azure Policy definition that helps you monitor unrestricted access to storage accounts. Monitoring these indicators can help you ensure remote access methods comply with your security policy.

- Show audit results from Linux VMs that allow remote connections from accounts without passwords
- Deploy prerequisites to audit Linux VMs that allow remote connections from accounts without passwords
- Storage accounts should restrict network access
- Remote debugging should be turned off for API App
- Remote debugging should be turned off for Function App
- Remote debugging should be turned off for Web Application

1.3 and 6.4 Content of Audit Records | Centralized Management of Planned Audit Record Content

Log data collected by Azure Monitor is stored in a Log Analytics workspace enabling centralized configuration and management. This blueprint helps you ensure events are logged by assigning [Azure Policy](#) definitions that audit and enforce deployment of the Log Analytics agent on Azure virtual machines.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Deploy Log Analytics Agent for Linux VMs
- Deploy Log Analytics Agent for Windows VMs

2.2, 2.7, and 6.4 Response to Audit Processing Failures

This blueprint assigns [Azure Policy](#) definitions that monitor audit and event logging configurations. Monitoring these configurations can provide an indicator of an audit system failure or misconfiguration and help you take corrective action.

- Advanced data security should be enabled on your SQL servers
- Audit diagnostic setting
- Auditing on SQL server should be enabled

1.3 and 6.4 Audit Review, Analysis, and Reporting | Central Review and Analysis

Log data collected by Azure Monitor is stored in a Log Analytics workspace enabling centralized reporting and analysis. This blueprint helps you ensure events are logged by assigning [Azure Policy](#) definitions that audit and enforce deployment of the Log Analytics agent on Azure virtual machines.

- [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Deploy Log Analytics Agent for Linux VMs
- Deploy Log Analytics Agent for Windows VMs

1.3, 2.2, 2.7, 6.4, and 6.5A Audit Generation

This blueprint helps you ensure system events are logged by assigning [Azure Policy](#) definitions that audit log settings on Azure resources. These policy definitions audit and enforce deployment of the Log Analytics agent on Azure virtual machines and configuration of audit settings for other Azure resource types. These policy definitions also audit configuration of diagnostic logs to provide insight into operations that are performed

within Azure resources. Additionally, auditing and Advanced Data Security are configured on SQL servers.

- Audit Log Analytics Agent Deployment - VM Image (OS) unlisted
- Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)
- Deploy Log Analytics Agent for Linux VMs
- Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)
- Deploy Log Analytics Agent for Windows VMs
- Audit diagnostic setting
- Audit SQL server level Auditing settings
- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Auditing on SQL server should be enabled
- Deploy Diagnostic Settings for Network Security Groups

1.1 Least Functionality | Prevent Program Execution

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application filtering solution that can block or prevent specific software from running on your virtual machines. Application control can run in an enforcement mode that prohibits non-approved application from running. This blueprint assigns an Azure Policy definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive application controls for defining safe applications should be enabled on your machines

1.1 Least Functionality | Authorized Software / Whitelisting

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application filtering solution that can block or prevent specific software from running on your virtual machines. Application control helps you create approved application lists for your virtual machines. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive application controls for defining safe applications should be enabled on your machines

1.1 User-Installed Software

Adaptive application control in Azure Security Center is an intelligent, automated end-to-end application filtering solution that can block or prevent specific software from running on your virtual machines. Application control can help you enforce and monitor compliance with software restriction policies. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines where an application allowlist is recommended but has not yet been configured.

- Adaptive application controls for defining safe applications should be enabled on your machines
- Virtual machines should be migrated to new Azure Resource Manager resources

4.2 Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts

This blueprint helps you restrict and control privileged access by assigning [Azure Policy](#) definitions to audit accounts with owner and/or write permissions that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled on accounts with write permissions on your subscription

4.2 Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

This blueprint helps you restrict and control access by assigning an [Azure Policy](#) definition to audit accounts with read permissions that don't have multi-factor authentication enabled. Multi-factor authentication helps keep accounts secure even if one piece of authentication information is compromised. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be compromised.

- MFA should be enabled on accounts with read permissions on your subscription

2.3 and 4.1 Authenticator Management

This blueprint assigns [Azure Policy](#) definitions that audit Linux virtual machines that allow remote connections from accounts without passwords and/or have incorrect permissions set on the passwd file. This blueprint also assigns policy definitions that audit the configuration of the password encryption type for Windows virtual machines. Monitoring these indicators helps you ensure that system authenticators comply with your organization's identification and authentication policy.

- Show audit results from Linux VMs that do not have the passwd file permissions set to 0644
- Deploy requirements to audit Linux VMs that do not have the passwd file permissions set to 0644
- Show audit results from Linux VMs that have accounts without passwords
- Deploy requirements to audit Linux VMs that have accounts without passwords
- Show audit results from Windows VMs that do not store passwords using reversible encryption
- Deploy requirements to audit Windows VMs that do not store passwords using reversible encryption

2.3 and 4.1 Authenticator Management | Password-Based Authentication

This blueprint helps you enforce strong passwords by assigning [Azure Policy](#) definitions that audit Windows virtual machines that don't enforce minimum strength and other password requirements. Awareness of virtual machines in violation of the password strength policy helps you take corrective actions to ensure passwords for all virtual machine user accounts comply with your organization's password policy.

- Show audit results from Windows VMs that allow re-use of the previous 24 passwords
- Show audit results from Windows VMs that do not have a maximum password age of 70 days
- Show audit results from Windows VMs that do not have a minimum password age of 1 day
- Show audit results from Windows VMs that do not have the password complexity setting enabled
- Show audit results from Windows VMs that do not restrict the minimum password length to 14 characters
- Show audit results from Windows VMs that do not store passwords using reversible encryption
- Deploy prerequisites to audit Windows VMs that allow re-use of the previous 24 passwords
- Deploy prerequisites to audit Windows VMs that do not have a maximum password age of 70 days
- Deploy prerequisites to audit Windows VMs that do not have a minimum password age of 1 day
- Deploy prerequisites to audit Windows VMs that do not have the password complexity setting enabled
- Deploy prerequisites to audit Windows VMs that do not restrict the minimum password length to 14 characters
- Deploy prerequisites to audit Windows VMs that do not store passwords using reversible encryption

2.2 and 2.7 Vulnerability Scanning

This blueprint helps you manage information system vulnerabilities by assigning [Azure Policy](#) definitions that monitor operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources. This blueprint also assigns policy definitions that audit and enforce Advanced Data Security on SQL servers. Advanced data security included vulnerability assessment and advanced threat protection capabilities to help you understand vulnerabilities in your deployed resources.

- Advanced data security should be enabled on your SQL servers
- Auditing on SQL server should be enabled
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities on your SQL databases should be remediated
- Vulnerabilities in security configuration on your machines should be remediated

1.3 Denial of Service Protection

Azure's distributed denial of service (DDoS) Standard tier provides additional features and mitigation capabilities over the basic service tier. These additional features include Azure Monitor integration and the ability to review post-attack mitigation reports. This blueprint assigns an [Azure Policy](#) definition that audits if the DDoS Standard tier is enabled. Understanding the capability difference between the service tiers can help you select the best solution to address denial of service protections for your Azure environment.

- Azure DDoS Protection Standard should be enabled

1.1 and 6.1 Boundary Protection

This blueprint helps you manage and control the system boundary by assigning an [Azure Policy](#) definition that monitors for network security group hardening recommendations in Azure Security Center. Azure Security Center analyzes traffic patterns of Internet facing virtual machines and provides network security group rule recommendations to reduce the potential attack surface. Additionally, this blueprint also assigns policy definitions that monitor unprotected endpoints, applications, and storage accounts. Endpoints and applications that aren't protected by a firewall, and storage accounts with unrestricted access can allow unintended access to information contained within the information system.

- Adaptive Network Hardening recommendations should be applied on internet facing virtual machines
- Access through Internet facing endpoint should be restricted
- Audit unrestricted network access to storage accounts

2.9A Boundary Protection | Access Points

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT virtual machine access helps you limit the number of external connections to your resources in Azure. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but have not yet been configured.

- Management ports of virtual machines should be protected with just-in-time network access control

2.9A Boundary Protection | External Telecommunications Services

Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. JIT virtual machine access helps you manage exceptions to your traffic flow policy by facilitating the access request and approval

processes. This blueprint assigns an [Azure Policy](#) definition that helps you monitor virtual machines that can support just-in-time access but have not yet been configured.

- Management ports of virtual machines should be protected with just-in-time network access control

2.1, 2.4, 2.4A, 2.5A, and 2.6 Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection

This blueprint helps you protect the confidentiality and integrity of transmitted information by assigning [Azure Policy](#) definitions that help you monitor cryptographic mechanism implemented for communications protocols. Ensuring communications are properly encrypted can help you meet your organization's requirements or protecting information from unauthorized disclosure and modification.

- API App should only be accessible over HTTPS
- Show audit results from Windows web servers that are not using secure communication protocols
- Deploy prerequisites to audit Windows web servers that are not using secure communication protocols
- Function App should only be accessible over HTTPS
- Only secure connections to your Redis Cache should be enabled
- Secure transfer to storage accounts should be enabled
- Web Application should only be accessible over HTTPS

2.2, 2.3, 2.5, 4.1, and 2.7 Protection of Information at Rest | Cryptographic Protection

This blueprint helps you enforce your policy on the use of cryptograph controls to protect information at rest by assigning [Azure Policy](#) definitions that enforce specific cryptograph controls and audit use of weak cryptographic settings. Understanding where your Azure resources may have non-optimal cryptographic configurations can help you take corrective actions to ensure resources are configured in accordance with your information security policy. Specifically, the policy definitions assigned by this blueprint require encryption for data lake storage accounts; require transparent data encryption on SQL databases; and audit missing encryption on SQL databases, virtual machine disks, and automation account variables.

- Advanced data security should be enabled on your SQL servers
- Deploy Advanced Data Security on SQL servers
- Deploy SQL DB transparent data encryption
- Transparent Data Encryption on SQL databases should be enabled

1.3, 2.2, and 2.7 Flaw Remediation

This blueprint helps you manage information system flaws by assigning [Azure Policy](#) definitions that monitor missing system updates, operating system vulnerabilities, SQL vulnerabilities, and virtual machine vulnerabilities in Azure Security Center. Azure Security Center provides reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources. This blueprint also assigns a policy definition that ensures patching of the operating system for virtual machine scale sets.

- Require automatic OS image patching on Virtual Machine Scale Sets
- System updates on virtual machine scale sets should be installed
- System updates should be installed on your virtual machines
- Audit Dependency agent deployment in virtual machine scale sets - VM Image (OS) unlisted
- Automation account variables should be encrypted
- Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
- Vulnerabilities in security configuration on your virtual machines should be remediated

- Vulnerabilities on your SQL databases should be remediated

6.1 Malicious Code Protection

This blueprint helps you manage endpoint protection, including malicious code protection, by assigning [Azure Policy](#) definitions that monitor for missing endpoint protection on virtual machines in Azure Security Center and enforce the Microsoft antimalware solution on Windows virtual machines.

- Deploy default Microsoft IaaS Antimalware extension for Windows Server
- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center
- Storage accounts should be migrated to new Azure Resource Manager resources

6.1 Malicious Code Protection | Central Management

This blueprint helps you manage endpoint protection, including malicious code protection, by assigning [Azure Policy](#) definitions that monitor for missing endpoint protection on virtual machines in Azure Security Center. Azure Security Center provides centralized management and reporting capabilities that enable you to have real-time insight into the security state of deployed Azure resources.

- Endpoint protection solution should be installed on virtual machine scale sets
- Monitor missing Endpoint Protection in Azure Security Center

1.1, 1.3, 2.2, 2.7, 2.8, and 6.4 Information System Monitoring

This blueprint helps you monitor your system by auditing and enforcing logging and data security across Azure resources. Specifically, the policies assigned audit and enforce deployment of the Log Analytics agent, and enhanced security settings for SQL databases, storage accounts and network resources. These capabilities can help you detect anomalous behavior and indicators of attacks so you can take appropriate action.

- Show audit results from Windows VMs on which the Log Analytics agent is not connected as expected
- Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)
- Deploy Log Analytics Agent for Linux VMs
- Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)
- Deploy Log Analytics Agent for Windows VMs
- Advanced data security should be enabled on your SQL servers
- Advanced data security settings for SQL server should contain an email address to receive security alerts
- Diagnostic logs in Azure Stream Analytics should be enabled
- Deploy Advanced Data Security on SQL servers
- Deploy Auditing on SQL servers
- Deploy network watcher when virtual networks are created
- Deploy Threat Detection on SQL servers

2.2 and 2.8 Information System Monitoring | Analyze Traffic / Covert Exfiltration

Advanced Threat Protection for Azure Storage detects unusual and potentially harmful attempts to access or exploit storage accounts. Protection alerts include anomalous access patterns, anomalous extracts/uploads, and suspicious storage activity. These indicators can help you detect covert exfiltration of information.

- Deploy Threat Detection on SQL servers

NOTE

Availability of specific Azure Policy definitions may vary in Azure Government and other national clouds.

Next steps

Now that you've reviewed the control mapping of the SWIFT CSP-CSCF v2020 blueprint, visit the following articles to learn about the blueprint and how to deploy this sample:

[SWIFT CSP-CSCF v2020 blueprint - Overview](#) [SWIFT CSP-CSCF v2020 blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the SWIFT CSP-CSCF v2020 blueprint sample

5/3/2021 • 7 minutes to read • [Edit Online](#)

To deploy the Azure Blueprints SWIFT CSP-CSCF v2020 blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** and search for and select **Policy** in the left pane. On the **Policy** page, select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **SWIFT CSP-CSCF v2020** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the SWIFT CSP-CSCF v2020 blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with SWIFT CSP-CSCF v2020 controls.

1. Select **All services** and search for and select **Policy** in the left pane. On the **Policy** page, select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the SWIFT CSP- CSCF v2020 blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** and search for and select **Policy** in the left pane. On the **Policy** page, select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - **Basics**
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - **Lock Assignment**

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - **Managed Identity**

Leave the default *system assigned* managed identity option.
 - **Artifact parameters**

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are **priced by product**. Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
[Preview]: Audit SWIFT CSP-CSCF v2020 controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of resource types that should have diagnostic logs enabled	List of resource types to audit if diagnostic log setting is not enabled. Acceptable values can be found at Azure Monitor resource logs categories .
[Preview]: Audit SWIFT CSP-CSCF v2020 controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Connected workspace IDs	A semicolon-separated list of the workspace IDs that the Log Analytics agent should be connected to
[Preview]: Audit SWIFT CSP-CSCF v2020 controls and deploy specific VM Extensions to support audit requirements	Policy assignment	List of users that should be included in Windows VM Administrators group	A semicolon-separated list of members that should be included in the Administrators local group. Ex: Administrator; myUser1; myUser2
[Preview]: Audit SWIFT CSP-CSCF v2020 controls and deploy specific VM Extensions to support audit requirements	Policy assignment	Domain Name (FQDN)	The fully qualified domain name (FQDN) that the Windows VMs should be joined to
Deploy Log Analytics Agent for Linux VMs	Policy assignment	Log Analytics workspace for Linux VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Log Analytics workspace for Windows VM Scale Sets (VMSS)	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Deploy Log Analytics Agent for Windows VMs	Policy assignment	Log Analytics workspace for Windows VMs	If this workspace is outside of the scope of the assignment you must manually grant 'Log Analytics Contributor' permissions (or similar) to the policy assignment's principal ID.
Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope	An empty array may be used to indicate no optional parameters: []
Deploy Advanced Threat Protection on Storage Accounts	Policy assignment	Effect	Information about policy effects can be found at Understand Azure Policy Effects
Deploy Auditing on SQL servers	Policy assignment	The value in days of the retention period (0 indicates unlimited retention)	Retention days (optional, 180 days if unspecified)
Deploy Auditing on SQL servers	Policy assignment	Resource group name for storage account for SQL server auditing	Auditing writes database events to an audit log in your Azure Storage account (a storage account will be created in each region where a SQL Server is created that will be shared by all servers in that region). Important - for proper operation of Auditing do not delete or rename the resource group or the storage accounts.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Storage account prefix for network security group diagnostics	This prefix will be combined with the network security group location to form the created storage account name.
Deploy diagnostic settings for Network Security Groups	Policy assignment	Resource group name for storage account for network security group diagnostics (must exist)	The resource group that the storage account will be created in. This resource group must already exist.

Next steps

Now that you've reviewed the steps to deploy the SWIFT CSP-CSCF v2020 blueprint sample, visit the following articles to learn about the blueprint and control mapping:

[SWIFT CSP-CSCF v2020 blueprint - Overview](#) [SWIFT CSP-CSCF v2020 blueprint - Control mapping](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).

- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

UK OFFICIAL and UK NHS blueprint sample

5/4/2021 • 5 minutes to read • [Edit Online](#)

The UK OFFICIAL and UK NHS blueprint sample provides governance guardrails using [Azure Policy](#) that help you assess specific [UK OFFICIAL and UK NHS](#) controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement controls for UK OFFICIAL and UK NHS.

Control mapping

The [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the **controls** in the UK OFFICIAL and UK NHS framework. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions. For more information, see [Azure Policy](#).

Deploy

To deploy the Azure Blueprints UK OFFICIAL and UK NHS blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **UK OFFICIAL and UK NHS** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name**: Provide a name for your copy of the UK OFFICIAL and UK NHS blueprint sample.
 - **Definition location**: Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that are included in the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from alignment with UK OFFICIAL and UK NHS controls.

1. Select **All services** in the left pane. Search for and select **Blueprints**.

2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the UK OFFICIAL and UK NHS blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:

- Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.

- Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).

- Managed Identity

Leave the default *system assigned* managed identity option.

- Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).

5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Blueprint initiative for UK OFFICIAL or UK NHS	Policy assignment	Resource types to audit diagnostic logs (Policy: Blueprint initiative for UK OFFICIAL or UK NHS)	List of resource types to audit if diagnostic log setting is not enabled. For acceptable values, see Supported services, schemas, and categories for Azure Diagnostic Logs .
[Preview]: Deploy Log Analytics Agent for Linux VMs	Policy assignment	Optional: List of VM images that have supported Linux OS to add to scope (Policy: [Preview]: Deploy Log Analytics Agent for Linux VMs)	(Optional) Default value is <i>none</i> . For more information, see Create a Log Analytics workspace in the Azure portal .
[Preview]: Deploy Log Analytics Agent for Windows VMs	Policy assignment	Optional: List of VM images that have supported Windows OS to add to scope (Policy: [Preview]: Deploy Log Analytics Agent for Windows VMs)	(Optional) Default value is <i>none</i> . For more information, see Create a Log Analytics workspace in the Azure portal .

Next steps

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

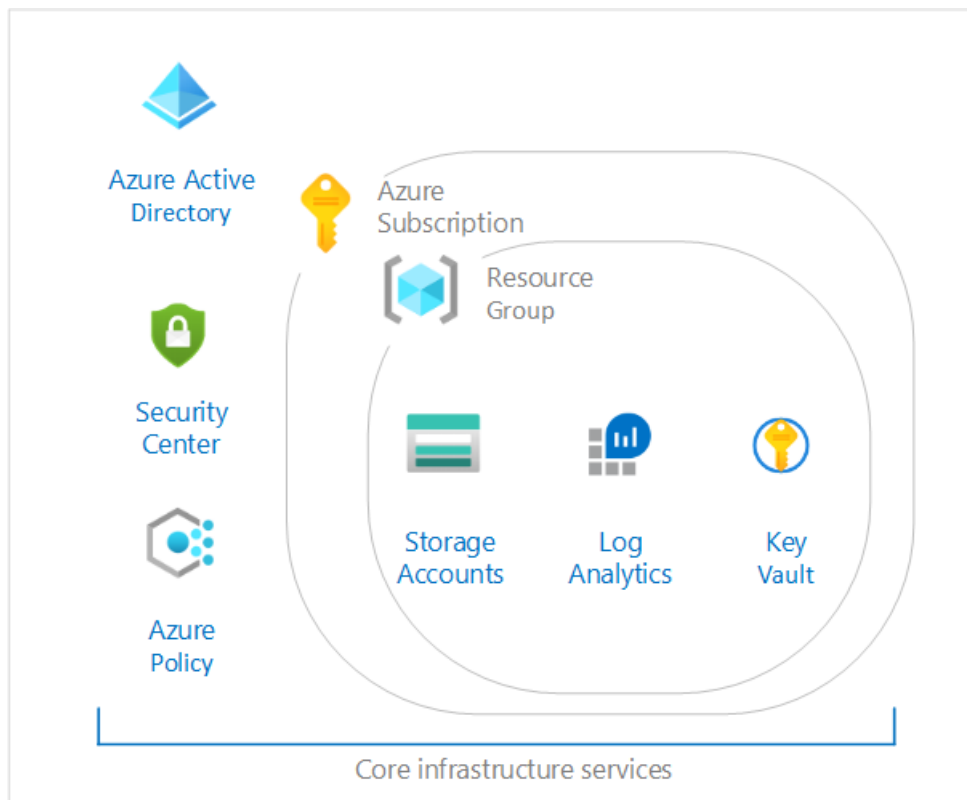
Overview of the Microsoft Cloud Adoption Framework for Azure Foundation blueprint sample

5/3/2021 • 2 minutes to read • [Edit Online](#)

The Microsoft Cloud Adoption Framework for Azure (CAF) Foundation blueprint deploys a set of core infrastructure resources and policy controls required for your first production grade Azure application. This foundation blueprint is based on the recommended pattern found in CAF.

Architecture

The CAF Foundation blueprint sample deploys recommended infrastructure resources in Azure that can be used by organizations to put in place the foundation controls necessary to manage their cloud estate. This sample will deploy and enforce resources, policies, and templates that will allow an organization to confidently get started with Azure.



Describes an Azure architecture which is achieved by deploying the C A F Foundation blueprint. It's applicable to a subscription with resource groups which consists of a storage account for storing logs, Log Analytics configured to store in the storage account. It also depicts Azure Key Vault configured with Azure Security Center standard setup. All these core infrastructures are accessed using Azure Active Directory and enforced using Azure Policy.

This implementation incorporates several Azure services used to provide a secure, fully monitored, enterprise-ready foundation. This environment is composed of:

- An [Azure Key Vault](#) instance used to host secrets used for the VMs deployed in the shared services environment
- Deploy [Log Analytics](#) is deployed to ensure all actions and services log to a central location from the moment you start your secure deployment in to [Storage Accounts](#) for diagnostic logging

- Deploy [Azure Security Center](#) (standard version) provides threat protection for your migrated workloads
- The blueprint also defines and deploys [Azure Policy](#) definitions:
 - Policy definitions:
 - Tagging (CostCenter) applied to resource groups
 - Append resources in resource group with the CostCenter Tag
 - Allowed Azure Region for Resources and Resource Groups
 - Allowed Storage Account SKUs (choose while deploying)
 - Allowed Azure VM SKUs (choose while deploying)
 - Require Network Watcher to be deployed
 - Require Azure Storage Account Secure transfer Encryption
 - Deny resource types (choose while deploying)
 - Policy initiatives:
 - Enable Monitoring in Azure Security Center (100+ policy definitions)

All these elements abide to the proven practices published in the [Azure Architecture Center - Reference Architectures](#).

NOTE

The CAF Foundation lays out a foundational architecture for workloads. You still need to deploy workloads behind this foundational architecture.

For more information, see the [Microsoft Cloud Adoption Framework for Azure - Ready](#).

Next steps

You've reviewed the overview and architecture of the CAF Foundation blueprint sample.

[CAF Foundation blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the Microsoft Cloud Adoption Framework for Azure Foundation blueprint sample

5/2/2021 • 5 minutes to read • [Edit Online](#)

To deploy the Microsoft Cloud Adoption Framework for Azure (CAF) Foundation blueprint sample, the following steps must be taken:

- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **CAF Foundation** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name:** Provide a name for your copy of the CAF Foundation blueprint sample.
 - **Definition location:** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from the CAF Foundation blueprint.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the CAF Foundation blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in.
 - Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - Managed Identity

Choose either the default *system assigned* managed identity option or the *user assigned* identity option.
 - Blueprint parameters

The parameters defined in this section are used by many of the artifacts in the blueprint definition to provide consistency.

 - **Organization**: Enter your organization name, such as Contoso, must be unique.
 - **Azure Region**: Select the Azure Region for Deployment.
 - **Allowed locations**: Which Azure Regions will you allow resources to be built in?
 - Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly an hour. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are [priced by product](#). Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Allowed storage account SKUs	Policy assignment	Policy_Allowed-StorageAccount-SKUs	SKU used in Diagnostic Log storage accounts
Allowed virtual machine SKUs	Policy assignment	Policy_Allowed-VM-SKUs	Allowed virtual machine SKUs
Append CostCenter TAG to Resource Groups	Policy assignment	Policy_CostCenter_Tag	Append CostCenter TAG and its value from the Resource Group
Resource Types that you do not want to allow in your environment	Policy assignment	Policy _Allowed-Resource-Types	Which Azure Resources you want to allow in your environment
Deploy Key Vault	Resource Manager template	KV-AccessPolicy	Locked - Azure AD Group or User to grant permissions to in Key Vault
Deploy Log Analytics	Resource Manager template	LogAnalytics_DataRetention	Locked - Number of days data will be retained in Log Analytics
Deploy Log Analytics	Resource Manager template	LogAnalytics_Location	Locked - Region used when establishing the workspace

Next steps

Now that you've reviewed the steps to deploy the CAF Foundation blueprint sample, visit the following article to learn about the architecture:

[CAF Foundation blueprint - Overview](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Overview of the Microsoft Cloud Adoption Framework for Azure Migration landing zone blueprint sample

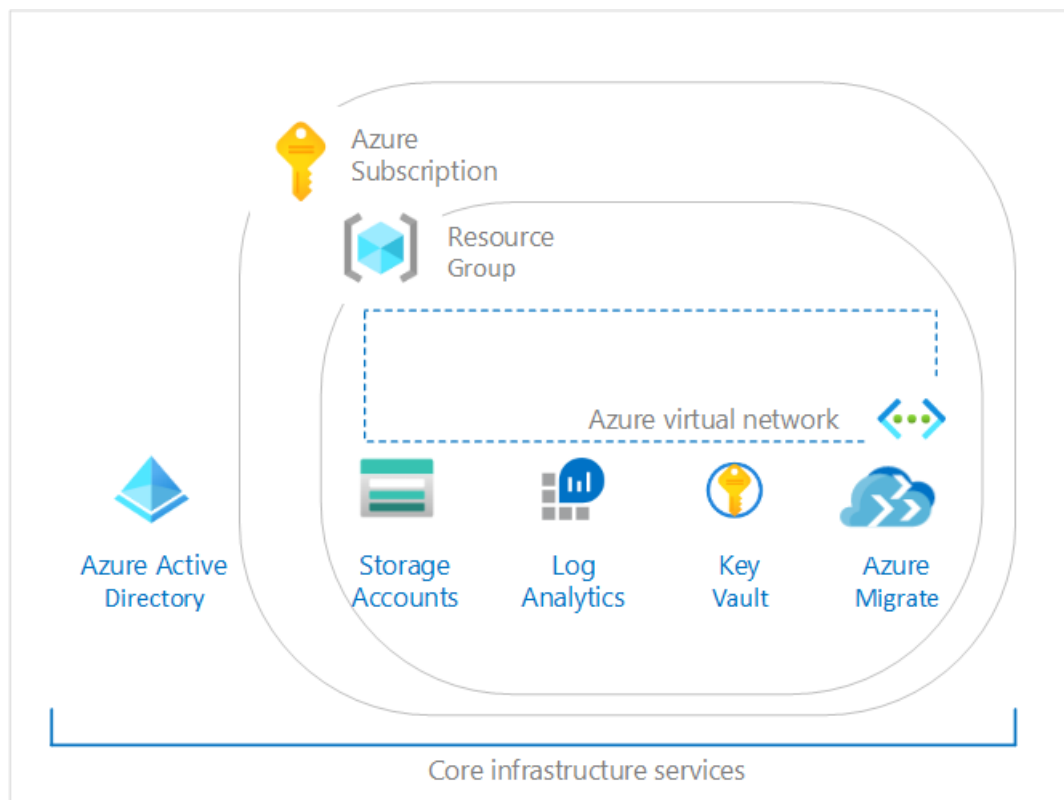
5/3/2021 • 2 minutes to read • [Edit Online](#)

The Microsoft Cloud Adoption Framework for Azure (CAF) Migration landing zone blueprint is a set of infrastructure to help you set up for migrating your first workload and manage your cloud estate in alignment with CAF.

The [CAF Foundation](#) blueprint sample extends this sample.

Architecture

The CAF Migration landing zone blueprint sample deploys foundation infrastructure resources in Azure that can be used by organizations to prepare their subscription for migrating virtual machines in to. It also helps put in place the governance controls necessary to manage their cloud estate. This sample will deploy and enforce resources, policies, and templates that will allow an organization to confidently get started with Azure.



Describes an Azure architecture which is achieved by deploying the C A F migration blueprint. It's applicable to a subscription with resource groups which consists of an Azure virtual network, storage account for storing logs, Log Analytics configured to store in the storage account. It also depicts Azure Key Vault configured and Azure Migrate initial setup created. All these core infrastructures are accessed using Azure Active Directory.

This environment is composed of several Azure services used to provide a secure, fully monitored, enterprise-ready governance. This environment is composed of:

- An [Azure Key Vault](#) instance used to host secrets used for the Certificates, Keys, and Secrets deployed in the shared services environment

- Deploy [Log Analytics](#) is deployed to ensure all actions and services log to a central location from the moment you start your migration
- Deploy [Azure Virtual Network](#) providing an isolated network and subnets for your virtual machine.
- Deploy [Azure Migrate Project](#) for discovery and assessment. We're adding the tools for Server assessment, Server migration, Database assessment, and Database migration.

All these elements abide to the proven practices published in the [Azure Architecture Center - Reference Architectures](#).

NOTE

The CAF Migration blueprint lays out a landing zone for your workloads. You still need to perform the assessment and migration of your Virtual Machines / Databases on top of this foundational architecture.

For more information, see the [Microsoft Cloud Adoption Framework for Azure - Migrate](#).

Next steps

You've reviewed the overview and architecture of the CAF Migrate landing zone blueprint sample.

[CAF Migration landing zone blueprint - Deploy steps](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Deploy the Microsoft Cloud Adoption Framework for Azure migrate landing zone blueprint sample

5/3/2021 • 4 minutes to read • [Edit Online](#)

To deploy the Azure Blueprints CAF Migration landing zone blueprint sample, the following steps must be taken:

- Recommended to deploy the [CAF Foundation](#) blueprint sample
- Create a new blueprint from the sample
- Mark your copy of the sample as **Published**
- Assign your copy of the blueprint to an existing subscription

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create blueprint from sample

First, implement the blueprint sample by creating a new blueprint in your environment using the sample as a starter.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. From the **Getting started** page on the left, select the **Create** button under *Create a blueprint*.
3. Find the **CAF Migration landing zone** blueprint sample under *Other Samples* and select **Use this sample**.
4. Enter the *Basics* of the blueprint sample:
 - **Blueprint name** Provide a name for your copy of the CAF Migration landing zone blueprint sample.
 - **Definition location** Use the ellipsis and select the management group to save your copy of the sample to.
5. Select the *Artifacts* tab at the top of the page or **Next: Artifacts** at the bottom of the page.
6. Review the list of artifacts that make up the blueprint sample. Many of the artifacts have parameters that we'll define later. Select **Save Draft** when you've finished reviewing the blueprint sample.

Publish the sample copy

Your copy of the blueprint sample has now been created in your environment. It's created in **Draft** mode and must be **Published** before it can be assigned and deployed. The copy of the blueprint sample can be customized to your environment and needs, but that modification may move it away from the CAF migrate landing zone guidance.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Publish blueprint** at the top of the page. In the new page on the right, provide a **Version** for your copy of the blueprint sample. This property is useful for if you make a modification later. Provide **Change notes** such as "First version published from the CAF migration landing zone blueprint sample." Then select **Publish** at the bottom of the page.

Assign the sample copy

Once the copy of the blueprint sample has been successfully **Published**, it can be assigned to a subscription within the management group it was saved to. This step is where parameters are provided to make each deployment of the copy of the blueprint sample unique.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select the **Blueprint definitions** page on the left. Use the filters to find your copy of the blueprint sample and then select it.
3. Select **Assign blueprint** at the top of the blueprint definition page.
4. Provide the parameter values for the blueprint assignment:
 - Basics
 - **Subscriptions**: Select one or more of the subscriptions that are in the management group you saved your copy of the blueprint sample to. If you select more than one subscription, an assignment will be created for each using the parameters entered.
 - **Assignment name**: The name is pre-populated for you based on the name of the blueprint. Change as needed or leave as is.
 - **Location**: Select a region for the managed identity to be created in.
 - Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint. To learn more, see [managed identities for Azure resources](#).
 - **Blueprint definition version**: Pick a **Published** version of your copy of the blueprint sample.
 - Lock Assignment

Select the blueprint lock setting for your environment. For more information, see [blueprints resource locking](#).
 - Managed Identity

Choose either the default *system assigned* managed identity option or the *user assigned* identity option.
 - Blueprint parameters

The parameters defined in this section are used by many of the artifacts in the blueprint definition to provide consistency.

 - **Organization**: Enter your organization name such as Contoso or Fabrikam, must be unique.
 - **AzureRegion**: Select one Azure Region for Deployment.
 - Artifact parameters

The parameters defined in this section apply to the artifact under which it's defined. These parameters are [dynamic parameters](#) since they're defined during the assignment of the blueprint. For a full list of artifact parameters and their descriptions, see [Artifact parameters table](#).
5. Once all parameters have been entered, select **Assign** at the bottom of the page. The blueprint assignment is created and artifact deployment begins. Deployment takes roughly five minutes. To check on the status of deployment, open the blueprint assignment.

WARNING

The Azure Blueprints service and the built-in blueprint samples are **free of cost**. Azure resources are **priced by product**. Use the [pricing calculator](#) to estimate the cost of running resources deployed by this blueprint sample.

Artifact parameters table

The following table provides a list of the blueprint artifact parameters:

ARTIFACT NAME	ARTIFACT TYPE	PARAMETER NAME	DESCRIPTION
Deploy vNET Landing Zone	Resource Manager template	IPAddress_Space	Locked - Provide first two octets example, 10.0
Deploy Key Vault	Resource Manager template	KV-AccessPolicy	Locked - Group or User Object ID to grant permissions to in Key Vault
Deploy Log Analytics	Resource Manager template	LogAnalytics_DataRetention	Locked - Number of days data will be retained in Log Analytics
Deploy Log Analytics	Resource Manager template	LogAnalytics_Location	Locked - Region used when establishing the workspace
Deploy Azure Migrate	Resource Manager template	Azure_Migrate_Location	Locked - Select the Region to deploy Azure Migrate

Next steps

Now that you've reviewed the steps to deploy the CAF migrate landing zone blueprint sample, visit the following articles to learn about the architecture:

[CAF Migration landing zone blueprint - Overview](#)

Additional articles about blueprints and how to use them:

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).

Understand the lifecycle of an Azure Blueprint

5/3/2021 • 4 minutes to read • [Edit Online](#)

Like many resources within Azure, a blueprint in Azure Blueprints has a typical and natural lifecycle. They're created, deployed, and finally deleted when no longer needed or relevant. Azure Blueprints supports standard lifecycle operations. It then builds upon them to provide additional levels of status that support common continuous integration and continuous deployment pipelines for organizations that manage their Infrastructure as Code - a key element in DevOps.

To fully understand a blueprint and the stages, we'll cover a standard lifecycle:

- Creating and editing a blueprint
- Publishing the blueprint
- Creating and editing a new version of the blueprint
- Publishing a new version of the blueprint
- Deleting a specific version of the blueprint
- Deleting the blueprint

Creating and editing a blueprint

When creating a blueprint, add artifacts to it, save to a management group or subscription, and provided a unique name and a unique version. The blueprint is now in a **Draft** mode and can't yet be assigned. While in the **Draft** mode, it can continue to be updated and changed.

A never published blueprint in **Draft** mode displays a different icon on the **Blueprint Definitions** page than ones that have been **Published**. The **Latest Version** is displayed as **Draft** for these never published blueprints.

Create and edit a blueprint with the [Azure portal](#) or [REST API](#).

Publishing a blueprint

Once all planned changes have been made to a blueprint in **Draft** mode, it can be **Published** and made available for assignment. The **Published** version of the blueprint can't be altered. Once **Published**, the blueprint displays with a different icon than **Draft** blueprints and displays the provided version number in the **Latest Version** column.

Publish a blueprint with the [Azure portal](#) or [REST API](#).

Creating and editing a new version of the blueprint

A **Published** version of a blueprint can't be altered. However, a new version of the blueprint can be added to the existing blueprint and modified as needed. Make changes to an existing blueprint by editing it. When the new changes are saved, the blueprint now has **Unpublished Changes**. These changes are a new **Draft** version of the blueprint.

Edit a blueprint with the [Azure portal](#).

Publishing a new version of the blueprint

Each edited version of a blueprint must be **Published** before it can be assigned. When **Unpublished Changes** have been made to a blueprint but not **Published**, the **Publish Blueprint** button is available on the edit

blueprint page. If the button isn't visible, the blueprint has already been **Published** and has no **Unpublished Changes**.

NOTE

A single blueprint can have multiple **Published** versions that can each be assigned to subscriptions.

To publish a blueprint with **Unpublished Changes**, use the same steps for publishing a new blueprint.

Deleting a specific version of the blueprint

Each version of a blueprint is a unique object and can be individually **Published**. As such, each version of a blueprint can also be deleted. Deleting a version of a blueprint doesn't have any impact on other versions of that blueprint.

NOTE

It's not possible to delete a blueprint that has active assignments. Delete the assignments first and then delete the version you wish to remove.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select **Blueprint definitions** from the page on the left and use the filter options to locate the blueprint you want to delete a version of. Select it to open the edit page.
3. Select the **Published versions** tab and locate the version you wish to delete.
4. Right-click on the version to delete and select **Delete this version**.

Deleting the blueprint

The core blueprint can also be deleted. Deleting the core blueprint also deletes any blueprint versions of that blueprint, including both **Draft** and **Published** blueprints. As with deleting a version of a blueprint, deleting the core blueprint doesn't remove the existing assignments of any of the blueprint versions.

NOTE

It's not possible to delete a blueprint that has active assignments. Delete the assignments first and then delete the version you wish to remove.

Delete a blueprint with the [Azure portal](#) or [REST API](#).

Assignments

There's several points during the lifecycle a blueprint can be assigned to a subscription. When the mode of a version of the blueprint is **Published**, then that version can be assigned to a subscription. This lifecycle enables versions of a blueprint to be used and actively assigned while a newer version is being developed.

As versions of blueprints are assigned, it's important to understand where they're assigned and with what parameters they've been assigned with. The parameters can either be static or dynamic. To learn more, see [static and dynamic parameters](#).

Updating assignments

When a blueprint is assigned, the assignment can be updated. There are several reasons for updating an existing

assignment, including:

- Add or remove [resource locking](#)
- Change the value of [dynamic parameters](#)
- Upgrade the assignment to a newer **Published** version of the blueprint

To learn how, see [update existing assignments](#).

Unassigning assignments

If the blueprint is no longer needed, it can be unassigned from the management group or subscription. During blueprint unassignment, the following occurs:

- Removal of [blueprint resource locking](#)
- Deletion of the blueprint assignment object
- (Conditional) If a **system-assigned managed identity** was used, it's also deleted

NOTE

All resources deployed by the blueprint assignment remain in place, but are no longer protected by Azure Blueprints.

Next steps

- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).

Stages of a blueprint deployment

4/30/2021 • 3 minutes to read • [Edit Online](#)

When a blueprint gets deployed, a series of actions is taken by the Azure Blueprints service to deploy the resources defined in the blueprint. This article provides details about what each step involves.

Blueprint deployment is triggered by assigning a blueprint to a subscription or [updating an existing assignment](#). During the deployment, Azure Blueprints takes the following high-level steps:

- Azure Blueprints granted owner rights
- The blueprint assignment object is created
- Optional - Azure Blueprints creates **system-assigned** managed identity
- The managed identity deploys blueprint artifacts
- Azure Blueprints service and **system-assigned** managed identity rights are revoked

Azure Blueprints granted owner rights

The Azure Blueprints service principal is granted owner rights to the assigned subscription or subscriptions when a [system-assigned managed identity](#) managed identity is used. The granted role allows Azure Blueprints to create, and later revoke, the **system-assigned** managed identity. If using a **user-assigned** managed identity, the Azure Blueprints service principal doesn't get and doesn't need owner rights on the subscription.

The rights are granted automatically if the assignment is done through the portal. However, if the assignment is done through the REST API, granting the rights needs to be done with a separate API call. The Azure Blueprints AppId is `f71766dc-90d9-4b7d-bd9d-4499c4331c3f`, but the service principal varies by tenant. Use [Azure Active Directory Graph API](#) and REST endpoint [servicePrincipals](#) to get the service principal. Then, grant the Azure Blueprints the *Owner* role through the [Portal](#), [Azure CLI](#), [Azure PowerShell](#), [REST API](#), or an [Azure Resource Manager template](#).

The Azure Blueprints service doesn't directly deploy the resources.

The blueprint assignment object is created

A user, group, or service principal assigns a blueprint to a subscription. The assignment object exists at the subscription level where the blueprint was assigned. Resources created by the deployment aren't done in context of the deploying entity.

While creating the blueprint assignment, the type of [managed identity](#) is selected. The default is a **system-assigned** managed identity. A **user-assigned** managed identity can be chosen. When using a **user-assigned** managed identity, it must be defined and granted permissions before the blueprint assignment is created. Both the [Owner](#) and [Blueprint Operator](#) built-in roles have the necessary `blueprintAssignment/write` permission to create an assignment that uses a **user-assigned** managed identity.

Optional - Azure Blueprints creates system-assigned managed identity

When [system-assigned managed identity](#) is selected during assignment, Azure Blueprints creates the identity and grants the managed identity the [owner](#) role. If an [existing assignment is upgraded](#), Azure Blueprints uses the previously created managed identity.

The managed identity related to the blueprint assignment is used to deploy or redeploy the resources defined in

the blueprint. This design avoids assignments inadvertently interfering with each other. This design also supports the [resource locking](#) feature by controlling the security of each deployed resource from the blueprint.

The managed identity deploys blueprint artifacts

The managed identity then triggers the Resource Manager deployments of the artifacts within the blueprint in the defined [sequencing order](#). The order can be adjusted to ensure artifacts dependent on other artifacts are deployed in the correct order.

An access failure by a deployment is often the result of the level of access granted to the managed identity. The Azure Blueprints service manages the security lifecycle of the **system-assigned** managed identity. However, the user is responsible for managing the rights and lifecycle of a **user-assigned** managed identity.

Blueprint service and system-assigned managed identity rights are revoked

Once the deployments are completed, Azure Blueprints revokes the rights of the **system-assigned** managed identity from the subscription. Then, the Azure Blueprints service revokes its rights from the subscription. Rights removal prevents Azure Blueprints from becoming a permanent owner on a subscription.

Next steps

- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).

Creating dynamic blueprints through parameters

5/3/2021 • 7 minutes to read • [Edit Online](#)

A fully defined blueprint with various artifacts such as resource groups, Azure Resource Manager templates (ARM templates), policies, or role assignments, offers the rapid creation and consistent creation of objects within Azure. To enable flexible use of these reusable design patterns and containers, Azure Blueprints supports parameters. The parameter creates flexibility, both during definition and assignment, to change properties on the artifacts deployed by the blueprint.

A simple example is the resource group artifact. When a resource group is created, it has two required values that must be provided: name and location. When adding a resource group to your blueprint, if parameters didn't exist, you would define that name and location for every use of the blueprint. This repetition would cause every use of the blueprint to create artifacts in the same resource group. Resources inside that resource group would become duplicated and cause a conflict.

NOTE

It isn't an issue for two different blueprints to include a resource group with the same name. If a resource group included in a blueprint already exists, the blueprint continues to create the related artifacts in that resource group. This could cause a conflict as two resources with the same name and resource type cannot exist within a subscription.

The solution to this problem is parameters. Azure Blueprints allows you to define the value for each property of the artifact during assignment to a subscription. The parameter makes it possible to reuse a blueprint that creates a resource group and other resources within a single subscription without having conflict.

Blueprint parameters

Through the REST API, parameters can be created on the blueprint itself. These parameters are different than the parameters on each of the supported artifacts. When a parameter is created on the blueprint, it can be used by the artifacts in that blueprint. An example might be the prefix for naming of the resource group. The artifact can use the blueprint parameter to create a "mostly dynamic" parameter. As the parameter can also be defined during assignment, this pattern allows for a consistency that may adhere to naming rules. For steps, see [setting static parameters - blueprint level parameter](#).

Using `secureString` and `secureObject` parameters

While an ARM template *artifact* supports parameters of the `secureString` and `secureObject` types, Azure Blueprints requires each to be connected with an Azure Key Vault. This security measure prevents the unsafe practice of storing secrets along with the Blueprint and encourages employment of secure patterns. Azure Blueprints supports this security measure, detecting the inclusion of either secure parameter in an ARM template *artifact*. The service then prompts during assignment for the following Key Vault properties per detected secure parameter:

- Key Vault resource ID
- Key Vault secret name
- Key Vault secret version

If the blueprint assignment uses a **system-assigned managed identity**, the referenced Key Vault *must* exist in the same subscription the blueprint definition is assigned to.

If the blueprint assignment uses a **user-assigned managed identity**, the referenced Key Vault *may* exist in a

centralized subscription. The managed identity must be granted appropriate rights on the Key Vault prior to blueprint assignment.

IMPORTANT

In both cases, the Key Vault must have **Enable access to Azure Resource Manager for template deployment** configured on the **Access policies** page. For directions on how to enable this feature, see [Key Vault - Enable template deployment](#).

For more information about Azure Key Vault, see [Key Vault Overview](#).

Parameter types

Static parameters

A parameter value defined in the definition of a blueprint is called a **static parameter**, because every use of the blueprint will deploy the artifact using that static value. In the resource group example, while it doesn't make sense for the name of the resource group, it might make sense for the location. Then, every assignment of the blueprint would create the resource group, whatever it's called during assignment, in the same location. This flexibility allows you to be selective in what you define as required vs what can be changed during assignment.

Setting static parameters in the portal

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select **Blueprint definitions** from the page on the left.
3. Select an existing blueprint and then select **Edit blueprint** OR select + **Create blueprint** and fill out the information on the **Basics** tab.
4. Select **Next: Artifacts** OR select the **Artifacts** tab.
5. Artifacts added to the blueprint that have parameter options display **X of Y parameters populated** in the **Parameters** column. Select the artifact row to edit the artifact parameters.

Role assignment	1 out of 1 parameters populated
Policy assignment	None
Resource group	1 out of 2 parameters populated

6. The **Edit Artifact** page displays value options appropriate to the artifact selected. Each parameter on the artifact has a title, a value box, and a checkbox. Set the box to unchecked to make it a **static parameter**. In the following example, only *Location* is a **static parameter** as it's unchecked and *Resource Group Name* is checked.

Resource Group Name

Set value(s)

☒ This value should be specified when the blueprint is assigned

Location

East US

☐ This value should be specified when the blueprint is assigned

Resource Group Tags (Optional):

TAG NAME	TAG VALUE
<i>Enter tag name</i>	:

Setting static parameters from REST API

In each REST API URI, there are variables that are used that you need to replace with your own values:

- {YourMG} - Replace with the name of your management group
- {subscriptionId} - Replace with your subscription ID

Blueprint level parameter

When creating a blueprint through REST API, it's possible to create [blueprint parameters](#). To do so, use the following REST API URI and body format:

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint?api-version=2018-11-01-preview
```

- Request Body

```
{
  "properties": {
    "description": "This blueprint has blueprint level parameters.",
    "targetScope": "subscription",
    "parameters": {
      "owners": {
        "type": "array",
        "metadata": {
          "description": "List of AAD object IDs that is assigned Owner role at the resource group"
        }
      }
    },
    "resourceGroups": {
      "storageRG": {
        "description": "Contains the resource template deployment and a role assignment."
      }
    }
  }
}
```

Once a blueprint level parameter is created, it can be used on artifacts added to that blueprint. The following REST API example creates a role assignment artifact on the blueprint and uses the blueprint level parameter.

- REST API URI


```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/artifacts/roleOwner?api-version=2018-11-01-preview
```

- Request Body

```
{
  "kind": "roleAssignment",
  "properties": {
    "resourceGroup": "storageRG",
    "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bc635",
    "principalIds": "[parameters('owners')]"
  }
}
```

In this example, the **principalIds** property uses the **owners** blueprint level parameter by using a value of `[parameters('owners')]`. Setting a parameter on an artifact using a blueprint level parameter is still an example of a **static parameter**. The blueprint level parameter can't be set during blueprint assignment and will be the same value on each assignment.

Artifact level parameter

Creating **static parameters** on an artifact is similar, but takes a straight value instead of using the `parameters()` function. The following example creates two static parameters, **tagName** and **tagValue**. The value on each is directly provided and doesn't use a function call.

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/artifacts/policyStorageTags?api-version=2018-11-01-preview
```

- Request Body

```
{
  "kind": "policyAssignment",
  "properties": {
    "description": "Apply storage tag and the parameter also used by the template to resource groups",
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-6fd1-46fd-a676-f12d1d3a4c71",
    "parameters": {
      "tagName": {
        "value": "StorageType"
      },
      "tagValue": {
        "value": "Premium_LRS"
      }
    }
  }
}
```

Dynamic parameters

The opposite of a static parameter is a **dynamic parameter**. This parameter isn't defined on the blueprint, but instead is defined during each assignment of the blueprint. In the resource group example, use of a **dynamic parameter** makes sense for the resource group name. It provides a different name for every assignment of the blueprint. For a list of blueprint functions, see the [blueprint functions](#) reference.

Setting dynamic parameters in the portal

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select **Blueprint definitions** from the page on the left.
3. Right-click on the blueprint that you want to assign. Select **Assign blueprint** OR select the blueprint you want to assign, then use the **Assign blueprint** button.
4. On the **Assign blueprint** page, find the **Artifact parameters** section. Each artifact with at least one **dynamic parameter** displays the artifact and the configuration options. Provide required values to the parameters before assigning the blueprint. In the following example, *Name* is a **dynamic parameter** that must be defined to complete blueprint assignment.

Artifact parameters	
ARTIFACT / PARAMETER	PARAMETER VALUE
🔑 Subscription	
▼ 🌐 ResourceGroup	
Resource Group: Name	<input type="text" value="Set value(s)"/>
Resource Group: Location	<input type="text" value="eastus"/>

Setting dynamic parameters from REST API

Setting **dynamic parameters** during the assignment is done by entering the value directly. Instead of using a function, such as `parameters()`, the value provided is an appropriate string. Artifacts for a resource group are defined with a "template name", **name**, and **location** properties. All other parameters for included artifact are defined under **parameters** with a **<name>** and **value** key pair. If the blueprint is configured for a dynamic parameter that isn't provided during assignment, the assignment will fail.

- REST API URI

```
PUT
https://management.azure.com/subscriptions/{subscriptionId}/providers/Microsoft.Blueprint/blueprintAssignments/assignMyBlueprint?api-version=2018-11-01-preview
```

- Request Body

```

{
  "properties": {
    "blueprintId": "/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint",
    "resourceGroups": {
      "storageRG": {
        "name": "StorageAccount",
        "location": "eastus2"
      }
    },
    "parameters": {
      "storageAccountType": {
        "value": "Standard_GRS"
      },
      "tagName": {
        "value": "CostCenter"
      },
      "tagValue": {
        "value": "ContosoIT"
      },
      "contributors": {
        "value": [
          "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
          "38833b56-194d-420b-90ce-cff578296714"
        ]
      },
      "owners": {
        "value": [
          "44254d2b-a0c7-405f-959c-f829ee31c2e7",
          "316deb5f-7187-4512-9dd4-21e7798b0ef9"
        ]
      }
    },
    "identity": {
      "type": "systemAssigned"
    },
    "location": "westus"
  }
}

```

Next steps

- See the list of [blueprint functions](#).
- Learn about the [blueprint lifecycle](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).

Understand the deployment sequence in Azure Blueprints

4/30/2021 • 3 minutes to read • [Edit Online](#)

Azure Blueprints uses a **sequencing order** to determine the order of resource creation when processing the assignment of a blueprint definition. This article explains the following concepts:

- The default sequencing order that is used
- How to customize the order
- How the customized order is processed

There are variables in the JSON examples that you need to replace with your own values:

- `{YourMG}` - Replace with the name of your management group

Default sequencing order

If the blueprint definition contains no directive for the order to deploy artifacts or the directive is null, then the following order is used:

- Subscription level **role assignment** artifacts sorted by artifact name
- Subscription level **policy assignment** artifacts sorted by artifact name
- Subscription level **Azure Resource Manager template** (ARM templates) artifacts sorted by artifact name
- **Resource group** artifacts (including child artifacts) sorted by placeholder name

Within each **resource group** artifact, the following sequence order is used for artifacts to be created within that resource group:

- Resource group child **role assignment** artifacts sorted by artifact name
- Resource group child **policy assignment** artifacts sorted by artifact name
- Resource group child **Azure Resource Manager template** (ARM templates) artifacts sorted by artifact name

NOTE

Use of `artifacts()` creates an implicit dependency on the artifact being referred to.

Customizing the sequencing order

When composing large blueprint definitions, it may be necessary for resources to be created in a specific order. The most common use pattern of this scenario is when a blueprint definition includes several ARM templates. Azure Blueprints handles this pattern by allowing the sequencing order to be defined.

The ordering is accomplished by defining a `dependsOn` property in the JSON. The blueprint definition, for resource groups, and artifact objects support this property. `dependsOn` is a string array of artifact names that the particular artifact needs to be created before it's created.

NOTE

When creating blueprint objects, each artifact resource gets its name from the filename, if using [PowerShell](#), or the URL endpoint, if using [REST API](#). *resourceGroup* references in artifacts must match those defined in the blueprint definition.

Example - ordered resource group

This example blueprint definition has a resource group that has defined a custom sequencing order by declaring a value for `dependsOn`, along with a standard resource group. In this case, the artifact named **assignPolicyTags** will be processed before the **ordered-rg** resource group. **standard-rg** will be processed per the default sequencing order.

```
{
  "properties": {
    "description": "Example blueprint with custom sequencing order",
    "resourceGroups": {
      "ordered-rg": {
        "dependsOn": [
          "assignPolicyTags"
        ],
        "metadata": {
          "description": "Resource Group that waits for 'assignPolicyTags' creation"
        }
      },
      "standard-rg": {
        "metadata": {
          "description": "Resource Group that follows the standard sequence ordering"
        }
      }
    },
    "targetScope": "subscription"
  },
  "type": "Microsoft.Blueprint/blueprints"
}
```

Example - artifact with custom order

This example is a policy artifact that depends on an ARM template. By default ordering, a policy artifact would be created before the ARM template. This ordering allows the policy artifact to wait for the ARM template to be created.

```
{
  "properties": {
    "displayName": "Assigns an identifying tag",
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/2a0e14a6-b0a6-4fab-991a-187a4f81c498",
    "resourceGroup": "standard-rg",
    "dependsOn": [
      "customTemplate"
    ]
  },
  "kind": "policyAssignment",
  "type": "Microsoft.Blueprint/artifacts"
}
```

Example - subscription level template artifact depending on a resource group

This example is for an ARM template deployed at the subscription level to depend on a resource group. In default ordering, the subscription level artifacts would be created before any resource groups and child artifacts in those resource groups. The resource group is defined in the blueprint definition like this:

```

"resourceGroups": {
  "wait-for-me": {
    "metadata": {
      "description": "Resource Group that is deployed prior to the subscription level template artifact"
    }
  }
}

```

The subscription level template artifact depending on the **wait-for-me** resource group is defined like this:

```

{
  "properties": {
    "template": {
      ...
    },
    "parameters": {
      ...
    },
    "dependsOn": ["wait-for-me"],
    "displayName": "SubLevelTemplate",
    "description": ""
  },
  "kind": "template",
  "type": "Microsoft.Blueprint/blueprints/artifacts"
}

```

Processing the customized sequence

During the creation process, a topological sort is used to create the dependency graph of the blueprints artifacts. The check makes sure each level of dependency between resource groups and artifacts is supported.

If an artifact dependency is declared that wouldn't alter the default order, then no change is made. An example is a resource group that depends on a subscription level policy. Another example is a resource group 'standard-rg' child policy assignment that depends on resource group 'standard-rg' child role assignment. In both cases, the `dependsOn` wouldn't have altered the default sequencing order and no changes would be made.

Next steps

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).

Understand resource locking in Azure Blueprints

4/22/2021 • 5 minutes to read • [Edit Online](#)

The creation of consistent environments at scale is only truly valuable if there's a mechanism to maintain that consistency. This article explains how resource locking works in Azure Blueprints. To see an example of resource locking and application of *deny assignments*, see the [protecting new resources](#) tutorial.

NOTE

Resource locks deployed by Azure Blueprints are only applied to [non-extension resources](#) deployed by the blueprint assignment. Existing resources, such as those in resource groups that already exist, don't have locks added to them.

Locking modes and states

Locking Mode applies to the blueprint assignment and it has three options: **Don't Lock**, **Read Only**, or **Do Not Delete**. The locking mode is configured during artifact deployment during a blueprint assignment. A different locking mode can be set by updating the blueprint assignment. Locking modes, however, can't be changed outside of Azure Blueprints.

Resources created by artifacts in a blueprint assignment have four states: **Not Locked**, **Read Only**, **Cannot Edit / Delete**, or **Cannot Delete**. Each artifact type can be in the **Not Locked** state. The following table can be used to determine the state of a resource:

MODE	ARTIFACT RESOURCE TYPE	STATE	DESCRIPTION
Don't Lock	*	Not Locked	Resources aren't protected by Azure Blueprints. This state is also used for resources added to a Read Only or Do Not Delete resource group artifact from outside a blueprint assignment.
Read Only	Resource group	Cannot Edit / Delete	The resource group is read only and tags on the resource group can't be modified. Not Locked resources can be added, moved, changed, or deleted from this resource group.
Read Only	Non-resource group	Read Only	The resource can't be altered in any way. No changes and it can't be deleted.
Do Not Delete	*	Cannot Delete	The resources can be altered, but can't be deleted. Not Locked resources can be added, moved, changed, or deleted from this resource group.

Overriding locking states

It's typically possible for someone with appropriate [Azure role-based access control \(Azure RBAC\)](#) on the subscription, such as the 'Owner' role, to be allowed to alter or delete any resource. This access isn't the case when Azure Blueprints applies locking as part of a deployed assignment. If the assignment was set with the **Read Only** or **Do Not Delete** option, not even the subscription owner can perform the blocked action on the protected resource.

This security measure protects the consistency of the defined blueprint and the environment it was designed to create from accidental or programmatic deletion or alteration.

Assign at management group

The only option to prevent subscription owners from removing a blueprint assignment is to assign the blueprint to a management group. In this scenario, only **Owners** of the management group have the permissions needed to remove the blueprint assignment.

To assign the blueprint to a management group instead of a subscription, the REST API call changes to look like this:

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{assignmentMG}/providers/Microsoft.Blueprint/blueprintAssignments/{assignmentName}?api-version=2018-11-01-preview
```

The management group defined by `{assignmentMG}` must be either within the management group hierarchy or be the same management group where the blueprint definition is saved.

The request body of the blueprint assignment looks like this:


```

{
  "identity": {
    "type": "SystemAssigned"
  },
  "location": "eastus",
  "properties": {
    "description": "enforce pre-defined simpleBlueprint to this XXXXXXXX subscription.",
    "blueprintId":
"/providers/Microsoft.Management/managementGroups/{blueprintMG}/providers/Microsoft.Blueprint/blueprints/simpleBlueprint",
    "scope": "/subscriptions/{targetSubscriptionId}",
    "parameters": {
      "storageAccountType": {
        "value": "Standard_LRS"
      },
      "costCenter": {
        "value": "Contoso/Online/Shopping/Production"
      },
      "owners": {
        "value": [
          "johnDoe@contoso.com",
          "johnsteam@contoso.com"
        ]
      }
    },
    "resourceGroups": {
      "storageRG": {
        "name": "defaultRG",
        "location": "eastus"
      }
    }
  }
}

```

The key difference in this request body and one being assigned to a subscription is the `properties.scope` property. This required property must be set to the subscription that the blueprint assignment applies to. The subscription must be a direct child of the management group hierarchy where the blueprint assignment is stored.

NOTE

A blueprint assigned to management group scope still operates as a subscription level blueprint assignment. The only difference is where the blueprint assignment is stored to prevent subscription owners from removing the assignment and associated locks.

Removing locking states

If it becomes necessary to modify or delete a resource protected by an assignment, there are two ways to do so.

- Updating the blueprint assignment to a locking mode of **Don't Lock**
- Delete the blueprint assignment

When the assignment is removed, the locks created by Azure Blueprints are removed. However, the resource is left behind and would need to be deleted through normal means.

How blueprint locks work

An Azure RBAC [deny assignments](#) deny action is applied to artifact resources during assignment of a blueprint if the assignment selected the **Read Only** or **Do Not Delete** option. The deny action is added by the managed

identity of the blueprint assignment and can only be removed from the artifact resources by the same managed identity. This security measure enforces the locking mechanism and prevents removing the blueprint lock outside Azure Blueprints.

LockedByBlueprints - Access control (IAM)

Resource group

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Events

+

 Add

≡

 Edit columns

↺

 Refresh

🗑

 Remove

Check access

Role assignments

Deny assignments

Classic administrators

Roles

Deny assignments block users from performing specific actions even if a role assignment grants them access. At this time, deny assignments are read-only and can only be set by Azure. [Learn more](#)

NAME	DENIED	EXCLUDED PRINCIPALS	SCOPE
Deny assignment '27ae2c52-ef23...		All principals	Yes

The [deny assignment properties](#) of each mode are as follows:

MODE	PERMISSIONS.ACTIONS	PERMISSIONS.NOT ACTIONS	PRINCIPALS[[]].TYPE	EXCLUDEPRINCIPALS[[]].ID	DONOTAPPLYTOCHILDSCOPES
Read Only	*	*/read Microsoft.Authorization/locks/delete Microsoft.Network/virtualNetwork/subnets/join/action	SystemDefined (Everyone)	blueprint assignment and user-defined in excludedPrincipals	Resource group - <i>true</i> ; Resource - <i>false</i>
Do Not Delete	*/delete	Microsoft.Authorization/locks/delete Microsoft.Network/virtualNetwork/subnets/join/action	SystemDefined (Everyone)	blueprint assignment and user-defined in excludedPrincipals	Resource group - <i>true</i> ; Resource - <i>false</i>

IMPORTANT

Azure Resource Manager caches role assignment details for up to 30 minutes. As a result, deny assignments deny action's on blueprint resources may not immediately be in full effect. During this period of time, it might be possible to delete a resource intended to be protected by blueprint locks.

Exclude a principal from a deny assignment

In some design or security scenarios, it may be necessary to exclude a principal from the [deny assignment](#) the blueprint assignment creates. This step is done in REST API by adding up to five values to the `excludedPrincipals` array in the `locks` property when [creating the assignment](#). The following assignment definition is an example of a request body that includes `excludedPrincipals`:

```
{
  "identity": {
    "type": "SystemAssigned"
  },
  "location": "eastus",
  "properties": {
    "description": "enforce pre-defined simpleBlueprint to this XXXXXXXX subscription.",
    "blueprintId":
"/providers/Microsoft.Management/managementGroups/{mgId}/providers/Microsoft.Blueprint/blueprints/simpleBlue
print",
    "locks": {
      "mode": "AllResourcesDoNotDelete",
      "excludedPrincipals": [
        "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
        "38833b56-194d-420b-90ce-cff578296714"
      ]
    },
    "parameters": {
      "storageAccountType": {
        "value": "Standard_LRS"
      },
      "costCenter": {
        "value": "Contoso/Online/Shopping/Production"
      },
      "owners": {
        "value": [
          "johnDoe@contoso.com",
          "johnsteam@contoso.com"
        ]
      }
    },
    "resourceGroups": {
      "storageRG": {
        "name": "defaultRG",
        "location": "eastus"
      }
    }
  }
}
```

Exclude an action from a deny assignment

Similar to [excluding a principal](#) on a [deny assignment](#) in a blueprint assignment, you can exclude specific [Azure resource provider operations](#). Within the `properties.locks` block, in the same place that `excludedPrincipals` is, an `excludedActions` can be added:

```
"locks": {
  "mode": "AllResourcesDoNotDelete",
  "excludedPrincipals": [
    "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
    "38833b56-194d-420b-90ce-cff578296714"
  ],
  "excludedActions": [
    "Microsoft.ContainerRegistry/registries/push/write",
    "Microsoft.Authorization/*/read"
  ]
},
```

While `excludedPrincipals` must be explicit, `excludedActions` entries can make use of `*` for wildcard matching of resource provider operations.

Next steps

- Follow the [protect new resources](#) tutorial.
- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Learn how to [update existing assignments](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).

How to manage assignments with PowerShell

4/30/2021 • 9 minutes to read • [Edit Online](#)

A blueprint assignment can be managed using the **Az.Blueprint** Azure PowerShell module. The module supports fetching, creating, updating, and removing assignments. The module can also fetch details on existing blueprint definitions. This article covers how to install the module and start using it.

Add the Az.Blueprint module

To enable Azure PowerShell to manage blueprint assignments, the module must be added. This module can be used with locally installed PowerShell, with [Azure Cloud Shell](#), or with the [Azure PowerShell Docker image](#).

Base requirements

The Azure Blueprints module requires the following software:

- Azure PowerShell 1.5.0 or higher. If it isn't yet installed, follow [these instructions](#).
- PowerShellGet 2.0.1 or higher. If it isn't installed or updated, follow [these instructions](#).

Install the module

The Azure Blueprints module for PowerShell is **Az.Blueprint**.

1. From an **administrative** PowerShell prompt, run the following command:

```
# Install the Azure Blueprints module from PowerShell Gallery
Install-Module -Name Az.Blueprint
```

NOTE

If **Az.Accounts** is already installed, it may be necessary to use `-AllowClobber` to force the installation.

2. Validate that the module has been imported and is the correct version (0.2.6):

```
# Get a list of commands for the imported Az.Blueprint module
Get-Command -Module 'Az.Blueprint' -CommandType 'Cmdlet'
```

Get blueprint definitions

The first step to working with an assignment is often getting a reference to a blueprint definition. The `Get-AzBlueprint` cmdlet gets one or more blueprint definitions. The cmdlet can get blueprint definitions from a management group with `-ManagementGroupId {mgId}` or a subscription with `-SubscriptionId {subId}`. The **Name** parameter gets a blueprint definition, but must be used with **ManagementGroupId** or **SubscriptionId**. **Version** can be used with **Name** to be more explicit about which blueprint definition is returned. Instead of **Version**, the switch `-LatestPublished` grabs the most recently published version.

The following example uses `Get-AzBlueprint` to get all versions of a blueprint definition named '101-blueprints-definition-subscription' from a specific subscription represented as `{subId}`:

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get all versions of the blueprint definition in the specified subscription
$blueprints = Get-AzBlueprint -SubscriptionId '{subId}' -Name '101-blueprints-definition-subscription'

# Display the blueprint definition object
$blueprints
```

The example output for a blueprint definition with multiple versions looks like this:

```
Name           : 101-blueprints-definition-subscription
Id             : /subscriptions/{subId}/providers/Microsoft.Blueprint/blueprints/101
               -blueprints-definition-subscription
DefinitionLocationId : {subId}
Versions       : {1.0, 1.1}
TimeCreated    : 2019-02-25
TargetScope    : Subscription
Parameters     : {storageAccount_storageAccountType, storageAccount_location,
                  allowedlocations_listOfAllowedLocations,
                  [Usergrouporapplicationname]:Reader_RoleAssignmentName}
ResourceGroups : ResourceGroup
```

The [blueprint parameters](#) on the blueprint definition can be expanded to provide more information.

```
$blueprints.Parameters
```

Key	Value
---	----
storageAccount_storageAccountType	Microsoft.Azure.Commands.Blueprint.Models.PSParameterDefinition
storageAccount_location	Microsoft.Azure.Commands.Blueprint.Models.PSParameterDefinition
allowedlocations_listOfAllowedLocations	Microsoft.Azure.Commands.Blueprint.Models.PSParameterDefinition
[Usergrouporapplicationname]:Reader_RoleAssignmentName	Microsoft.Azure.Commands.Blueprint.Models.PSParameterDefinition

Get blueprint assignments

If the blueprint assignment already exists, you can get a reference to it with the `Get-AzBlueprintAssignment` cmdlet. The cmdlet takes **SubscriptionId** and **Name** as optional parameters. If **SubscriptionId** isn't specified, the current subscription context is used.

The following example uses `Get-AzBlueprintAssignment` to get a single blueprint assignment named 'Assignment-lock-resource-groups' from a specific subscription represented as `{subId}`:

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get the blueprint assignment in the specified subscription
$blueprintAssignment = Get-AzBlueprintAssignment -SubscriptionId '{subId}' -Name 'Assignment-lock-resource-groups'

# Display the blueprint assignment object
$blueprintAssignment
```

The example output for a blueprint assignment looks like this:

```
Name          : Assignment-lock-resource-groups
Id            : /subscriptions/{subId}/providers/Microsoft.Blueprint/blueprintAssignments/Assignment-lock-resource-groups
Scope        : /subscriptions/{subId}
LastModified  : 2019-02-19
LockMode     : AllResourcesReadOnly
ProvisioningState : Succeeded
Parameters    :
ResourceGroups : ResourceGroup
```

Create blueprint assignments

If the blueprint assignment doesn't exist yet, you can create it with the `New-AzBlueprintAssignment` cmdlet. This cmdlet uses the following parameters:

- **Name** [required]
 - Specifies the name of the blueprint assignment
 - Must be unique and not already exist in **SubscriptionId**
- **Blueprint** [required]
 - Specifies the blueprint definition to assign
 - Use `Get-AzBlueprint` to get the reference object
- **Location** [required]
 - Specifies the region for the system-assigned managed identity and subscription deployment object to be created in
- **Subscription** (optional)
 - Specifies the subscription the assignment is deployed to
 - If not provided, defaults to the current subscription context
- **Lock** (optional)
 - Defines the [blueprint resource locking](#) to use for deployed resources
 - Supported options: *None*, *AllResourcesReadOnly*, *AllResourcesDoNotDelete*
 - If not provided, defaults to *None*
- **SystemAssignedIdentity** (optional)
 - Select to create a system-assigned managed identity for the assignment and to deploy the resources
 - Default for the "identity" parameter set
 - Can't be used with **UserAssignedIdentity**
- **UserAssignedIdentity** (optional)
 - Specifies the user-assigned managed identity to use for the assignment and to deploy the resources
 - Part of the "identity" parameter set
 - Can't be used with **SystemAssignedIdentity**
- **Parameter** (optional)
 - A [hash table](#) of key/value pairs for setting [dynamic parameters](#) on the blueprint assignment
 - Default for a dynamic parameter is the **defaultValue** in the definition
 - If a parameter isn't provided and has no **defaultValue**, the parameter isn't optional

NOTE

Parameter doesn't support `secureStrings`.

- **ResourceGroupParameter** (optional)
 - A [hash table](#) of resource group artifacts
 - Each resource group artifact placeholder has key/value pairs for dynamically setting **Name** and **Location** on that resource group artifact
 - If a resource group parameter isn't provided and has no **defaultValue**, the resource group parameter isn't optional
- **AssignmentFile** (optional)
 - The path to a JSON file representation of a blueprint assignment
 - This parameter is part of a PowerShell parameter set that only includes **Name**, **Blueprint**, and **SubscriptionId**, plus the common parameters.

Example 1: Provide parameters

The following example creates a new assignment of version '1.1' of the 'my-blueprint' blueprint definition fetched with `Get-AzBlueprint`, sets the managed identity and assignment object location to 'westus2', locks the resources with *AllResourcesReadOnly*, and sets the hash tables for both **Parameter** and **ResourceGroupParameter** on specific subscription represented as `{subId}`:

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get version '1.1' of the blueprint definition in the specified subscription
$bpDefinition = Get-AzBlueprint -SubscriptionId '{subId}' -Name 'my-blueprint' -Version '1.1'

# Create the hash table for Parameters
$bpParameters = @{storageAccount_storageAccountType='Standard_GRS'}

# Create the hash table for ResourceGroupParameters
# ResourceGroup is the resource group artifact placeholder name
$bpRGParameters = @{ResourceGroup=@{name='storage_rg';location='westus2'}}

# Create the new blueprint assignment
$bpAssignment = New-AzBlueprintAssignment -Name 'my-blueprint-assignment' -Blueprint $bpDefinition `
    -SubscriptionId '{subId}' -Location 'westus2' -Lock AllResourcesReadOnly `
    -Parameter $bpParameters -ResourceGroupParameter $bpRGParameters
```

The example output for creating a blueprint assignment looks like this:

```
Name           : my-blueprint-assignment
Id             : /subscriptions/{subId}/providers/Microsoft.Blueprint/blueprintAssi
               : gnments/my-blueprint-assignment
Scope          : /subscriptions/{subId}
LastModified   : 2019-03-13
LockMode       : AllResourcesReadOnly
ProvisioningState : Creating
Parameters     : {storageAccount_storageAccountType}
ResourceGroups : ResourceGroup
```

Example 2: Use a JSON assignment definition file

The following example creates nearly the same assignment as [Example 1](#). Instead of passing parameters to the cmdlet, the example shows use of a JSON assignment definition file and the **AssignmentFile** parameter. Additionally, the **excludedPrincipals** property is configured as part of **locks**. There isn't a PowerShell

parameter for **excludedPrincipals** and the property can only be configured by setting it through the JSON assignment definition file.

```
{
  "identity": {
    "type": "SystemAssigned"
  },
  "location": "westus2",
  "properties": {
    "description": "Assignment of the 101-blueprint-definition-subscription",
    "blueprintId": "/subscriptions/{subId}/providers/Microsoft.Blueprint/blueprints/101-blueprints-definition-subscription",
    "locks": {
      "mode": "AllResourcesReadOnly",
      "excludedPrincipals": [
        "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
        "38833b56-194d-420b-90ce-cff578296714"
      ]
    },
    "parameters": {
      "storageAccount_storageAccountType": {
        "value": "Standard_GRS"
      }
    },
    "resourceGroups": {
      "ResourceGroup": {
        "name": "storage_rg",
        "location": "westus2"
      }
    }
  }
}
```

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Create the new blueprint assignment
$bpAssignment = New-AzBlueprintAssignment -Name 'my-blueprint-assignment' -SubscriptionId '{subId}' `
  -AssignmentFile '.\assignment.json'
```

For an example of the JSON assignment definition file for a user-assigned managed identity, see the request body in [Example: Assignment with user-assigned managed identity](#) for REST API.

Update blueprint assignments

Sometimes it's necessary to update a blueprint assignment that has already been created. The

`Set-AzBlueprintAssignment` cmdlet handles this action. The cmdlet takes most of the same parameters that the `New-AzBlueprintAssignment` cmdlet does, allowing anything that was set on the assignment to be updated. The exceptions are the *Name*, *Blueprint*, and *SubscriptionId*. Only the values provided are updated.

To understand what happens when updating a blueprint assignment, see [rules for updating assignments](#).

- **Name** [required]
 - Specifies the name of the blueprint assignment to update
 - Used to locate the assignment to update, not to change the assignment
- **Blueprint** [required]
 - Specifies the blueprint definition of the blueprint assignment
 - Use `Get-AzBlueprint` to get the reference object
 - Used to locate the assignment to update, not to change the assignment

- **Location** (optional)
 - Specifies the region for the system-assigned managed identity and subscription deployment object to be created in
- **Subscription** (optional)
 - Specifies the subscription the assignment is deployed to
 - If not provided, defaults to the current subscription context
 - Used to locate the assignment to update, not to change the assignment
- **Lock** (optional)
 - Defines the [blueprint resource locking](#) to use for deployed resources
 - Supported options: *None*, *AllResourcesReadOnly*, *AllResourcesDoNotDelete*
- **SystemAssignedIdentity** (optional)
 - Select to create a system-assigned managed identity for the assignment and to deploy the resources
 - Default for the "identity" parameter set
 - Can't be used with **UserAssignedIdentity**
- **UserAssignedIdentity** (optional)
 - Specifies the user-assigned managed identity to use for the assignment and to deploy the resources
 - Part of the "identity" parameter set
 - Can't be used with **SystemAssignedIdentity**
- **Parameter** (optional)
 - A [hash table](#) of key/value pairs for setting [dynamic parameters](#) on the blueprint assignment
 - Default for a dynamic parameter is the **defaultValue** in the definition
 - If a parameter isn't provided and has no **defaultValue**, the parameter isn't optional

NOTE

Parameter doesn't support secureStrings.

- **ResourceGroupParameter** (optional)
 - A [hash table](#) of resource group artifacts
 - Each resource group artifact placeholder has key/value pairs for dynamically setting **Name** and **Location** on that resource group artifact
 - If a resource group parameter isn't provided and has no **defaultValue**, the resource group parameter isn't optional

The following example updates the assignment of version '1.1' of the 'my-blueprint' blueprint definition fetched with `Get-AzBlueprint` by changing the lock mode:

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get version '1.1' of the blueprint definition in the specified subscription
$bpDefinition = Get-AzBlueprint -SubscriptionId '{subId}' -Name 'my-blueprint' -Version '1.1'

# Update the existing blueprint assignment
$bpAssignment = Set-AzBlueprintAssignment -Name 'my-blueprint-assignment' -Blueprint $bpDefinition `
  -SubscriptionId '{subId}' -Lock AllResourcesDoNotDelete
```

The example output for creating a blueprint assignment looks like this:

```
Name           : my-blueprint-assignment
Id             : /subscriptions/{subId}/providers/Microsoft.Blueprint/blueprintAssi
               gnments/my-blueprint-assignment
Scope          : /subscriptions/{subId}
LastModified   : 2019-03-13
LockMode       : AllResourcesDoNotDelete
ProvisioningState : Updating
Parameters     : {storageAccount_storageAccountType}
ResourceGroups : ResourceGroup
```

Remove blueprint assignments

When it's time for a blueprint assignment to be removed, the `Remove-AzBlueprintAssignment` cmdlet handles this action. The cmdlet takes either **Name** or **InputObject** to specify which blueprint assignment to remove.

SubscriptionId is *required* and must be provided in all cases.

The following example fetches an existing blueprint assignment with `Get-AzBlueprintAssignment` and then removes it from the specific subscription represented as `{subId}`:

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get the blueprint assignment in the specified subscription
$blueprintAssignment = Get-AzBlueprintAssignment -Name 'Assignment-lock-resource-groups'

# Remove the existing blueprint assignment
Remove-AzBlueprintAssignment -InputObject $blueprintAssignment -SubscriptionId '{subId}'
```

Code example

Bringing all the steps together, the following example gets the blueprint definition, then creates, updates, and removes a blueprint assignment in the specific subscription represented as `{subId}`:

```

# Login first with Connect-AzAccount if not using Cloud Shell

#region GetBlueprint
# Get version '1.1' of the blueprint definition in the specified subscription
$bpDefinition = Get-AzBlueprint -SubscriptionId '{subId}' -Name 'my-blueprint' -Version '1.1'
#endregion

#region CreateAssignment
# Create the hash table for Parameters
$bpParameters = @{storageAccount_storageAccountType='Standard_GRS'}

# Create the hash table for ResourceGroupParameters
# ResourceGroup is the resource group artifact placeholder name
$bpRGParameters = @{ResourceGroup=@{name='storage_rg';location='westus2'}}

# Create the new blueprint assignment
$bpAssignment = New-AzBlueprintAssignment -Name 'my-blueprint-assignment' -Blueprint $bpDefinition `
    -SubscriptionId '{subId}' -Location 'westus2' -Lock AllResourcesReadOnly `
    -Parameter $bpParameters -ResourceGroupParameter $bpRGParameters
#endregion CreateAssignment

# Wait for the blueprint assignment to finish deployment prior to the next steps

#region UpdateAssignment
# Update the existing blueprint assignment
$bpAssignment = Set-AzBlueprintAssignment -Name 'my-blueprint-assignment' -Blueprint $bpDefinition `
    -SubscriptionId '{subId}' -Lock AllResourcesDoNotDelete
#endregion UpdateAssignment

# Wait for the blueprint assignment to finish deployment prior to the next steps

#region RemoveAssignment
# Remove the existing blueprint assignment
Remove-AzBlueprintAssignment -InputObject $bpAssignment -SubscriptionId '{subId}'
#endregion

```

Next steps

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).

Import and export blueprint definitions with PowerShell

4/30/2021 • 3 minutes to read • [Edit Online](#)

Azure Blueprints can be fully managed through Azure portal. As organizations advance in their use of Azure Blueprints, they should start thinking of blueprint definitions as managed code. This concept is often referred to as Infrastructure as Code (IaC). Treating your blueprint definitions as code offers additional advantages beyond what Azure portal offers. These benefits include:

- Sharing blueprint definitions
- Backing up your blueprint definitions
- Reusing blueprint definitions in different tenants or subscriptions
- Placing the blueprint definitions in source control
 - Automated testing of blueprint definitions in test environments
 - Support of continuous integration and continuous deployment (CI/CD) pipelines

Whatever your reasons, managing your blueprint definitions as code has benefits. This article shows how to use the `Import-AzBlueprintWithArtifact` and `Export-AzBlueprintWithArtifact` commands in the [Az.Blueprint](#) module.

Prerequisites

This article assumes a moderate working knowledge of Azure Blueprints. If you haven't done so yet, work through the following articles:

- [Create a blueprint in the portal](#)
- Read about [deployment stages](#) and [the blueprint lifecycle](#)
- [Creating](#) and [managing](#) blueprint definitions and assignments with PowerShell

If it isn't already installed, follow the instructions in [Add the Az.Blueprint module](#) to install and validate the [Az.Blueprint](#) module from the PowerShell Gallery.

Folder structure of a blueprint definition

Before looking at exporting and importing blueprints, let's look at how the files that make up the blueprint definition are structured. A blueprint definition should be stored in its own folder.

IMPORTANT

If no value is passed to the **Name** parameter of the `Import-AzBlueprintWithArtifact` cmdlet, the name of the folder the blueprint definition is stored in is used.

Along with the blueprint definition, which must be named `blueprint.json`, are the artifacts that the blueprint definition is composed of. Each artifact must be in the subfolder named `artifacts`. Put together, the structure of your blueprint definition as JSON files in folders should look as follows:

```
.
|
|- MyBlueprint/ _____ # Root folder name becomes default name of blueprint definition
|   |- blueprint.json _____ # The blueprint definition. Fixed name.
|
|   |- artifacts/ _____ # Subfolder for all blueprint artifacts. Fixed name.
|       |- artifact.json _____ # Blueprint artifact as JSON file. Artifact named from file.
|       |- ...
|       |- more-artifacts.json
```

Export your blueprint definition

The steps to exporting your blueprint definition are straightforward. Exporting the blueprint definition can be useful for sharing, backup, or placing into source control.

- **Blueprint** [required]
 - Specifies the blueprint definition
 - Use `Get-AzBlueprint` to get the reference object
- **OutputPath** [required]
 - Specifies the path to save the blueprint definition JSON files to
 - The output files are in a subfolder with the name of the blueprint definition
- **Version** (optional)
 - Specifies the version to output if the **Blueprint** reference object contains references to more than one version.

1. Get a reference to the blueprint definition to export from the subscription represented as `{subId}`:

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get version '1.1' of the blueprint definition in the specified subscription
$bpDefinition = Get-AzBlueprint -SubscriptionId '{subId}' -Name 'MyBlueprint' -Version '1.1'
```

2. Use the `Export-AzBlueprintWithArtifact` cmdlet to export the specified blueprint definition:

```
Export-AzBlueprintWithArtifact -Blueprint $bpDefinition -OutputPath 'C:\Blueprints'
```

Import your blueprint definition

Once you have either an [exported blueprint definition](#) or have a manually created blueprint definition in the [required folder structure](#), you can import that blueprint definition to a different management group or subscription.

For examples of built-in blueprint definitions, see the [Azure Blueprint GitHub repo](#).

- **Name** [required]
 - Specifies the name for the new blueprint definition
- **InputPath** [required]
 - Specifies the path to create the blueprint definition from
 - Must match the [required folder structure](#)
- **ManagementGroupId** (optional)
 - The management group ID to save the blueprint definition to if not the current context default

- Either **ManagementGroupId** or **SubscriptionId** must be specified
- **SubscriptionId** (optional)
 - The subscription ID to save the blueprint definition to if not the current context default
 - Either **ManagementGroupId** or **SubscriptionId** must be specified

1. Use the `Import-AzBlueprintWithArtifact` cmdlet to import the specified blueprint definition:

```
# Login first with Connect-AzAccount if not using Cloud Shell

Import-AzBlueprintWithArtifact -Name 'MyBlueprint' -ManagementGroupId 'DevMG' -InputPath
'C:\Blueprints\MyBlueprint'
```

Once the blueprint definition is imported, [assign it with PowerShell](#).

For information about creating advanced blueprint definitions, see the following articles:

- Use [static and dynamic parameters](#).
- Customize the [blueprint sequencing order](#).
- Protect deployments with [blueprint resource locking](#).
- [Manage Blueprints as Code](#).

Next steps

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).

How to update an existing blueprint assignment

5/3/2021 • 2 minutes to read • [Edit Online](#)

When a blueprint is assigned, the assignment can be updated. There are several reasons for updating an existing assignment, including:

- Add or remove [resource locking](#)
- Change the value of [dynamic parameters](#)
- Upgrade the assignment to a newer **Published** version of the blueprint

Updating assignments

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select **Assigned blueprints** from the page on the left.
3. In the list of blueprints, select the blueprint assignment. Then use the **Update assignment** button OR select and hold (or right-click) the blueprint assignment and select **Update assignment**.

Home > Blueprints - Assigned blueprints > Assignment-MyBlueprint

Assignment-MyBlueprint

Blueprint assignment

Update assignment Unassign blueprint View activity log Refresh

✓ Assignment succeeded!

Assigned subscription name Contoso	Blueprint MyBlueprint
Assigned subscription {subscriptionId}	Latest assignment status Succeeded
	Lock mode None

Assignment operation
Version 'v1.0', assigned on 4/23/2019. (Succeeded)

Managed resources

RESOURCE	LOCK STATE	RESOURCE TYPE
ResourceGroupOne	Not locked	Resource group

4. The **Assign blueprint** page loads pre-filled with all values from the original assignment. You can change the **blueprint definition version**, the **Lock Assignment** state, and any of the dynamic parameters that exist on the blueprint definition. Select **Assign** when done making changes.
5. On the updated assignment details page, see the new status. In this example, we added **Locking** to the assignment.

Home > Blueprints - Assigned blueprints > Assignment-MyBlueprint

Assignment-MyBlueprint

Blueprint assignment

[Update assignment](#)
[Unassign blueprint](#)
[View activity log](#)
[Refresh](#)

✓ Assignment succeeded!

Assigned subscription name Contoso	Blueprint MyBlueprint
Assigned subscription {subscriptionId}	Latest assignment status Succeeded
	Lock mode All resources - read-only

Assignment operation
Version 'v1.0', assigned on 4/23/2... ▼

Managed resources

RESOURCE	LOCK STATE	RESOURCE TYPE
ResourceGroupOne	Cannot edit / delete	Resource group

6. Explore details about other **Assignment operations** using the dropdown list. The table of **Managed resources** updates by selected assignment operation.

Assignment operation

Version 'v1.0', assigned on 4/23/2... ^

- Version 'v1.0', assigned on 4/23/2019. (Succeeded)
- Version 'v1.0', assigned on 4/23/2019. (Succeeded)

Rules for updating assignments

The deployment of the updated assignments follows a few important rules. These rules determine what happens to already deployed resources. The requested change and the type of artifact resource being deployed or updated determine which actions are taken.

- Role Assignments
 - If the role or the role assignee (user, group, or app) changes, a new role assignment is created. Role assignments previously deployed are left in place.
- Policy Assignments
 - If the parameters of the policy assignment are changed, the existing assignment is updated.
 - If the definition of the policy assignment is changed, a new policy assignment is created. Policy assignments previously deployed are left in place.
 - If the policy assignment artifact is removed from the blueprint, deployed policy assignments are left in place.
- Azure Resource Manager templates (ARM templates)
 - The template is processed through Resource Manager as a **PUT**. As each resource type handles this action differently, review the documentation for each included resource to determine the impact of this action when run by Blueprints.

Possible errors on updating assignments

When updating assignments, it's possible to make changes that break when executed. An example is changing the location of a resource group after it has already been deployed. Any change that are supported by [Resource](#)

[Manager](#) can be made, but any change that would result in an error through Resource Manager will also result in the failure of the assignment.

There's no limit on how many times an assignment can be updated. If an error occurs, determine the error and make another update to the assignment. Example error scenarios:

- A bad parameter
- An already existing object
- A change not supported by Resource Manager

Next steps

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).

Configure your environment for a Blueprint Operator

4/30/2021 • 2 minutes to read • [Edit Online](#)

The management of your blueprint definitions and blueprint assignments can be assigned to different teams. It's common for an architect or governance team to be responsible for the lifecycle management of your blueprint definitions while an operations team is responsible for managing assignments of those centrally controlled blueprint definitions.

The **Blueprint Operator** built-in role is designed specifically for use in this type of scenario. The role allows for operations type teams to manage the assignment of the organizations blueprint definitions, but not the ability to modify them. Doing so requires some configuration in your Azure environment and this article explains the necessary steps.

Grant permission to the Blueprint Operator

The first step is to grant the **Blueprint Operator** role to the account or security group (recommended) that is going to be assigning blueprints. This action should be done at the highest level in the management group hierarchy that encompasses all of the management groups and subscriptions the operations team should have blueprint assignment access to. It's recommended to follow the principle of least privilege when granting these permissions.

1. (Recommended) [Create a security group and add members](#)
2. [Assign Azure role](#) of **Blueprint Operator** to the account or security group

User-assign managed identity

A blueprint definition can use either system-assigned or user-assigned managed identities. However, when using the **Blueprint Operator** role, the blueprint definition needs to be configured to use a user-assigned managed identity. Additionally, the account or security group being granted the **Blueprint Operator** role needs to be granted the **Managed Identity Operator** role on the user-assigned managed identity. Without this permission, blueprint assignments fail because of lack of permissions.

1. [Create a user-assigned managed identity](#) for use by an assigned blueprint.
2. Grant the user-assigned managed identity any roles or permissions required by the blueprint definition for the intended scope.
3. [Assign Azure role](#) of **Managed Identity Operator** to the account or security group. Scope the role assignment to the new user-assigned managed identity.
4. As the **Blueprint Operator**, [assign a blueprint](#) that uses the new user-assigned managed identity.

Next steps

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).

Troubleshoot errors using Azure Blueprints

5/3/2021 • 2 minutes to read • [Edit Online](#)

You may run into errors when creating, assigning, or removing blueprints. This article describes various errors that may occur and how to resolve them.

Finding error details

Many errors will be the result of assigning a blueprint to a scope. When an assignment fails, the blueprint provides details about the failed deployment. This information indicates the issue so that it can be fixed and the next deployment succeeds.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select **Assigned blueprints** from the page on the left and use the search box to filter the blueprint assignments to find the failed assignment. You can also sort the table of assignments by the **Provisioning State** column to see all failed assignments grouped together.
3. Select the blueprint with the *Failed* status or right-click and select **View assignment details**.
4. A red banner warning that the assignment has failed is at the top of the blueprint assignment page. Select anywhere on the banner to get more details.

It's common for the error to be caused by an artifact and not the blueprint as a whole. If an artifact creates a Key Vault and Azure Policy prevents Key Vault creation, the entire assignment will fail.

General errors

Scenario: Policy Violation

Issue

The template deployment failed because of policy violation.

Cause

A policy may conflict with the deployment for the following reasons:

- The resource being created is restricted by policy (commonly SKU or location restrictions)
- The deployment is setting fields that are configured by policy (common with tags)

Resolution

Change the blueprint so it doesn't conflict with the policies in the error details. If this change isn't possible, an alternative option is to have the scope of the policy assignment changed so the blueprint is no longer in conflict with the policy.

Scenario: Blueprint parameter is a function

Issue

Blueprint parameters that are functions are processed before being passed to artifacts.

Cause

Passing a blueprint parameter that uses a function, such as `[resourceGroup().tags.myTag]`, to an artifact results in the processed outcome of the function being set on the artifact instead of the dynamic function.

Resolution

To pass a function through as a parameter, escape the entire string with `[]` such that the blueprint parameter

looks like `[[resourceGroup().tags.myTag]]`. The escape character causes Blueprints to treat the value as a string when processing the blueprint. The Blueprints service then places the function on the artifact allowing it to be dynamic as expected. For more information, see [Syntax and expressions in Azure Resource Manager templates](#).

Delete errors

Scenario: Assignment deletion timeout

Issue

Deletion of a blueprint assignment doesn't complete.

Cause

A blueprint assignment may become stuck in a non-terminal state when deleted. This state is caused when resources created by the blueprint assignment are still pending deletion or don't return a status code to Azure Blueprints.

Resolution

Blueprint assignments in a non-terminal state are automatically marked **Failed** after a *six-hour* timeout. Once the timeout has adjusted the state of the blueprint assignment, the delete can be retried.

Next steps

If you didn't see your problem or are unable to solve your issue, visit one of the following channels for more support:

- Get answers from Azure experts through [Azure Forums](#).
- Connect with [@AzureSupport](#) - the official Microsoft Azure account for improving customer experience by connecting the Azure community to the right resources: answers, support, and experts.
- If you need more help, you can file an Azure support incident. Go to the [Azure support site](#) and select **Get Support**.

Functions for use with Azure Blueprints

5/3/2021 • 5 minutes to read • [Edit Online](#)

Azure Blueprints provides functions making a blueprint definition more dynamic. These functions are for use with blueprint definitions and blueprint artifacts. An Azure Resource Manager Template (ARM template) artifact supports the full use of Resource Manager functions in addition to getting a dynamic value through a blueprint parameter.

The following functions are supported:

- [artifacts](#)
- [concat](#)
- [parameters](#)
- [resourceGroup](#)
- [resourceGroups](#)
- [subscription](#)

artifacts

```
artifacts(artifactName)
```

Returns an object of properties populated with that blueprint artifacts outputs.

NOTE

The `artifacts()` function can't be used from inside an ARM Template. The function can only be used in the blueprint definition JSON or in the artifact JSON when managing the blueprint with Azure PowerShell or REST API as part of [Blueprints-as-code](#).

Parameters

PARAMETER	REQUIRED	TYPE	DESCRIPTION
artifactName	Yes	string	The name of a blueprint artifact.

Return value

An object of output properties. The **outputs** properties are dependent on the type of blueprint artifact being referenced. All types follow the format:

```
{
  "outputs": {collectionOfOutputProperties}
}
```

Policy assignment artifact

```
{
  "outputs": {
    "policyAssignmentId": "{resourceId-of-policy-assignment}",
    "policyAssignmentName": "{name-of-policy-assignment}",
    "policyDefinitionId": "{resourceId-of-policy-definition}",
  }
}
```

ARM template artifact

The **outputs** properties of the returned object are defined within the ARM template and returned by the deployment.

Role assignment artifact

```
{
  "outputs": {
    "roleAssignmentId": "{resourceId-of-role-assignment}",
    "roleDefinitionId": "{resourceId-of-role-definition}",
    "principalId": "{principalId-role-is-being-assigned-to}",
  }
}
```

Example

An ARM template artifact with the ID *myTemplateArtifact* containing the following sample output property:

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  ...
  "outputs": {
    "myArray": {
      "type": "array",
      "value": ["first", "second"]
    },
    "myString": {
      "type": "string",
      "value": "my string value"
    },
    "myObject": {
      "type": "object",
      "value": {
        "myProperty": "my value",
        "anotherProperty": true
      }
    }
  }
}
```

Some examples of retrieving data from the *myTemplateArtifact* sample are:

EXPRESSION	TYPE	VALUE
[artifacts("myTemplateArtifact").outputs.myArray]	Array	["first", "second"]
[artifacts("myTemplateArtifact").outputs.myString]	String	"first"
[artifacts("myTemplateArtifact").outputs.myObject]	Object	{ "myProperty": "my value", "anotherProperty": true }
[artifacts("myTemplateArtifact").outputs.myObject.myProperty]	String	"my value"
[artifacts("myTemplateArtifact").outputs.myObject.anotherProperty]	Boolean	true

EXPRESSION	TYPE	VALUE
[artifacts("myTemplateArtifact").outputs.myObject]	Object	{ "myproperty": "my value", "anotherProperty": true }
[artifacts("myTemplateArtifact").outputs.myObject.myProperty]	String	"my value"
[artifacts("myTemplateArtifact").outputs.myObject.anotherProperty]	Boolean	True

concat

```
concat(string1, string2, string3, ...)
```

Combines multiple string values and returns the concatenated string.

Parameters

PARAMETER	REQUIRED	TYPE	DESCRIPTION
string1	Yes	string	The first value for concatenation.
additional arguments	No	string	Additional values in sequential order for concatenation

Return value

A string of concatenated values.

Remarks

The Azure Blueprint function differs from the ARM template function in that it only works with strings.

Example

```
concat(parameters('organizationName'), '-vm')
```

parameters

```
parameters(parameterName)
```

Returns a blueprint parameter value. The specified parameter name must be defined in the blueprint definition or in blueprint artifacts.

Parameters

PARAMETER	REQUIRED	TYPE	DESCRIPTION
parameterName	Yes	string	The name of the parameter to return.

Return value

The value of the specified blueprint or blueprint artifact parameter.

Remarks

The Azure Blueprint function differs from the ARM template function in that it only works with blueprint parameters.

Example

Define parameter *principalIds* in the blueprint definition:

```
{
  "type": "Microsoft.Blueprint/blueprints",
  "properties": {
    ...
    "parameters": {
      "principalIds": {
        "type": "array",
        "metadata": {
          "displayName": "Principal IDs",
          "description": "This is a blueprint parameter that any artifact can reference. We'll display these descriptions for you in the info bubble. Supply principal IDs for the users,groups, or service principals for the Azure role assignment.",
          "strongType": "PrincipalId"
        }
      }
    },
    ...
  }
}
```

Then use *principalIds* as the argument for `parameters()` in a blueprint artifact:

```
{
  "type": "Microsoft.Blueprint/blueprints/artifacts",
  "kind": "roleAssignment",
  ...
  "properties": {
    "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
    "principalIds": "[parameters('principalIds')]",
    ...
  }
}
```

resourceGroup

`resourceGroup()`

Returns an object that represents the current resource group.

Return value

The returned object is in the following format:

```
{
  "name": "{resourceGroupName}",
  "location": "{resourceGroupLocation}",
}
```

Remarks

The Azure Blueprint function differs from the ARM template function. The `resourceGroup()` function can't be used in a subscription level artifact or the blueprint definition. It can only be used in blueprint artifacts that are part of a resource group artifact.

A common use of the `resourceGroup()` function is to create resources in the same location as the resource group artifact.

Example

To use the resource group's location, set in either the blueprint definition or during assignment, as the location for another artifact, declare a resource group placeholder object in your blueprint definition. In this example, *NetworkingPlaceholder* is the name of the resource group placeholder.

```
{
  "type": "Microsoft.Blueprint/blueprints",
  "properties": {
    ...
    "resourceGroups": {
      "NetworkingPlaceholder": {
        "location": "eastus"
      }
    }
  }
}
```

Then use the `resourceGroup()` function in the context of a blueprint artifact that is targeting a resource group placeholder object. In this example, the template artifact is deployed into the *NetworkingPlaceholder* resource group and provides parameter *resourceLocation* dynamically populated with the *NetworkingPlaceholder* resource group location to the template. The location of the *NetworkingPlaceholder* resource group could have been statically defined on the blueprint definition or dynamically defined during assignment. In either case, the template artifact is provided that information as a parameter and uses it to deploy the resources to the correct location.

```
{
  "type": "Microsoft.Blueprint/blueprints/artifacts",
  "kind": "template",
  "properties": {
    "template": {
      ...
    },
    "resourceGroup": "NetworkingPlaceholder",
    ...
    "parameters": {
      "resourceLocation": {
        "value": "[resourceGroup().location]"
      }
    }
  }
}
```

resourceGroups

`resourceGroups(placeholderName)`

Returns an object that represents the specified resource group artifact. Unlike `resourceGroup()`, which requires context of the artifact, this function is used to get the properties of a specific resource group placeholder when not in context of that resource group.

Parameters

PARAMETER	REQUIRED	TYPE	DESCRIPTION
placeholderName	Yes	string	The placeholder name of the resource group artifact to return.

Return value

The returned object is in the following format:

```
{
  "name": "{resourceGroupName}",
  "location": "{resourceGroupLocation}",
}
```

Example

To use the resource group's location, set in either the blueprint definition or during assignment, as the location for another artifact, declare a resource group placeholder object in your blueprint definition. In this example, *NetworkingPlaceholder* is the name of the resource group placeholder.

```
{
  "type": "Microsoft.Blueprint/blueprints",
  "properties": {
    ...
    "resourceGroups": {
      "NetworkingPlaceholder": {
        "location": "eastus"
      }
    }
  }
}
```

Then use the `resourceGroups()` function from the context of any blueprint artifact to get a reference to the resource group placeholder object. In this example, the template artifact is deployed outside the *NetworkingPlaceholder* resource group and provides parameter *artifactLocation* dynamically populated with the *NetworkingPlaceholder* resource group location to the template. The location of the *NetworkingPlaceholder* resource group could have been statically defined on the blueprint definition or dynamically defined during assignment. In either case, the template artifact is provided that information as a parameter and uses it to deploy the resources to the correct location.

```
{
  "kind": "template",
  "properties": {
    "template": {
      ...
    },
    ...
    "parameters": {
      "artifactLocation": {
        "value": "[resourceGroups('NetworkingPlaceholder').location]"
      }
    }
  },
  "type": "Microsoft.Blueprint/blueprints/artifacts",
  "name": "myTemplate"
}
```

subscription

`subscription()`

Returns details about the subscription for the current blueprint assignment.

Return value

The returned object is in the following format:

```
{
  "id": "/subscriptions/{subscriptionId}",
  "subscriptionId": "{subscriptionId}",
  "tenantId": "{tenantId}",
  "displayName": "{name-of-subscription}"
}
```

Example

Use the subscription's display name and the `concat()` function to create a naming convention passed as parameter *resourceName* to the template artifact.

```
{
  "kind": "template",
  "properties": {
    "template": {
      ...
    },
    ...
    "parameters": {
      "resourceName": {
        "value": "[concat(subscription().displayName, '-vm')]"
      }
    }
  },
  "type": "Microsoft.Blueprint/blueprints/artifacts",
  "name": "myTemplate"
}
```

Next steps

- Learn about the [blueprint lifecycle](#).
- Understand how to use [static and dynamic parameters](#).
- Learn to customize the [blueprint sequencing order](#).
- Find out how to make use of [blueprint resource locking](#).
- Learn how to [update existing assignments](#).
- Resolve issues during the assignment of a blueprint with [general troubleshooting](#).