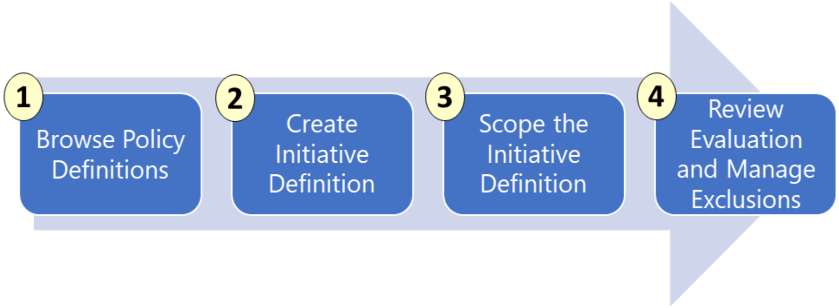
Manage Azure Governance

- Managing Subscription Policies
- Azure Blueprints
- Locking Resources
- Checking Resources Limits
- Resource Tags

Management Subscription Policies

- Azure Policy is a service in Azure that you use to create, assign and manage policy definitions.
- Policy definitions enforce different rules and actions over your resources, so those resources stay compliant with your corporate standards and service level agreements.
- Azure Policy does this by running an evaluation of your resources, scanning for those not compliant with the policy definitions you have. For example, you can have a policy to allow only certain type of virtual machines. Another requires that all resources have a particular tag. These policies are then evaluated when creating and updating resources.

To implement Azure Policies, you can follow these steps.


1
Browse Policy Definitions
2
Create Initiative Definition
3
Scope the Initiative Definition
4
Review Evaluation and Manage Exclusions

About Policy definition:

A Policy Definition expresses what to evaluate and what actions to take. Every policy definition has conditions under which it is enforced. And, it has an accompanying effect that takes place if the conditions are met.

- **Allowed Virtual Machine SKUs**: This policy enables you to specify a set of virtual machine SKUs that your organization can deploy.
- **Allowed Storage Account SKUs**: This policy definition has a set of conditions/rules that determine if a storage account that is being deployed is within a set of SKU sizes. Its action is to deny all servers that do not adhere to the set of defined SKU sizes.

- **Require SQL Server 12.0**: This policy definition has conditions/rules to ensure that all SQL servers use version 12.0. Its action is to deny all servers that do not meet these criteria.
- **Allowed Resource Type**: This policy definition has a set of conditions/rules to specify the resource types that your organization can deploy. Its action is to deny all resources that are not part of this defined list.
- **Allowed Locations**: This policy enables you to restrict the locations that your organization can specify when deploying resources. Its action is used to enforce your geo-compliance requirements.
- **Apply tag and its default value**: This policy applies a required tag and its default value, if it is not specified by the user.
- **Enforce tag and its value**: This policy enforces a required tag and its value to a resource.
- **Not allowed resource types**: This policy enables you to specify the resource types that your organization cannot deploy.

Step1: To view all Policy Definitions

Azure → All Services → Policy → **Definitions** → Filter: Search = Location → Select Allowed locations

Note the Definition (JSON)

Note: If you don't see what you need you can **add a Policy Definition**. The easiest way to do this is to Import a policy from GitHub. New Policy Definitions are added almost every day.

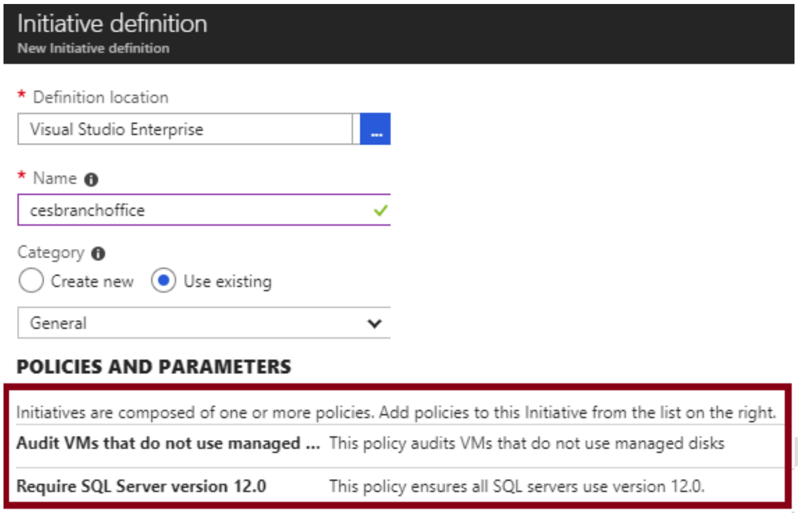
To Assign a Policy Definition to Subscription or Resource Group

Azure → All Services → Policy → Definitions → Select Any Definition → **Assign** → Select Subscription and Optionally Resource Group → Assign

About Initiative definition: An initiative definition **is collection of policy** definitions that are tailored towards achieving a singular goal.

Step 2: To create Initiative Definition

Azure → All Services → Policy → Definitions → **+Initiative definition**



Initiative definition
New Initiative definition

* Definition location
Visual Studio Enterprise

* Name
cesbranchoffice

Category
○ Create new ● Use existing

General

POLICIES AND PARAMETERS

Initiatives are composed of one or more policies. Add policies to this Initiative from the list on the right.

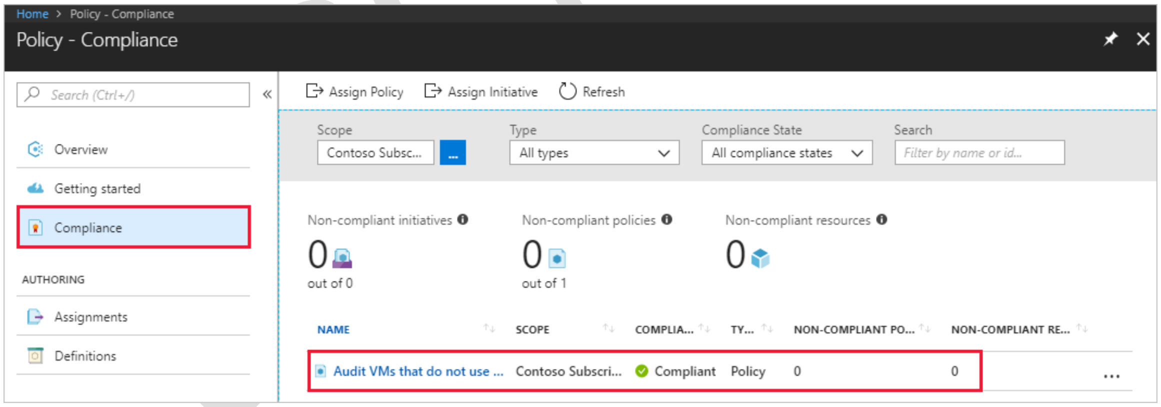
Audit VMs that do not use managed ...	This policy audits VMs that do not use managed disks
Require SQL Server version 12.0	This policy ensures all SQL servers use version 12.0.

To ASSIGN / SCOPE an Initiative Definition to Subscription or Resource Group

Azure → All Services → Policy → Definitions → Select Any Definition → **Assign** → Select Subscription and Optionally Resource Group → Assign

Step 4: Determine Compliance

Once your policy is in place you can use the Compliance blade to review non-compliant initiatives, non-compliant policies, and non-compliant resources.

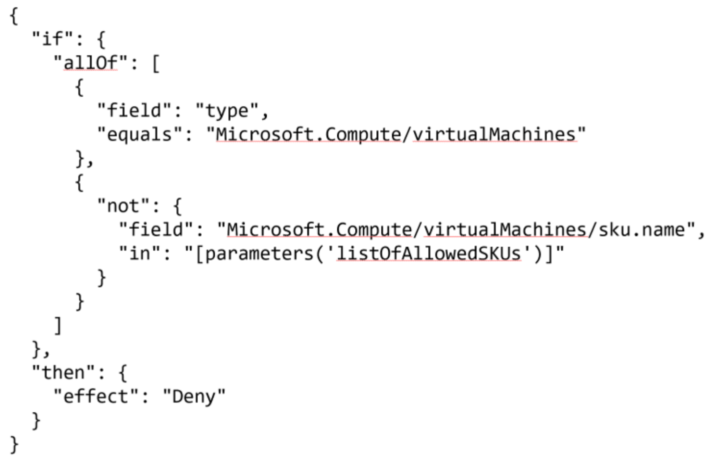


Scope: Contoso Subsc...
Type: All types
Compliance State: All compliance states
Search: Filter by name or id...

Non-compliant initiatives: 0 out of 0
Non-compliant policies: 0 out of 1
Non-compliant resources: 0

NAME	SCOPE	COMPLIA...	TY...	NON-COMPLIANT PO...	NON-COMPLIANT RE...
Audit VMs that do not use ...	Contoso Subscri...	✓ Compliant	Policy	0	0

✔ Policy evaluation happens about once an hour, which means that if you make changes to your policy definition and create a policy assignment then it will be re-evaluated over your resources within the hour.



```
{
  "if": {
    "allOf": [
      {
        "field": "type",
        "equals": "Microsoft.Compute/virtualMachines"
      },
      {
        "not": {
          "field": "Microsoft.Compute/virtualMachines/sku.name",
          "in": "[parameters('listOfAllowedSKUs')]"
        }
      }
    ]
  },
  "then": {
    "effect": "Deny"
  }
}
```

Azure Blueprints

Azure Blueprints is a declarative way to orchestrate the deployment of such artifacts as policy

- Role assignments
- Policy assignments
- Resource groups
- ARM templates

How is this different from ARM templates ?

Azure Policy vs. Azure Blueprints

Azure Policy

- Helps to enforce organizational standards and to assess compliance at-scale.
- Provides an aggregated view to evaluate the overall state of the environment.
- Helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources

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
- Makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance.

Lock Resources

- As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to **CanNotDelete** or **ReadOnly**.
- When you apply a lock at a parent scope, all resources within that scope inherit the same lock.
- Resource changes are restricted, but resource operations are not restricted. For example, a ReadOnly lock on a SQL Database prevents you from deleting or modifying the database, but it does not prevent you from creating, updating, or deleting data in the database.

Applying Locks using Portal

1. Settings blade for the resource, resource group, or subscription → Locks → + Add
2. Lock name = DatabaseServerLock, Lock type = **Delete**, Notes = "Prevent deleting the database server"
3. OK

Template:

The following example shows a template that creates a lock on a storage account. The storage account on which to apply the lock is provided as a parameter.

```
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
  "lockedResource": {
   "type": "string"
  }
 },
 "resources": [
  {
   "name": "[concat(parameters('lockedResource'), '/Microsoft.Authorization/myLock')]",
   "type": "Microsoft.Storage/storageAccounts/providers/locks",
   "apiVersion": "2015-01-01",
   "properties": {
    "level": "CannotDelete"
   }
```

```
    }
  ]
}
```

Using PowerShell

To lock a resource:

```
New-AzResourceLock -LockLevel CanNotDelete -LockName LockSite `
  -ResourceName examplesite -ResourceType Microsoft.Web/sites `
  -ResourceGroupName exampleresourcegroup
```

To lock a Resource Group

```
New-AzResourceLock -LockName LockGroup -LockLevel CanNotDelete `
  -ResourceGroupName exampleresourcegroup
```

To get all locks in a subscription

```
Get-AzResourceLock
```

To get all locks for a resource:

```
Get-AzResourceLock -ResourceName examplesite -ResourceType Microsoft.Web/sites `
  -ResourceGroupName exampleresourcegroup
```

To get all locks for a resource group

```
Get-AzResourceLock -ResourceGroupName exampleresourcegroup
```

Using Azure CLI:

```
az lock create --name LockSite --lock-type CanNotDelete \
  --resource-group exampleresourcegroup --resource-name examplesite \
  --resource-type Microsoft.Web/sites
```

To get all the locks in your subscription:

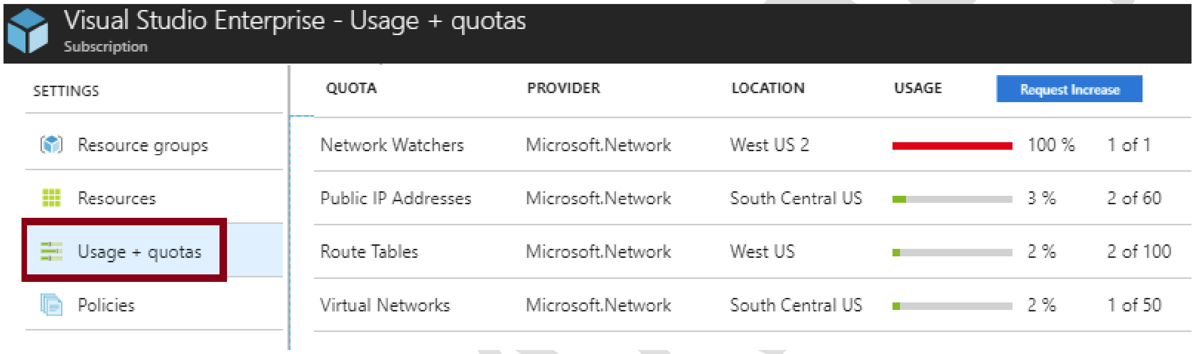
```
az lock list
```

To get all locks for a resource, use:

```
az lock list --resource-group exampleresourcegroup --resource-name examplesite \
 --namespace Microsoft.Web --resource-type sites --parent ""
```

Checking Resources Limits

Azure provides the ability to see the number of each network resource type that you've deployed in your subscription and what your subscription limits are. The ability to view resource usage against limits is helpful to track current usage, and plan for future use. In this example, there are two Public IP Addresses in South Central US and the limit is 60.



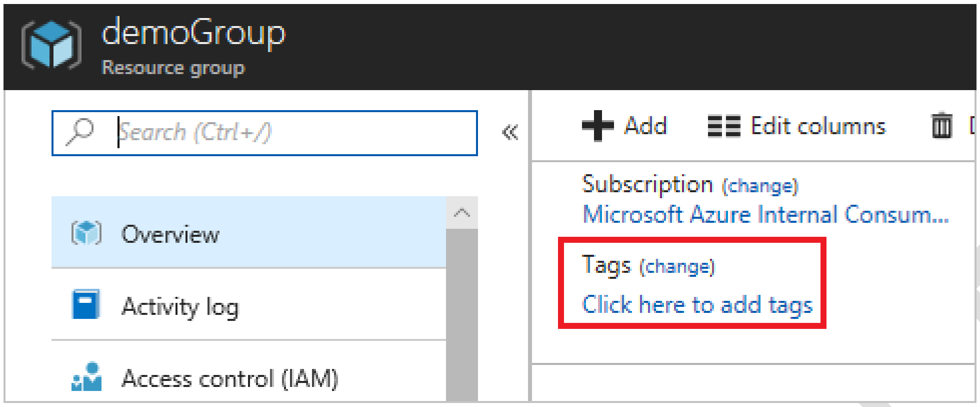
QUOTA	PROVIDER	LOCATION	USAGE	
Network Watchers	Microsoft.Network	West US 2	100 %	1 of 1
Public IP Addresses	Microsoft.Network	South Central US	3 %	2 of 60
Route Tables	Microsoft.Network	West US	2 %	2 of 100
Virtual Networks	Microsoft.Network	South Central US	2 %	1 of 50

The limits shown are the limits for your subscription. If you need to increase a default limit, there is a Request Increase link. You will complete and submit the support request. All resources have a maximum limit listed in Azure limits. If your current limit is already at the maximum number, the limit can't be increased.

Resource Tags

You can apply tags to your Azure resources to logically organize them by categories. Each tag consists of a name and a value. For example, you can apply the name "Environment" and the value "Production" or "Development" to your resources. After creating your tags, you associate them with the appropriate resources.

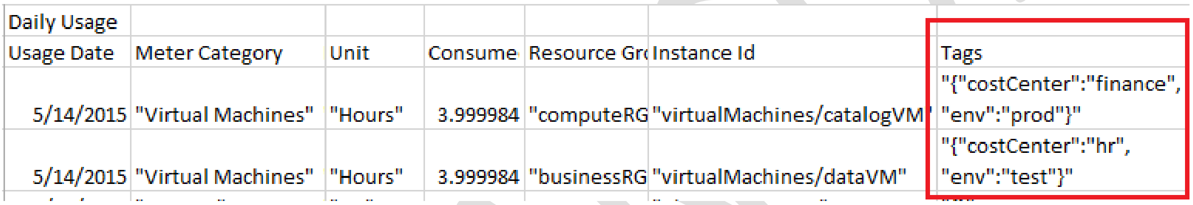
With tags in place, you can retrieve all the resources in your subscription with that tag name and value. This means, you can retrieve related resources from different resource groups.



Subscription (change)
Microsoft Azure Internal Consum...

Tags (change)
Click here to add tags

Perhaps one of the best uses of tags is to group billing data. When you download the usage CSV for services, the tags appear in the Tags column. For example, you could group virtual machines by cost center and production environment.



Daily Usage						
Usage Date	Meter Category	Unit	Consume	Resource Gr	Instance Id	Tags
5/14/2015	"Virtual Machines"	"Hours"	3.999984	"computeRG	"virtualMachines/catalogVM	"{"costCenter":"finance", "env":"prod"}"
5/14/2015	"Virtual Machines"	"Hours"	3.999984	"businessRG	"virtualMachines/dataVM"	"{"costCenter":"hr", "env":"test"}"

There are a few things to consider about tagging (more at the reference link):

- Each resource or resource group can have a maximum of 15 tag name/value pairs.
- Tags applied to the resource group are not inherited by the resources in that resource group.
- Tag names are limited to 512 characters, except for storage accounts, which are limited to 256.
- Tag values are limited to 256 characters, except for storage accounts, which are limited to 128.