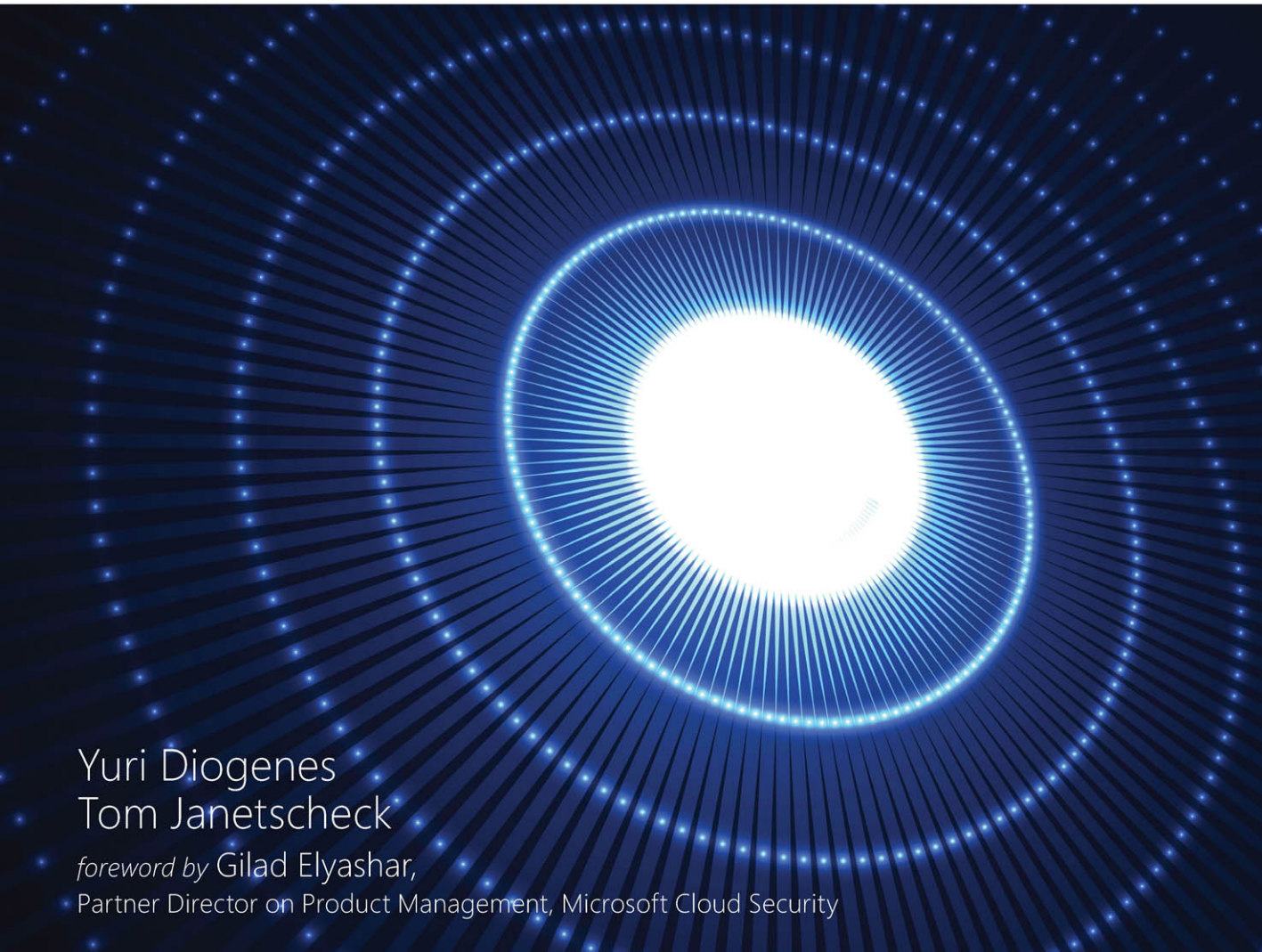
Microsoft

Microsoft Defender for Cloud



Yuri Diogenes
Tom Janetscheck

foreword by Gilad Elyashar,
Partner Director on Product Management, Microsoft Cloud Security

Microsoft

Microsoft Defender for Cloud

Yuri Diogenes and Tom Janetscheck

Configure auto-provisioning at scale

As you learned earlier in this chapter, when configuring auto-provisioning from the Defender for Cloud portal, the back-end will create policy assignments on a particular subscription. Also, for a Log Analytics agent on Azure VMs, there are built-in policy definitions, too. With that being said, all you need to do is assign these policies to your management group instead of subscriptions, as explained earlier in this chapter.

Chapter 4

Policy management

Policies, guardrails, and definitions. Many ambiguous terms are used synonymously when describing the same topic: a set of rules used to define the boundaries in which an environment can be configured. Since Microsoft Defender for Cloud's beginnings, the Cloud Security Posture Management capability has been built upon Azure Policy, which is a Microsoft Azure service used to technically define a company's governance concept.

In this chapter, you will learn about policies and assessments within the scope of Microsoft Defender for Cloud, and you'll learn about regulatory compliance standards and how to customize the experience in hybrid and multi-cloud environments.

Introduction to Azure Policy

We remember the days when IT environments were made up of server racks within office rooms or corporate datacenters. In those days, IT security mainly meant physical security and security in operations. It was a reactive process that could easily be done as a manual task.

Today, with cloud computing being the most popular operations model, we are facing ever-changing environments, which is both a benefit and a challenge. Cloud environments are meant to be solution-focused instead of resource-focused, which means that once your solution needs more compute power, there ideally is a process in place to spin up new machines once needed (and remove them if they're not needed). Or, if you move one abstraction layer higher, you don't even care about infrastructure resources because you are using PaaS (Platform as a Service) offerings. You can easily create new Storage Accounts or remove Azure Key Vaults from your environments within seconds. But, from an operational perspective, it is impossible to keep track of all these dynamic changes manually.

It is well known that there is no such thing as total security, which means there will always be a chance of being successfully attacked. But, more importantly, without rules, there is no security *at all*! Therefore, rules are important not only for security but also for compliance and governance purposes. In real life, rules are called *laws* defined by

a government, and there is an instance to control and enforce these laws, called the *police*. From a technical perspective within Microsoft Azure, this is when Azure Policy comes into play. Azure Policy is that instance to control and enforce the rules that an authority in your company has defined.

Azure Policy is a service that consists of *definitions* and *assignments*, both of which can apply to *policies* and *initiatives*.

1. **Definitions** Definitions are the configurations that you set up within a policy or initiative. They can be referred to as a *template*, which can later be applied to resources within your environment. Definitions can be compared with your current configuration, and any resources that do not meet the requirements of your policy are determined to be out of compliance. You can then focus on the out-of-compliance assets and bring them into compliance. All policy definitions are created in JavaScript Object Notation, or JSON.
2. **Assignments** Assignments are definitions that are assigned to a specific scope within your Azure environment. This scope can vary from management groups, over subscriptions, and down to a single resource group. By default, an assignment will be inherited top-down, which means that if you assign a policy definition on a subscription, its settings will apply to all resources within the subscription. However, when creating the assignment, you can also exclude a particular scope from applying your policy or initiative definition. For example, you might use definitions that are supposed to apply to most subscriptions within your Azure environment, but not for particular resources. Let's say you have test resources in one or several resource groups. In this case, you could create an assignment on your management group and exclude this particular resource group so resources within that scope would not apply the definition's settings.

When creating a new definition, you need to be careful with the definition location, which can either be a management group or a subscription. The location will determine to what scope the definition can be assigned later. For example, if you create the definition on a management group, you can assign it to this management group and all child management groups and subscriptions, whereas if you create a definition on a subscription, you can only assign it to this particular subscription and its resources and resource groups.

An *initiative definition* is a collection of *policy definitions* that is tailored toward achieving a singular overarching goal. Initiative definitions simplify the management and assignment of policy definitions by grouping a set of policies into a single item. Each policy definition contains a policy rule that defines in which case the policy definition will assess a resource, and what effect the policy assessment will have. Figure 4-1 shows these components.

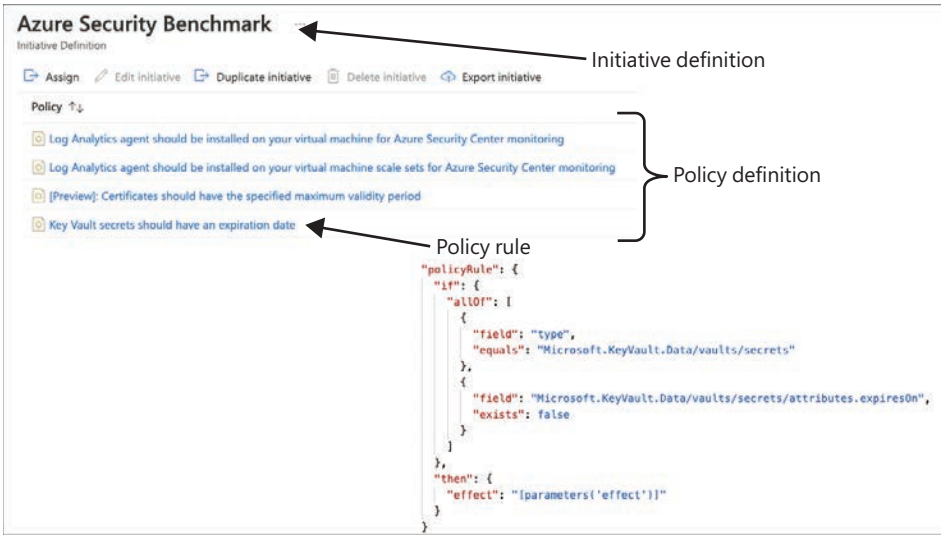


FIGURE 4-1 Azure Policy components

> ***IMPORTANT*** **When working with Azure Policy and automation, you will not find the word *initiative*. You should look for *policy set* instead.**

A policy definition can have different effects to the scope it is assigned to. The `append` mode is used to add additional fields to a resource when it is created or updated. For example, you can use `append` to add a list of allowed IP addresses to a storage resource. A policy definition in `audit` mode will report resources that are non-compliant regarding the settings within your definition. For example, if you have an internal agreement that organizational resources are only deployed to Azure regions within Europe, you can use an `audit` policy to report resources that are deployed in a US region. A similar effect is `auditifnotexists`, which will report resources that do not have a particular configuration or setting. For example, you would use `auditifnotexists` if you want to see resources that do not have a particular tag configured.

If you configure a definition in `deployifnotexists` (DINE) mode, once you deploy a resource, a particular setting or configuration is automatically remediated if it has not already been defined when configuring the resource to be deployed. For example, you can use a DINE policy to ensure that the Azure Monitoring Agent is installed on all VMs created within your Azure environment.

A definition that is configured in `deny` mode will prevent the deployment of resources that are non-compliant regarding a particular setting. In the first example with the Azure

regions, you can use a `deny` policy to not only audit but also prevent the deployment of resources to a US region. Finally, there is the `modify` mode, which is used to add, update, or remove properties or tags on a resource when it is created or updated. This effect is commonly used to update tags on resources. Also, with `modify`, you can remediate existing resources using remediation tasks.

While having this core understanding of Azure Policy is important, you don't need to create any initiative or policy when using security policy integration with Azure Policy because Defender for Cloud will automatically create it for you. All security controls and recommendations are based on this default policy initiative, called Azure Security Benchmark, which is maintained by Microsoft. This initiative includes a curation of `audit` and `auditifnotexists` policies that are automatically assigned to your subscriptions. If there are changes to existing policy definitions, definitions are removed, or new policy definitions are created and added to the Azure Security Benchmark initiative, these changes will automatically apply to Microsoft Defender for Cloud.

You can also leverage Azure Policy for deployment, remediation, and protection at scale. So, Azure Policy is not only a random governance tool within the Microsoft Azure ecosystem, but it's also an important service you need to understand to implement the best CSPM concept for your organization.

Policy exemptions

Policy exemptions (announced at Microsoft Ignite 2020) are an exciting new feature within the context of Azure Policy. Although it might seem similar to the exclusion scope you can define when assigning a definition, it is *way* more than that. With policy exemptions, you can exclude a management group, subscription, resource group, or a particular resource from an assignment. Additionally, you can configure an expiration date for the exemption or enter a justification for the exemption. You can select `waiver` as the exemption category if you decide to temporarily accept the non-compliance state of a resource, or you can select `mitigated` if the policy's intent was met through a different method or process.

> ***MORE INFO*** **To learn more about policy exemptions, see *https://docs.microsoft.com/en-us/azure/governance/policy/concepts/exemption-structure*.**

When you configure an exclusion scope, you need to do it within the assignment, and doing so is a static decision, whereas when you create a policy exemption, the policy assignment itself is not changed. As you can see in Figure 4-2, there is an **Exemptions** button in the left navigation pane within Azure Policy. This figure shows an exemption that has been created from within Defender for Cloud for the subscription's default assignment.

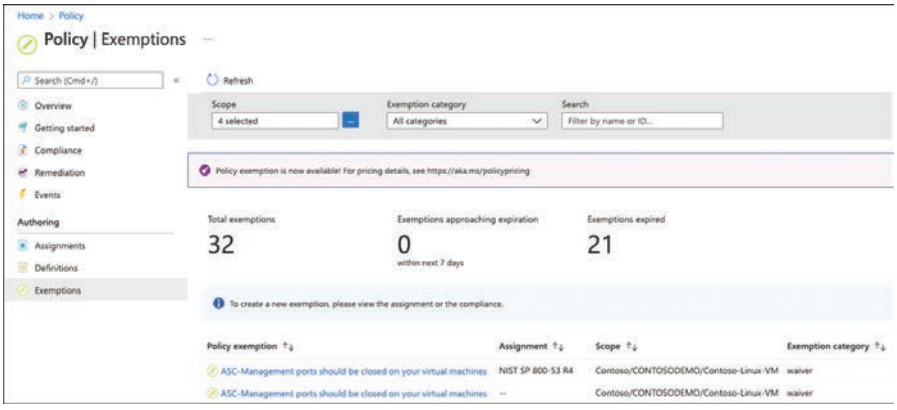


FIGURE 4-2 Policy exemption in the Azure Policy dashboard

You will learn more about how to create an exemption in Defender for Cloud in the next chapter, though you can also create policy exemptions directly from the Azure Policy dashboard. That is useful if you do not want to create an exemption for the Azure Security Benchmark policy initiative, but you want to do so for other policies that are not necessarily related to Defender for Cloud.

Follow these steps to create a new policy exemption:

1. Open the Azure portal and sign in with a user who has Resource Policy Contributor or Security Admin privileges.
2. In the search bar, type **Policy** and click the **Policy** service; the **Policy** blade appears, as shown in Figure 4-3.

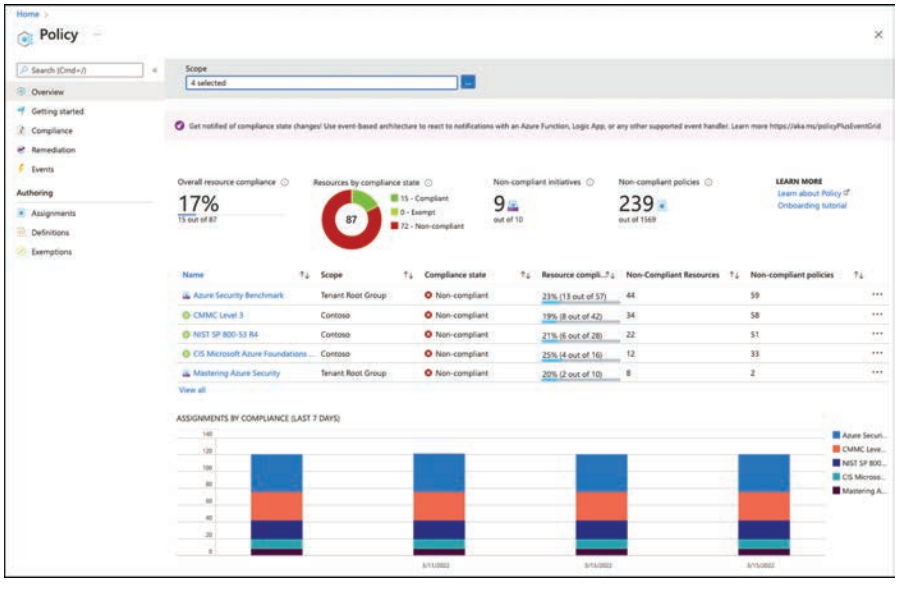


FIGURE 4-3 Azure Policy dashboard