Cloud Custodian Filters and Actions for AWS Resources

Common Filters for all Resources

https://cloudcustodian.io/docs/aws/resources/aws-common-filters.html

Filters	Description
check-permissions	Checks the Identity Access Management (IAM) permissions associated with a resource
config-compliance	Filters resources by their compliance with one or more AWS config rules like tagging, encryption, etc
iam-analyzer	Used to analyze embedded resource iam access policies to determine access outside of a zone of trust
image	Filter Auto Scaling Groups (ASG) by image
logging	Checks the resource logging status and attributes
marked-for-op	Filter resources for tag specified future action, uses 'custodian_status' tag which specifies a future date for an action.
metrics	Supports cloud watch metrics filters on resources. Can use 'missing_value' key when cloud watch has no data to report
offhour	Schedule off hours for resources
onhour	Schedule on hours for resources
reduce	Used to group, sort, and limit resources
security-group	Filter a resource by its associated security groups
subnet	Filter a resource by its associated subnets
tag-count	Counts all the tags that are associated with resources
usage	Filter iam resources by their api/service usage
vpc	Filter a resource by its associated vpc

finding	Check if there are Security Hub Findings related to the resources
event	Filter a resource based on an event
ops-item	Filter resources associated to extant OpsCenter operational items

Common Actions for all Resources

https://cloudcustodian.io/docs/aws/resources/aws-common-actions.html

Actions	Descriptions
auto-tag-user	Used to tag a resource with the user who created/modified it
copy-related-tag	Copies a related resource tag to its associated resource
invoke-lambda	Invokes an arbitrary lambda
invoke-sfn	Invokes step function on resources. By default this will invoke a step function for each resource providing both the policy and resource as input.
mark-for-op	Tags resources for future action
modify-policy	Action to modify SQS Queue IAM policy statements.
modify-security-groups	Modify security groups on a Redshift cluster
normalize-tag	Transform the value of a tag. Set the tag value to uppercase, title, lowercase, or strip text from a tag key
notify	Notifies the users with appropriate actions
post-finding	Report a finding to AWS Security Hub.
put-metric	Action to put metrics based on an expression into CloudWatch metrics
remove-tag	Removes the specified tags from the specified resources
rename-tag	Create a new tag with identical value & remove old tag
tag	Applies one or more tags to the specified resources.

tag-trim	Automatically remove tags from an ec2 resource
webhook	Calls a webhook with optional parameters and body populated from JMESPath queries

Filters and Actions for EC2 Resource

aws.ami

https://cloudcustodian.io/docs/aws/resources/ami.html

Filters	Description
cross-account	Check a resource's embedded iam policy for cross account access
image	Filters images based on the age (in days)
unused	Filters images based on usage

Actions	Description
remove-launch-permissions	This action will remove any launch permissions granted to other AWS accounts from the image, leaving only the owner capable of launching it
deregister	Action to deregister AMI
copy	Action to copy AMIs with optional encryption

aws.ec2

https://cloudcustodian.io/docs/aws/resources/ec2.html

Filters	Description
ebs	Filters EC2 instances with EBS backed storage devices
ephemeral	Filters EC2 instances that have ephemeral storage
image-age	Filters EC2 instances based on the age of their AMI image (in days)
instance-age	Filters instances based on their age (in days)

instance-attribute	Filters EC2 Instances with the given instance attribute
instance-uptime	Automatically filter resources older than a given date
Singelton	Filters EC2 instances that are not members of an autoscaling group and do not have Cloudwatch recover alarms
default-vpc	Matches if an ec2 database is in the default vpc
ssm	Filter ec2 instances by their ssm status information.
ssm-compliance	Filter ec2 instances by their ssm compliance status
state-age	Age an instance has been in the given state
termination-protected	Filters EC2 instances with disableApiTermination attribute set to true
user-data	Filter on EC2 instances which have matching userdata using regex

Actions	Description
autorecover-alarm	Adds a cloudwatch metric alarm to recover an EC2 instance. This action takes effect on instances that are NOT part of an ASG
propagate-stop-tags	Propagate Tags that are set at Spot Request level to EC2 instances
reboot	Reboots a previously running EC2 instance
resize	Change an instance's size
send-command	Run an SSM Automation Document on an instance
set-instance-profile	Sets (add, modify, remove) the instance profile for a running EC2 instance
set-metadata-access	Set instance metadata server access for an instance
set monitoring	Action on EC2 Instances to enable/disable detailed monitoring

snapshot	Snapshot the volumes attached to an EC2 instance
start	Starts a previously stopped EC2 instance
stop	Stops or hibernates a running EC2 instances
terminate	Terminate a set of instances

aws.ebs

https://cloudcustodian.io/docs/aws/resources/ebs.html

Filters	Description
fault-tolerant	This filter will return any EBS volume that does/does not have a snapshot within the last 7 days
instance	Filter volumes based on filtering on their attached instance
json-diff	Compute the diff from the current resource to a previous version
modifiable	Check if an ebs volume is modifiable online

Actions	Description
copy-instance-tags	Copy instance tags to its attached volume
delete	Delete an ebs volume
detach	Detach an EBS volume from an Instance
encrypt-instance-volumes	Encrypt extant volumes attached to an instance
modify	Modify an ebs volume online
snapshot	Snapshot an EBS volume

aws.key-pair

https://cloudcustodian.io/docs/aws/resources/key-pair.html

Filters	Description

unused	Filter for used or unused keys

Actions	Description
delete	Delete all ec2 keys that are not in use

aws.security-group

https://cloudcustodian.io/docs/aws/resources/security-group.html

Filters	Description
default-vpc	Filter that returns any security group that exists within the default vpc
diff	Compute the diff from the current resource to a previous version.
egress	Filter for verifying security group ingress and egress permissions
ingress	Filter for verifying security group ingress and egress permissions
json-diff	Compute the diff from the current resource to a previous version.
stale	Filter to find security groups that contain stale references to other groups that are either no longer present or traverse a broken vpc peering connection
unused	Filter to just vpc security groups that are not used.
used	Filter to security groups that are used.

Action	Description
delete	It is recommended to apply a filter to the delete policy to avoid the deletion of all security groups returned.
patch	Modify a resource via application of a reverse delta.
remove-permissions	Action to remove ingress/egress rule(s) from a security

	group
set permissions	Action to add/remove ingress/egress rule(s) to a security group

aws.eni

Filters	Description
flow-logs	find all vpcs with flows logs disabled we can do this
json-diff	Compute the diff from the current resource to a previous version.

Actions	Description
delete	Delete a network interface.
set-flow-log	Create flow logs for a network resource

Aws.network-acl

https://cloudcustodian.io/docs/aws/resources/network-acl.html

Filters	Description
json-diff	Compute the diff from the current resource to a previous version.
s3-cidr	Filter network acls by those that allow access to s3 cidrs.

The action policies for aws.network-acl follows the general policies.

Dynamodb Resources

Filters and Actions of Dynamodb-backup

https://cloudcustodian.io/docs/aws/resources/dynamodb-backup.html

Filters	event, finding, ops-item, reduce and value from common filters

Action	Description
delete	Deletes backups of a DynamoDB table

Filters and Actions of Dynamodb-table:

https://cloudcustodian.io/docs/aws/resources/dynamodb-table.html

Filters	Description
continuous backup	Check for continuous backups and point in time recovery (PITR) on a dynamodb table
json-diff	Compute the diff from the current resource to a previous version
kms-key	Filter a resource by its associated kms key

Actions	Description
backup	Creates a manual backup of a DynamoDB table.
delete	Action to delete dynamodb tables
set-continuous-backup	Set continuous backups and point in time recovery (PITR) on a dynamodb table.
set-stream	Action to enable/disable streams on table

Filters and Actions of Lambda Resource

aws.lambda

https://cloudcustodian.io/docs/aws/resources/lambda.html

Filters	Description
cross-account	Filters lambda functions with cross-account permissions
json-diff	Compute the diff from the current resource to a previous version
kms-key	Filter a resource by its associcated kms key

Actions	Description
delete	Delete a lambda function (including aliases and older versions)
remove-statements	Action to remove policy/permission statements from lambda functions.
set-concurrency	Set lambda function concurrency to the desired level

aws.lambda-layer

https://cloudcustodian.io/docs/aws/resources/lambda-layer.html

Filters	Description
cross-account	Check a resource's embedded iam policy for cross account access.

Actions	Description
delete	Parent base class for filters and actions.
remove-statements	Parent base class for filters and actions.

Filter and Action for RDS Resources

aws.rds

Resource Manager for RDS DB instances

https://cloudcustodian.io/docs/aws/resources/rds.html

Filters	Description
db-parameter	Applies value type filter on set db parameter values.
default -vpc	Matches if an rds database is in the default vpc
json-diff	Compute the diff from the current resource to a previous version. A resource matches the filter if a diff exists between the current resource and selected revision. Utilizes config as a resource revision database.
Upgrade-available	Scan DB instances for available engine upgrades

Action	Description
Auto-patch	Toggle AutoMinorUpgrade flag on RDS instance
Delete	Deletes selected RDS instances
modify-db	Modifies an RDS instance based on specified parameter using ModifyDbInstance.
resize	Change the allocated storage of an rds instance.
retention	Sets the 'BackupRetentionPeriod' value for automated snapshots, enforce (min, max, exact) sets retention days accordingly
set-public-access	This action allows for toggling an RDS instance 'PubliclyAccessible' flag to true or false
set-snapshot-copy-tags	Enables copying tags from rds instance to snapshot
snapshot	Creates a manual snapshot of a RDS instance
start	Start an rds instance
stop	Stop an rds instance
upgrade	Upgrades a RDS instance to the latest major/minor version available

Aws.rds-cluster: Resource Manager for RDS Clusters
https://cloudcustodian.io/docs/aws/resources/rds-cluster.html

Filters	Description
json-diff	Compute the diff from the current resource to a previous version

Action	Description
delete	Action to delete a RDS cluster
modify-db-cluster	Modifies an RDS instance based on specified parameter using ModifyDbInstance
retention	Action to set the retention period on rds cluster snapshots, enforce (min, max, exact) sets retention days accordingly.
snapshot	Action to create a snapshot of a rds cluster
start	Start a stopped db cluster
stop	Stop a running db cluster

aws.rds-snapshots

Filters	Description
age	Filters RDS snapshots based on age (in days)
cross-account	Check a resource's embedded iam policy for cross account access.
json-diff	Compute the diff from the current resource to a previous version.
latest	Return the latest snapshot for each database

Action	Description
delete	Deletes a RDS snapshot resource
region-copy	Copy a snapshot across regions.

restore	Restore an rds instance from a snapshot.

aws.rds-subnet:RDS subnet group

Filter	Description
json-diff	Compute the diff from the current resource to a previous version.
unused	Filters all launch rds subnet groups that are not in use but exist

Action	Description
delete	Action to delete RDS Subnet Group

S3 Resources

Filter and Action Policies

Filters	Description
bucket-encryption	Filters for S3 buckets that have bucket-encryption
Bucket-logging	Filter based on bucket logging configuration.
bucket-notification	Filter based on bucket notification configuration.
check-public-block	Filter for s3 bucket public blocks. If no filter paramaters are provided it checks to see if any are unset or False. If parameters are provided only the provided ones are checked.
cross-account	Filters cross-account access to S3 buckets
data-events	Parent base class for filters and actions.
global-grants	Filters for all S3 buckets that have global-grants
Has-statement	Find buckets with set of policy statements.

Inventory	Filter inventories for a bucket
is-log-target	Filter and return buckets are log destinations.
json-diff	Compute the diff from the current resource to a previous version.
missing -policy-statement	Find buckets missing a set of named policy statements.
no-encryption-statement	Find buckets with missing encryption policy statements.

Actions	**Description**
Attach-encrypt	Action attaches lambda encryption policy to S3 bucket
configure-lifecycle	Action applies a lifecycle policy to versioned S3 buckets
delete	Action deletes a S3 bucket
delete-bucket-notification	Action to delete S3 bucket notification configurations
delete-global-grants	Deletes global grants associated to a S3 bucket
encrypt-keys	Action to encrypt unencrypted S3 objects
encryption-policy	Action to apply an encryption policy to S3 buckets
no-op	Parent base class for filters and actions.

remove-statements	Action to remove policy statements from S3 buckets
remove-website-hosting	Action that removes website hosting configuration.
set-bucket-encryption	Action enables default encryption on S3 buckets
Set-inventory	Configure bucket inventories for an s3 bucket.
set-public-block	Action to update Public Access blocks on S3 buckets
set-replication	Action to add or remove replication configuration statement from S3 buckets
set-statements	Action to add or update policy statements to S3 buckets
toggle-logging	Action to enable/disable logging on a S3 bucket.
toggle-versioning	Action to enable/suspend versioning on a S3 bucket