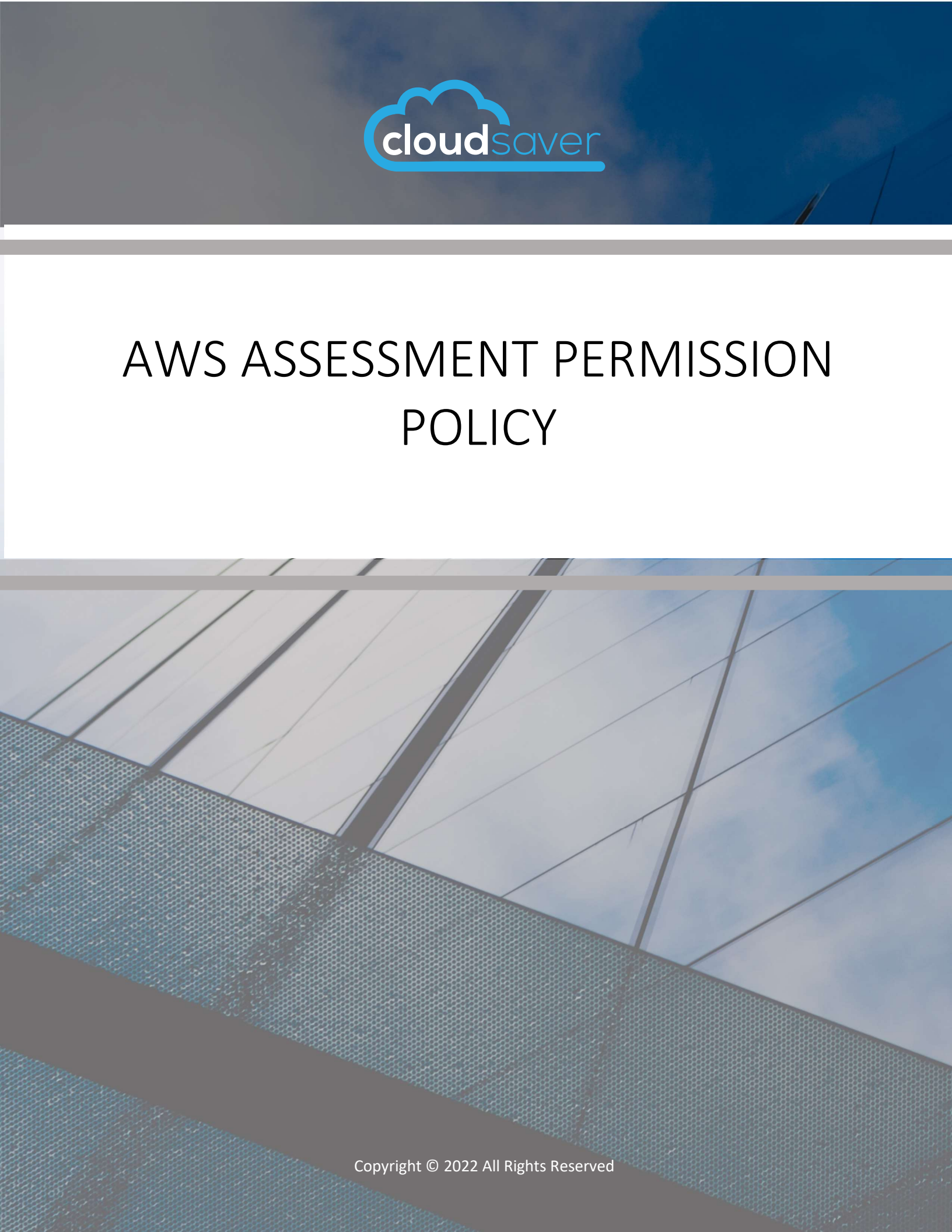

AWS ASSESSMENT PERMISSION POLICY

Overview

CloudSaver provides managed AWS cost optimization solutions. Using Cloudsaver's proprietary application and extensive experience, our engineers help companies reduce their AWS costs by eliminating unnecessary spend and optimizing key resources. As used herein, CloudSaver refers to both application and team depending on context.

Before engaging with a customer, CloudSaver performs a free assessment to obtain a thorough understanding of that customer's AWS environment. During the free assessment period CloudSaver connects with the customer's AWS environment and collects certain billing, environmental and operational data which is then analyzed and used to determine the approximate savings opportunity.

After the assessment is completed and the customer has decided to engage CloudSaver, the customer must expand the permissions to enable CloudSaver's access to complete operational data and allow execution of the cost saving actions identified during the assessment.

The purpose of this document is to describe the full set of AWS permissions CloudSaver requires to collect billing and environmental data from the customer environment, as well as the specific permissions needed to make changes to customer's environment to realize the savings during the engagement

How CloudSaver Connects to Your Environment

The CloudSaver application follows AWS' best practices and uses a role-based access methodology which includes the use of unique external IDs and tokens that automatically expire at intervals of no longer than one hour.

Customers create a role for CloudSaver and then assign a permission policy to that role (see below for detailed discussion of the permission policy). CloudSaver must separately connect to each AWS account included in the scope of the engagement.

Enabling this access allows the customer to leverage the full set of features within the CloudSaver application, including approving & scheduling the execution of its powerful optimization tools and cost visibility provided by Invoice Explorer.

The customer may disconnect CloudSaver from their environment at any time simply by removing the role discussed above.

Permission Policies

CloudSaver adopts the principle of least privilege when connecting with customer environments. As such the permission policies have been designed to limit access to customers' environment to just the essential permissions necessary to complete the assessment.

CloudSaver has two separate permission policies. The first policy is used for 'standard accounts' and the second policy is used for 'master accounts.' These two types of accounts are generally the same, with the exception that AWS stores the billing data for ALL accounts on the master account. As such, Cloudsaver requires a slightly expanded set of permissions to collect and process the billing data.

Standard Accounts

Cloudsaver permission policy for standard accounts allows for collecting environmental and operational data from customer's AWS environment. Cloudsaver uses this data to identify specific cost saving opportunities for customer's resources. Additionally, this policy provides CloudSaver the ability to make changes to customer's environment necessary to provide our services and realize the savings opportunities.

Cloudsaver does not install any third-party agents but does enable or require access to certain native AWS tools such as Systems Manager Agent and CloudWatch Agent. These AWS tools are an integral part of our solution.

The entire policy for standard accounts may be found in Appendix A.

Permission Policy Line Item	**CloudSaver Use**
autoscaling:DescribeLaunchConfigurations Grants permission to describe one or more launch configurations. If you omit the list of names, then the call describes all launch configurations autoscaling:DescribeAutoScalingGroups Grants permission to describe one or more Auto Scaling groups. If a list of names is not provided, the call describes all Auto Scaling groups autoscaling:DescribeLoadBalancerTargetGroups Grants permission to describe the target groups for the specified Auto Scaling group autoscaling:DescribePolicies Grants permission to describe the policies for the specified Auto Scaling group autoscaling:DescribeScalingActivities Grants permission to describe one or more scaling activities for the specified Auto Scaling group	Load balancers may be part of Auto Scaling groups. Knowing the full extent of EC2 instances, load balancers, and Auto Scaling groups give CloudSaver the most knowledge about each EC2 instance. CloudSaver will then be able to determine the best optimization course of action for each EC2.
cloudwatch:ListMetrics Grants permission to retrieve a list of valid metrics stored for the AWS account owner cloudwatch:GetMetricData Retrieves cloudwatch metric values	CloudWatch metric data gives CloudSaver access to CPU utilization, network traffic, and EBS volume information. This data is used to determine whether an instance should be resized.
dynamodb:Listtables Grants permission to return an array of table names associated with the current account and endpoint dynamodb:Describetable Grants permission to return information about the table	These read permissions allow CloudSaver to list all AWS account DynamoDB instances for cost optimization opportunities.

dynamodb:ListTagsofResource Grants permission to list all tags on an Amazon DynamoDB resource	
ec2:DescribeImages Grants permission to describe one or more images (AMIs, AKIs, and ARIs) ec2:DescribeLaunchTemplates Grants permission to describe one or more launch Templates ec2:DescribeInstances Grants permission to describe one or more instances ec2:DescribeSpotFleetInstances Grants permission to describe the running instances for a Spot Fleet ec2:DescribeReservedInstances Grants permission to describe one or more purchased Reserved Instances in your account ec2:DescribeAddresses Grants permission to describe one or more Elastic IP addresses ec2:DescribeNatGateways Grants permission to describe one or more NAT gateways ec2:DescribeNetworkInterfaces Grants permission to describe one or more network interfaces ec2:DescribeSnapshots Grants permission to describe one or more EBS snapshots ec2:DescribeSnapshotAttribute Grants permission to describe an attribute of a snapshot ec2:DescribeVolumes Grants permission to describe one or more EBS volumes ec2:DescribeInstanceAttribute Grants permission to describe the attributes of an instance ec2:DescribeInstanceCreditSpecifications Grants permission to describe the credit option for CPU usage of one or more burstable performance instance	All “read” permissions allow CloudSaver to retrieve all attributes for EC2 instances, including running/stopped state, size, price per hour, and other attributes. As always, CloudSaver never makes any modification to any instance without the customer’s explicit permission.
eks:ListClusters Grants permission to list the Amazon EKS clusters in your AWS account (in the specified or default region) eks:DescribeCluster	Kubernetes can be used to deploy EC2 instances; CloudSaver needs to know about the EKS cluster to create EC2 recommendations.

Grants permission to retrieve descriptive information about an Amazon EKS cluster eks:ListNodegroups Grants permission to list the Amazon EKS nodegroups in your AWS account (in the specified or default region) attached to given cluster eks:DescribeNodegroup Grants permission to retrieve descriptive information about an Amazon EKS nodegroup	
elasticbeanstalk:DescribeEnvironments Grants permission to retrieve descriptions for existing environments elasticbeanstalk:DescribeEnvironmentResources Grants permission to retrieve a list of AWS resources for an environment elasticbeanstalk:DescribeInstancesHealth Retrieves detailed information about the health of beanstalk instances. elasticbeanstalk:DescribeEnvironmentHealth Retrieves information on beanstalk cluster environments overall health. elasticbeanstalk:DescribeConfigurationsSettings Retrieves settings for specified configurations in cluster environment elasticbeanstalk:DescribeConfigurationOptions Retrieves Configuration options used.	EC2 instances may be part of a Beanstalk cluster. Instances that are part of a cluster will be treated differently than stand-alone EC2 instances.
elasticmapreduce:ListClusters Grants permission to get the status of accessible clusters elasticmapreduce:ListInstances Grants permission to get details about the Amazon EC2 instances in a cluster elasticmapreduce:DescribeCluster Grants permission to get details about a cluster, including status, hardware, and software configuration, VPC settings, and so on elasticmapreduce:ListInstanceFleets Grants permission to get details of instance fleets in a cluster elasticmapreduce:listinstancegroups Provides all available details about the instance groups in a cluster. elasticmapreduce:GetManagedScaledPolicy	EC2 instances may be part of an EMR cluster. Instances that are part of a cluster will be treated differently than stand-alone EC2 instances.

Fetches the attached managed scaling policy for an Amazon EMR cluster. elasticmapreduce:GetAutoTerminationPolicy Returns the auto-termination policy for an Amazon EMR cluster.	
elasticloadbalancing:DescribeInstanceHealth Describes the state of the specified instances with respect to the specified load balancer. elasticloadbalancing:DescribeLoadBalancers Describes the specified load balancers. elasticloadbalancing:DescribeTags Describes the tags associated with the specified load balancers elasticloadbalancing:DescribeTargetGroups Describes the specified target groups or all of your target groups. elasticloadbalncing:DescribeTargetHealth Describes the health of the specified targets or all of your targets.	CloudSaver needs to know which EC2 instances are members of elastic load balancers. If an instance is a member, then it will be blocked from any individual modification. Instances that are part of a load balancer must be handled as a group.
es:ListDomainNames Grants permission to display the names of all OpenSearch Service domains that the current user owns es:DescribeDomains Grants permission to view a description of the domain configuration for up to five specified OpenSearch Service domains es:ListTags Grants permission to display all resource tags for an OpenSearch Service domain	Elastisearch read permissions provides all ES domains instances and storage type.
glue:ListJobs Retrieves the names of all job resources, or the resources with the specified tag. glue:BatchGetJobs Returns a list of resource metadata for a given list of job names. glue:GetJob Retrieves an existing job definition. glue:GetJobBookmark Returns information on a job bookmark entry. glue:GetJobRun Retrieves the metadata for a given job run. glue:GetJobRuns Retrieves metadata for all runs of a given job definition.	Glue is a serverless ETL service that provisions data processing units (DPUs) to perform various tasks; CloudSaver needs to know about Glue jobs to recommend optimizations for the service.

glue:GetJobs Retrieves all current job definitions. glue:GetMLTaskRuns Gets a list of runs for a machine learning transform. glue:GetMLTransforms Gets a sortable, filterable list of existing Glue machine learning transforms. glue:GetTags Retrieves a list of tags associated with a resource. glue:GetWorkflow Retrieves resource metadata for a workflow. glue:GetWorkflowRun Retrieves the metadata for a given workflow run. glue:GetWorkflowRunProperties Retrieves the workflow run properties which were set during the run. glue:GetWorkflowRuns Retrieves metadata for all runs of a given workflow.	
lambda:ListFunctions Grants permission to retrieve a list of AWS Lambda functions, with the version-specific configuration of each function lambda:ListTags Grants permission to retrieve a list of tags for an AWS Lambda function	CloudSaver retrieves all lambda functions, the number of invocations, the amount of memory allocated, and the duration. Used to optimize functions.
logs:DescribedLogGroups Grants permissions to return all the log groups that are associated with the AWS account making the request logs:DescribedLogstreams Grants permissions to return all the log streams that are associated with the specified log group	CloudSaver uses CloudWatch log files to access lambda actual memory usage.
organizations:ListAccounts Grants permission to list all the accounts in the organization. organizations:ListRoots Grants permission to list all the roots that are defined in the organization. organizations:ListChildren Grants permission to list all the OUs or accounts that are contained in a parent OU or root.	These read permissions allows CloudSaver permission to view organizations within client accounts for asset tagging.

organizations:DescribeOrganizationalUnit Grants permission to retrieve details about an organizational unit (OU).	
rds:DescribeDBInstances Grants permission to return information about provisioned RDS instances rds:ListTagsForResource Grants permission to list all tags on an Amazon RDS resource rds:DescribeDbSnapshots Grants permission to return information about DB snapshots rds:DescribeDbClusters Grants permission to return information about provisioned Aurora DB clusters rds:DescribeReservedDBInstances Grants permission to return information about reserved DB instances for this account, or about a specified reserved DB instance	CloudSaver has tools to rightsize RDS instances. These permissions give CloudSaver the ability to download RDS instance details.
redshift:DescribeClusters Grants permission to describe properties of provisioned clusters redshift:DescribeReservedNodes Grants permission to describe the reserved nodes redshift:DescribeNodeConfigurationOptions Grants permission to describe properties of possible node configurations such as node type, number of nodes, and disk usage for the specified action type	Identify Redshift clusters cost optimization opportunities
route53:ListHostedZones Grants permission to get a list of the public and private hosted zones that are associated with the current AWS account	Identify Route53 cost optimization opportunities
s3:ListBuckets Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000) s3:GetBucketPolicy Grants permission to return the policy of the specified bucket s3:GetBucketPolicyStatus Grants permission to retrieve the policy status for a specific Amazon S3 bucket, which indicates whether the bucket is public s3:GetBucketTagging Grants permission to return the tag set associated with an Amazon S3 bucket	CloudSaver uses an S3 bucket to hold billing data. This permission is needed so CloudSaver can make sure that the correct bucket exists.

s3:GetLifecycleConfiguration Grants permission to return the lifecycle configuration information set on an Amazon S3 bucket s3:GetObjectAttributes Grants permission to retrieve objects/files metadata from Amazon S3 buckets	
savingsplans:DescribeSavingsPlans Grants permission to describe the savings plans associated with customers account	This read permission allows Cloudsaver the ability to analyze any savings plan contracts that cover AWS resources.
workspaces:DescribeIPGroups Describes one or more of your IP access control groups. workspaces:DescribeTags Describes the specified tags for the specified WorkSpaces resource. workspaces:DescribeWorkspaceBundles Retrieves a list that describes the available WorkSpace bundles. workspaces:DescribeWorkSpaceDirectories Describes the available directories that are registered with Amazon WorkSpaces. workspaces:DescribeWorkspaceImagePermissions Describes the permissions that the owner of an image has granted to other AWS accounts for an image. workspaces:DescribeWorkspaceImages Retrieves a list that describes one or more specified images if the image identifiers are provided. workspaces:DescribeWorkspaces Describes the specified WorkSpaces. workspaces:DescribeWorkspacesConnectionStatus Describes the connection status of the specified WorkSpaces. workspaces:DescribeWorkspaceSnapshots Describes the snapshots for the specified WorkSpace.	These permissions allow Cloudsaver to Identify workspaces cost optimization opportunities.

Master Accounts

Master accounts differ from standard accounts because AWS holds the billing data for every account in the master account. As such, cloudsaver require a slightly expanded set of permissions so cloudsaver can collect and process the billing data.

CloudSaver does not install any third-party agents but does enable or require access to certain native AWS tools such as Systems Manager Agent and CloudWatch Agent. These AWS tools are an integral part of Cloudsaver's solution.

CloudSaver does not have access to any customer or internal data.
The permission policy for master accounts includes all the permissions from standard accounts plus the additional list of permissions described below.

The entire policy for master accounts may be found in Appendix B.

Permission Policy Line Item	CloudSaver Use
s3:CreateBucket Creates a new bucket. s3:DeleteBucket Deletes the bucket named in the URI. s3:ListBucket Returns some or all (up to 1000) of the objects in a bucket. s3:PutLifecycleConfiguration Creates a new lifecycle configuration for the bucket or replaces an existing lifecycle configuration. s3:PutBucketPolicy Add to or replace a policy on a bucket.	These permissions are all applied to the S3 bucket that CloudSaver creates to hold billing data. The delete command is only used if the customer does not renew their subscription with CloudSaver.
cur:DeleteReportDefinition Delete Cost and Usage Report Definition. cur:PutReportDefinition Write Cost and Usage Report Definition to the bucket.	These permissions open and close the pipeline from the Cost and Usage Reports in AWS to the S3 bucket that holds the billing data.

Data Security

Data security is paramount and CloudSaver has appropriate safeguards in place to protect customer's data. Any data that is transferred from a customer's environment to CloudSaver's environment is secured using modern 256-bit encryption algorithms. Additionally, CloudSaver maintains a separate database for each customer. As such, any customer data stored in CloudSaver's environment is never comingled with other customer data.

All customer data maintained in CloudSaver's environment is deleted when a customer no longer wishes to use our services. Additionally, all billing data stored in the S3 bucket created by CloudSaver is automatically removed after 90 days.

How CloudSaver Collect Billing Data

AWS stores all billing data for all accounts in the Master Account. CloudSaver needs to make the following changes to customer's master account in order to receive this billing data.

AWS requires that billing data be stored in an S3 bucket before it can be retrieved, so cloudsaver create an S3 bucket to hold this data. The bucket will be named "cloudsaver-xxxxxxxxxxxx-billing-files" where "xxxxxxxxxxxx" will be replaced with the master account number. Note, in the permission policy, this is the only bucket that CloudSaver will have permission to save and delete files.

Cloudsaver also add a 90-day lifecycle policy on this S3 bucket. This will give CloudSaver enough cushion to re-download previous billing files if necessary while keeping the size and cost of the s3 bucket relatively small.

Lastly, CloudSaver will create a cost and usage report that will send the billing files to the s3 bucket. AWS will periodically send billing files through the cost and usage report; CloudSaver will update the billing files every day between 4 and 6 am, and every evening between 8 and 10 pm.

How Cloudsaver Collect Operational Data

CloudSaver retrieves environmental and operational data via AWS' standard API. Substantially all operational data is retrieved on an as needed basis and then immediately deleted from the CloudSaver environment as soon as the data analysis has been completed. CloudSaver generally does not store detailed operational data in its environment.

Appendix A – Permission Policy for Standard Accounts

```
{
 “Version”: “2012-10-17”,
 “Statement”: [
  {
   “Sid”: “CloudSaverApiAccess”,
   “Effect”: “Allow”,
   “Action”: [
            "autoscaling:DescribeLaunchConfigurations",
            "autoscaling:DescribeAutoScalingGroups",
            "autoscaling:DescribeLoadBalancerTargetGroups",
            "autoscaling:DescribePolicies",
            "autoscaling:DescribeScalingActivities",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricData",
            "logs:DescribeLogGroups",
            "logs:DescribeLogstreams",
            "dynamodb:Listtables",
            "dynamodb:Describetable",
            "dynamodb:ListTagsofResource",
            "ec2:DescribeImages",
            "ec2:DescribeLaunchTemplates",
            "ec2:DescribeInstances",
            "ec2:DescribeSpotFleetInstances",
            "ec2:DescribeReservedInstances",
            "ec2:DescribeNatGateways",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeSnapshots",
            "ec2:DescribeSnapshotAttribute",
            "ec2:DescribeVolumes",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeInstanceCreditSpecifications",
            "eks:ListClusters",
            "eks:DescribeCluster",
            "eks:ListNodegroups",
            "eks:DescribeNodegroup",
            "elasticbeanstalk:Describeenvironments",
            "elasticbeanstalk:DescribeEnvironmentresources",
            "elasticbeanstalk:DescribeInstancesHealth",
            "elasticbeanstalk:DescribeEnvironmentHealth",
            "elasticbeanstalk:DescribeConfigurationSettings",
            "elasticbeanstalk:DescribeConfigurationOptions",
            "elasticloadbalancing:DescribeLoadBalancers",
            "elasticloadbalancing:DescribeInstanceHealth",
            "elasticloadbalancing:DescribeTags",
            "elasticloadbalancing:DescribeTargetGroups",
            "elasticloadbalancing:DescribeTargetHealth",
            "elasticmapreduce:DescribeCluster",
            "elasticmapreduce:GetManagedScalingPolicy",
            "elasticmapreduce:GetAutoTerminationPolicy",
            "elasticmapreduce:ListClusters",
            "elasticmapreduce:ListInstances",
            "elasticmapreduce:ListInstanceFleets",
            "elasticmapreduce:ListInstanceGroups",
            "es:DescribeDomains",
            "es:ListDomainNames",
            "es:ListTags",
            "glue:ListJobs",
```

```
            "glue:BatchGetJobs",
            "glue:GetJob",
            "glue:GetJobBookmark",
            "glue:GetJobRun",
            "glue:GetJobRuns",
            "glue:GetJobs",
            "glue:GetMLTaskRuns",
            "glue:GetMLTransforms",
            "glue:GetTags",
            "glue:GetWorkflow",
            "glue:GetWorkflowRun",
            "glue:GetWorkflowRunProperties",
            "glue:GetWorkflowRuns",
            "lambda:ListFunctions",
            "lambda:ListTags",
            "organizations:ListAccounts",
            "organizations:ListRoots",
            "organizations:ListChildren",
            "organizations:DescribeOrganizationalUnit",
            "rds:DescribeDBInstances",
            "rds:ListTagsForResource",
            "rds:DescribeDbSnapshots",
            "rds:DescribeDbClusters",
            "rds:DescribeReservedDBInstances",
            "redshift:DescribeClusters",
            "redshift:DescribeNodeConfigurationOptions",
            "redshift:DescribeReservedNodes",
            "route53:ListHostedZones",
            "s3:ListBucket",
            "s3:GetBucketPolicy",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketTagging",
            "s3:GetLifecycleConfiguration",
            "s3:GetStorageLensConfiguration",
            "s3:GetObjectAttributes",
            "savingsplans:DescribeSavingsPlans",
            "workspaces:Describeworkspaces",
            "workspaces:DescribeIPGroups",
            "workspaces:DescribeTags",
            "workspaces:DescribeWorkspaceBundles",
            "workspaces:DescribeWorkSpaceDirectories",
            "workspaces:DescribeWorkspaceImagePermissions",
            "workspaces:DescribeWorkspaceImages",
            "workspaces:DescribeWorkspacesConnectionStatus",
            "workspaces:DescribeWorkspaceSnapshots"
            ],
        “Resource”: “*”
      }
   ]
}
```

Appendix B – Permission Policy for Master Accounts

```
{
  “Version”: “2012-10-17”,
  “Statement”: [
    {
      “Sid”: “CloudSaverApiS3Bucket”,
      “Effect”: “Allow”,
      “Action”: [
        “s3:CreateBucket”,
        “s3:DeleteBucket”,
        “s3:ListBucket”,
        “s3:PutLifecycleConfiguration”,
        “s3:PutBucketPolicy”
      ],
      “Resource”: “arn:aws:s3:::cloudsaver-????????????-billing-files”
    },
    {
      “Sid”: “CloudSaverApiS3BucketObjects”,
      “Effect”: “Allow”,
      “Action”: [
        “s3:DeleteObject”,
        “s3:GetObject”
      ],
      “Resource”: “arn:aws:s3:::cloudsaver-????????????-billing-files/*”
    },
    {
      “Sid”: “CloudSaverApiSaveBillingReportToS3”,
      “Effect”: “Allow”,
      “Action”: [
        “cur:DeleteReportDefinition”,
        “cur:PutReportDefinition”
      ],
      “Resource”: “arn:aws:cur:*:*:definition/cloudsaver-????????????-billing-files”
    }
  ]
}
```