lightstream

Cloud Managed Services for AWS

Service Description

aws partner network

Advanced Consulting Partner

Cloud Managed Services for AWS – Service Description v1.0
Last Updated: November 2019

Introduction

The cloud delivers business agility by giving you an environment that can evolve and adapt continually. But this agility comes at cost: ensuring security, effective technology use, cost-efficiency, and operational oversight in this shifting landscape requires ongoing management.

Fortunately, Lightstream makes things simple. We give you the cloud expertise you need to design architectures that deliver the best business outcomes and ongoing management services that keep your cloud optimized as your business changes and grows.

You can rest easy knowing your cloud:

- Follows AWS best practices for:
  - Security
  - Finance
  - Technology
  - Operations
- Is built with architectures that deliver the best business outcomes
- Is modern, using that latest updates, features, and services
- Is simple and easy to manage
- Is managed effectively, in partnership with experts who educate your staff

This document provides an overview of Lightstream Cloud Managed Services. It includes a discussion of the three different tiers customers can choose from and provides detailed information about the services.

Lightstream Cloud Managed Services Tiers

Every organization is unique and has different cloud management challenges. Some businesses lack the technical expertise or capacity to operate cloud infrastructure, tools and applications while others may have the ability but want to focus on their core business. Others still are looking to enable and educate their staff from experts who have seen and done it all.

To meet these diverse needs, Lightstream offers managed services at the following tiers:[1]

Platinum

Lightstream becomes a partner in your cloud journey, adding Certified Cloud Engineer skills to your team. We will gain a deep understanding of your business needs and cloud goals, actively assist you in building and maintaining an ideal cloud environment, and also help you monitor, manage, and maintain your cloud on an ongoing basis.

Gold

Lightstream experts review your environment and advise your staff on an ongoing basis to ensure you are making the right tradeoffs in your architecture to achieve the best business outcomes.

Silver

Free subscriptions to cloud management software, training, and user groups give your organization the information you need to create a cloud built for your business. Lightstream will meet with your staff periodically to fill in any gaps.

[1] We indicate services available at each tier with "P" for Platinum, "G" for Gold, and "S" for Silver. Services are cumulative: Platinum includes all Gold and Silver services and Gold includes all Silver services.

About Security Services

Security is fundamental to protecting your information, systems, and assets. It’s vital for businesses to ensure data can only be accessed by authorized users and systems and that data is protected against loss. Lightstream ensures your cloud is secure through the following services.

Expert Security Reviews (P/G)

A Certified Cloud Engineer reviews available data to ensure your cloud follows best practices for:

- Identity and Access Management
- Detective Controls, Infrastructure Protection
- Data Protection
- Incident Response

See Appendix A. Data Evaluated in a Security Review for detailed information.

AWS CIS Benchmark (P/G)

CIS (Center for Internet Security) Benchmarks are best practices for the secure configuration of a system. CIS Benchmarks are developed through a unique consensus-based process comprised of cybersecurity professionals and subject matter experts around the world. A Certified Cloud Security Engineer will conduct a CIS (Center for Internet Security) benchmark on your cloud environment.

Security Development and Remediation (P)

Lightstream actively assists Platinum customers with security activities, including development and remediation for items identified in ongoing security reviews and periodic benchmarks.

At the Gold tier, Lightstream provides recommendations for remediation that your staff implements.

Tier 1 Technical Advisement (P/G)

Whenever you need assistance, Lightstream is here to help. You will have the direct phone number and email of a named contact.

Cloudcheckr Security Software and Training (P/G/S)

All tiers of Lightstream Cloud Managed Services include a subscription and training for Cloudcheckr software. This product dramatically improves visibility into your security posture, including the following:

- Log intelligence
- Best practices and alerts
- Perimeter assessment
- Configuration assurance
- User permissions

See the cloudcheckr web site for details.

About Finance Services

Lightstream finance services ensure your cloud spend is aligned to your technology needs. A Lightstream Cloud Financial Expert will ensure you aren't overspending on technology or services you aren't actively using – and will work with you to adjust your spending as cloud needs evolve.

Lightstream ensures your cloud is cost-efficient through the following services.

Reserved Instance and Cost Savings Management Program (P)

AWS's Reserved Instances (RIs) and Cost Savings programs are some of the most effective ways for you to reduce your cloud spend, but determining exactly what you need can be challenging and time consuming.

At the Platinum tier, Lightstream offers a fully managed Reserved Instance and Cost Savings program where we:

- Establish a strategy that aligns to your business strategy
- Assess your environment and identify sources of waste
- Negotiate and procure RI and Cost Savings contracts
- Monitor and make adjustments as your environment changes
- Review performance and savings on an ongoing basis
- Provide ad hoc support and education about RI and Cost Savings contracting

Expert Financial Reviews (P/G)

A Cloud Financial Expert will provide ongoing advice and consultation to ensure you have the visibility, including dashboards and reports, to effectively manage your cloud finances and achieve your strategic objectives.

At the Platinum tier, Lightstream will assess cloud spend on an ongoing basis and meet with your staff regularly to review and provide recommendations for cost optimization.

Lightstream Connect Subscription and Training (P/G/S)

All tiers of Lightstream Cloud Managed Services include a subscription to and training for Lightstream Connect software. This product is a clear, concise, and thorough reporting platform that makes it easy to manage cloud spend through the following features:

- Summary level reporting of each cloud account by day, month, and product category
- Reporting of the cloud environment by various tags
- Breakout of EC2 spend by server class, product type, region, and platform
- Detailed analysis of EC2 environment by instance type, platform, availability zone, and cost, by day and month
- Summary and secondary level views of spend trends

- Analysis and reporting of RI opportunities by RI contracting cluster, including savings and AWS fees by contract term and type
- Performance of each and RI contract, including utilization and financial results, by day

Lightstream can also create custom reports for Platinum tier customers, as needed.

About Technology Services

The cloud enables organizations to deploy any technology they need on the fly. While this accelerates business, it also makes it easy for to waste money excessively overprovisioning resources or risk quality by under-provisioning resources.

Lightstream ensures your cloud technology is optimized through the following services.

Ongoing Cloud Best Practice Reviews (P/G)

Lightstream reviews your environment on an ongoing basis to ensure:

- Alignment between line of business technical requirements and cloud best practices
- Assets and resources are tagged to streamline monitoring and management
- Reporting reflects information important to business

Ongoing Technology Reviews (P/G)

Lightstream reviews your environment on an ongoing basis to ensure your cloud follows best practices for technology. We review all available data and analytics to assess your environment and develop strategies to improve:

- Cost-efficiency
- Availability
- Usage (over- or under-utilization)
- AWS Trusted Advisor

See Appendix B. Data Evaluated for Technology Reviews for details.

Technical Remediation (P)

Lightstream creates a remediation plan for items identified in reviews and will assist or even perform remediation activities.

Level 1 Technical Advisement (P/G)

Lightstream staff can assist you with the following technology activities:

- Optimizing resources and configuration (P/G):
    - Compute
    - Storage
    - Network/CDN
    - Database
    - Security

- Build and assist with technical proofs of concept (POCs) (P)
- Research and assist with defining requirements and building product-specific technical capabilities (P)

Research and Development Services (P)

Lightstream can research and provide infrastructure recommendations to help you achieve your general cloud initiatives.

Project-Specific Cloud Professional Services (P/G)

Ensure project success by adding a Lightstream Certified Cloud Engineer to your staff. We will review your line of business requirements and perform profession services SOW-based work to help you achieve any business goal. Platinum and Gold members receive a 10% and 5% discount on cloud professional services, respectively.

Cloudcheckr technical software and training (P/G/S)

All tiers of Lightstream Cloud Managed Services include a subscription and training for Cloudcheckr software. This product dramatically improves visibility into your technical environment, including:

- Asset Inventory
    - Aggregated Metrics
    - Inventory Tracking
    - Asset Snapshots
    - Drill-Down Analytics

- Cost
    - Spend Optimization
    - Best Practices

- Resource Utilization
    - Comprehensive Analytics
    - Actionable Insights
    - Instance Rightsizing
    - Best Practices
    - IOPS Analysis and Rightsizing

- Automation Framework
    - Security
    - Continuous Monitoring
    - Scalable Resource Management
    - Automatic Snapshots
    - Cost Optimization
    - Best Practice Checks

See the cloudcheckr web site for details.

About Operations Services (P/G)

Lightstream lets you keep staff focused on value added work versus cloud infrastructure management. Designated contacts monitor your environment on an ongoing basis, perform reviews and schedule meetings to present findings, and take calls whenever you need assistance. Following are the tasks your contacts perform.

Client Engagement Manager (P/G)

Facilitates support requests.

- Provides general assistance for:
  - Billing questions
  - Vendor ticket
  - Escalation of issues to an engineer
- Custom reporting
  - Escalation to developers
  - Escalation to finance

Coordinates meetings, including:

- General business and cloud reviews
- Security best practice reviews
- Finance best practice reviews
- Technology reviews
- Operational best practice reviews
- Managed RI reviews
- Training sessions for Lightstream Connect and Cloudcheckr

Technical Account Management tasks

- New Master Payer setup
- New Accounts
- Product Update Briefings
- Announcements for events, training, best practice user group meetings, and updates

Certified Cloud Engineer (P/G)

- Assists with creating your overall cloud strategy (P/G)
- Performs analysis of cloud environment, reports technical and security findings, and provides recommendations (P/G)
- Creates remediation plan and assists with implementation (P)

SLAs for Support Requests

We respond to all support requests as soon as possible, but no longer than:

- Platinum: 4 hours
- Gold: 8 hours
- Silver: 12 hours

Our acknowledgement will include the following information:

1. The question we received.
2. Confirmation that we are working on it.
3. Estimated timing for the next step(s).

Appendix A. Data Evaluated in a Security Review

The following list shows all data points a Lightstream Certified Cloud Security Engineer reviews when evaluating your security posture:

AWS Config Delivery Failing
AWS Config Not Enabled
AWS Config S3 Bucket Missing
AWS Config SNS Topic Missing
Blocklisted IP Address in AWS Infrastructure
Blocklisted IP Address Logging Into Console
Blocklisted IP Address Making API Calls
CloudTrail Access From A New Location
CloudTrail Access From New IP Address
CloudTrail Access From New User
CloudTrail Access Outside of Normal Business Hours
CloudTrail Aggregate Buckets Not Set To Read-Only
CloudTrail Delivery Failing
CloudTrail Include Global Services Not Enabled
CloudTrail Integrated With CloudWatch Logs
CloudTrail Log File Validation Not Enabled
CloudTrail logs are not encrypted at rest using KMS CMK
CloudTrail Not Enabled
CloudTrail Notification Failing
CloudTrail S3 Buckets Without Logging Enabled
CloudTrail SNS Topic Missing
CloudTrail Unauthorized Access Attempts
Contact Details on AWS Accounts Are Not Up-To-Date
Contact Information Not Registered
DB Security Groups Inbound Rules Set To Allow Access To Broad IP Ranges
DB Security Groups Inbound Rules Set To Allow Access To Broad IP Ranges (No Resources)
DB Security Groups Inbound Rules Set To Allow Traffic From Any IP Address
DB Security Groups Inbound Rules Set To Allow Traffic From Any IP Address (No Resources)
DB Security Groups Inbound Rules With Possible CIDR Prefix Mistake
DB Security Groups Inbound Rules With Possible CIDR Prefix Mistake (No Resources)
Default Security Groups Allowing Traffic
EC2 Instances That Are Not Isolated Within A VPC
EC2 Instances With Embedded Credentials
EC2 Instances Without Attached IAM Profile Role
EC2-Classic Security Groups Allow Traffic From Any IP Address
EC2-Classic Security Groups Inbound Rules Allowing Traffic from All IPs and All Ports
EC2-Classic Security Groups Inbound Rules Allowing Traffic from All IPs and All Ports (No Resources)
EC2-Classic Security Groups Inbound Rules Allowing Traffic from Any IP Address

EC2-Classic Security Groups Inbound Rules Allowing Traffic from Any IP Address (No Resources)
EC2-Classic Security Groups Inbound Rules Allowing Traffic From Broad IP Ranges
EC2-Classic Security Groups Inbound Rules Allowing Traffic From Broad IP Ranges (No Resources)
EC2-Classic Security Groups Inbound Rules Set To All IPs And All Ports
EC2-Classic Security Groups Inbound Rules Set To All IPs And All Ports (No Resources)
EC2-Classic Security Groups Inbound Rules Set To All Ports
EC2-Classic Security Groups Inbound Rules Set To All Ports (No Resources)
EC2-Classic Security Groups Inbound Rules With Dangerous Ports Exposed
EC2-Classic Security Groups Inbound Rules With Dangerous Ports Exposed (No Resources)
EC2-Classic Security Groups Inbound Rules With Possible CIDR Prefix Mistake
EC2-Classic Security Groups Inbound Rules With Possible CIDR Prefix Mistake (No Resources)
EC2-Classic Security Groups Inbound Rules With Potentially Dangerous Port 22 Exposed
EC2-Classic Security Groups Inbound Rules With Potentially Dangerous Ports Exposed
EC2-Classic Security Groups Inbound Rules With Potentially Dangerous Ports Exposed (No Resources)
EC2-Classic Security Groups Inbound Rules With Specific Port 3389 Exposed From Any IP Address
EC2-Classic Security Groups Inbound Rules With Specific Ports Exposed From Any IP Address
EC2-Classic Security Groups Inbound Rules With Specific Ports Exposed From Any IP Address (No Resources)
EC2-VPC Security Groups Inbound Rules Allowing Traffic From Any IP Address
EC2-VPC Security Groups Inbound Rules Allowing Traffic From Any IP Address (No Resources)
EC2-VPC Security Groups Inbound Rules Allowing Traffic From Broad IP Ranges
EC2-VPC Security Groups Inbound Rules Allowing Traffic From Broad IP Ranges (No Resources)
EC2-VPC Security Groups Inbound Rules Set To All IPs And All Ports
EC2-VPC Security Groups Inbound Rules Set To All IPs And All Ports (No Resources)
EC2-VPC Security Groups Inbound Rules Set To All Ports
EC2-VPC Security Groups Inbound Rules Set To All Ports (No Resources)
EC2-VPC Security Groups Inbound Rules With Dangerous Ports Exposed
EC2-VPC Security Groups Inbound Rules With Dangerous Ports Exposed (No Resources)
EC2-VPC Security Groups Inbound Rules With Potentially Dangerous Ports Exposed
EC2-VPC Security Groups Inbound Rules With Potentially Dangerous Ports Exposed (No Resources)
EC2-VPC Security Groups Inbound Rules With Specific Ports Exposed From Any IP Address
EC2-VPC Security Groups Inbound Rules With Specific Ports Exposed From Any IP Address (No Resources)

EC2-VPC Security Groups Outbound Rules Allowing Traffic From Any IP Address
EC2-VPC Security Groups Outbound Rules Allowing Traffic From Any IP Address (No Resources)
EC2-VPC Security Groups Outbound Rules Allowing Traffic From Broad IP Ranges (No Resources)
EC2-VPC Security Groups Outbound Rules Allowing Traffic To Broad IP Ranges
EC2-VPC Security Groups Outbound Rules Set To All IPs And All Ports
EC2-VPC Security Groups Outbound Rules Set To All IPs And All Ports (No Resources)
EC2-VPC Security Groups Outbound Rules Set To All Ports
EC2-VPC Security Groups Outbound Rules Set To All Ports (No Resources)
EC2-VPC Security Groups Outbound Rules With Dangerous Ports Exposed
EC2-VPC Security Groups Outbound Rules With Dangerous Ports Exposed (No Resources)
EC2-VPC Security Groups Outbound Rules With Potentially Dangerous Ports Exposed
EC2-VPC Security Groups Outbound Rules With Potentially Dangerous Ports Exposed (No Resources)
EC2-VPC Security Groups With Possible CIDR Prefix Mistake
EC2-VPC Security Groups With Possible CIDR Prefix Mistake (No Resources)
Elastic Load Balancers Using An Unencrypted Protocol
Elastic MapReduce Clusters scheduled from Data Pipeline Need IAM Roles
Ensure routing tables for VPC peering are "least access"
Event In CloudTrail That Disabled CloudTrail
Expiring SSL Certificates
Expiring SSL Certificates (Unused)
Failed Management Console Login Attempts
IAM Access Keys That Needs To Be Rotated
IAM Admin User Login
IAM Admin User Password Changed
IAM Admin Users Not Utilizing Multi-Factor Authentication
IAM Master and IAM Manager Roles Are Not Active
IAM Password Policy Disabled
IAM Password Policy Does Not Allow Users To Change Their Own Password
IAM Password Policy Does Not Contain At Least One Uppercase Letter
IAM Password Policy Does Not Have Password Expiration
IAM Password Policy Does Not Prevent Password Reuse
IAM Password Policy Does Not Require Lowercase Letter
IAM Password Policy Does Not Require Non-Alphanumeric Character
IAM Password Policy Does Not Require Number
IAM Password Policy Minimum Length Too Short
IAM Policies Granted To IAM Users
IAM Role Policies with Full Admin Privileges
IAM User Policies with Full Admin Privileges
IAM Users Not Attested
IAM Users Not Utilizing Multi-Factor Authentication
IAM Users That Do Not Belong To Groups
IAM Users with Console Access Should Not Have Access Keys That Were Created at Initial User Setup
Ineffective Network ACL Deny Rule
Lambda Functions With Admin Privileges
Load Balancers Without Access Log Enabled

Log Metric Filter and Alarm Do Not Exist for AWS Config Configuration Changes
Log Metric Filter and Alarm Do Not Exist for AWS Management Console Authentication Failures
Log Metric Filter and Alarm Do Not Exist for Changes to Network Access Control Lists (NACL)
Log Metric Filter and Alarm Do Not Exist for Changes to Network Gateways
Log Metric Filter and Alarm Do Not Exist for CloudTrail Configuration Changes
Log Metric Filter and Alarm Do Not Exist for Disabling or Scheduled Deletion of Customer-Created CMKs
Log Metric Filter and Alarm Do Not Exist for Management Console Sign-In without MFA
Log Metric Filter and Alarm Do Not Exist for Route Table Changes
Log Metric Filter and Alarm Do Not Exist for S3 Bucket Policy Changes
Log Metric Filter and Alarm Do Not Exist for Security Group Changes
Log Metric Filter and Alarm Do Not Exist for Usage of "Root" Account
Log Metric Filters and Alarms Do Not Exist for IAM Policy Changes
Log Metric Filters and Alarms Do Not Exist for Unauthorized API Calls
Log Metric Filters and Alarms Do Not Exist for VPC Changes
Long Running Elastic MapReduce Cluster Need Role
Multi-Region CloudTrail Enabled
Multiple MySQL Vulnerabilities (January 2013 Critical Patch Update)
MySQL Vulnerability (CVE-2012-1702 - DoS)
MySQL Vulnerability (CVE-2012-2122 - Incorrect Passwords Authenticated)
MySQL Vulnerability (CVE-2013-0383 - DoS In Server Locking)
Network ACLs Allowing All Inbound Traffic
Network ACLs Allowing All Outbound Traffic
New Access Key(s) Created for IAM User
New IAM Admin Users Created Or Granted
New IAM Admin Users Not Attested
No IAM Administrators Group Found
No Support Role Has Been Created To Manage Incidents with AWS Support
Number Of ElastiCache Clusters That Are Not Isolated Within A VPC
Number Of RDS DB Instances That Are Not Isolated Within A VPC
Number Of Redshift Clusters That Are Not Isolated Within A VPC
Password Attacks on AWS Management Console
Passwords Not Reset For > 90 Days
Publicly Accessible AMIs
Publicly Accessible RDS DB Instances
Publicly Accessible RDS DB Instances With Open Security Group
Publicly Accessible Redshift Clusters
Publicly Accessible Redshift Clusters With Open Security Group
RDS Database Master Username Is 'awsuser'
RDS DB Instances Not Enforcing SSL Connections
RDS DB Instances Running on Default Ports
RDS DB Instances With MySQL Security Alert
Redshift Clusters Without Data-At-Rest Encrypted
Redshift Security Groups Inbound Rules Allowing Traffic From Any IP Address
Redshift Security Groups Inbound Rules Allowing Traffic From Any IP Address (No Resources)
Redshift Security Groups Inbound Rules Allowing Traffic From Broad IP Ranges

Redshift Security Groups Inbound Rules Allowing Traffic From Broad IP Ranges (No Resources)
Redshift Security Groups With Possible CIDR Prefix Mistake
Redshift Security Groups With Possible CIDR Prefix Mistake (No Resources)
Regions Without AWS Config Enabled
Regions Without CloudTrail Enabled
Root Account Has Access Keys
Root AWS Account Not Utilizing Multi-Factor Authentication
Root User Accessing AWS Account
Rotation Not Enabled For Customer Created CMKs for KMS Encryption
S3 Buckets Access Granted To User In A Different AWS Account
S3 Buckets Allowing Access via HTTP
S3 Buckets Do Not Have Default Encryption Enabled
S3 Buckets Not Enforcing Server-Side Encryption With A Bucket Policy
S3 Buckets That Allow Any AWS User To Access Billing Report Log Files
S3 Buckets That Allow Any AWS User To Access CloudFront Log Files
S3 Buckets That Allow Any AWS User To Access CloudTrail Log Files
S3 Buckets That Allow Any AWS User To Access S3 Log Files
S3 Buckets That Allow Everyone Access to Billing Reports
S3 Buckets That Allow Everyone Access to CloudFront Log Files
S3 Buckets That Allow Everyone Access to CloudTrail Log Files
S3 Buckets That Allow Everyone Access to S3 Log Files
S3 Buckets With 'Edit Permission' Permission Set To Any AWS User
S3 Buckets With 'Edit Permissions' Permission Set To Everyone
S3 Buckets With 'List' Permission Set To Any AWS User
S3 Buckets With 'List' Permission Set To Everyone
S3 Buckets With 'Upload/Delete' Permission Set To Any AWS User
S3 Buckets With 'Upload/Delete' Permission Set To Everyone
S3 Buckets With 'View Permissions' Permission Set To Any AWS User
S3 Buckets With 'View Permissions' Permission Set To Everyone
S3 Buckets With Any Permission Set To Any AWS User
S3 Buckets With Any Permission Set To Everyone
S3 Buckets With Logging Not Enabled
S3 Buckets with Public Policies
S3 Public Sensitive Objects Stored
S3 Public Sensitive Objects Stored Permission Set To Any AWS User
Security Questions Not Registered
Sensitive Directory Publicly Accessible In S3
SES Domains Without SPF Records Properly Configured
SNS Subscriptions not using HTTPS
SNS Topic not set to Limit Subscriptions to HTTPS
SNS Topic not using HTTPS
SNS Topic Subscribers Not Verified
SNS Topics That Allow 'Everyone' To Publish
SNS Topics That Allow 'Everyone' To Subscribe
SQS Queue Access Granted To User In A Different AWS Account
SQS Queue With Permission Set To Everyone
Stale IAM Admins
Stale IAM User Access Keys
Stale IAM Users
VPC Flow Log Not Enabled
VPC Peering Connections Requester and Peer Not Approved
WorkSpace Failed Logins

Appendix B. Data Evaluated in a Technology Review

This section provides detailed information about the data a Lightstream Certified Cloud Engineer reviews when evaluating your technical environment.

Cost Data

Detailed Billing Not Enabled
Disabled KMS Key
EBS PIOPS Volumes Should Be Converted To General Purpose SSD
EBS Volumes Attached to Stopped EC2 Instances
EC2 Instances Running As Dedicated
EC2 On-Demand Instances Not Using Reserved Instance Pricing
Glacier Total Possible Cost Savings
Heavy Utilization ElastiCache Reserved Nodes Not Fully Utilized
Idle DynamoDB Tables
Idle EC2 Instances
Idle Elastic Load Balancers
Idle ElastiCache Nodes
Idle RDS DB Instances
Idle Redshift Nodes
Medium or Light Reserved EC2 Instances Not Fully Utilized
Previous Generation EC2 Instances Should Be Migrated
Previous Generation ElastiCache Nodes Should Be Migrated
Previous Generation RDS DB Instances Should Be Migrated
Previous Generation Redshift Node Should Be Migrated
RDS On-Demand Instances Not Using Reserved Instance Pricing
RDS PIOPS Volumes Should Be Converted To General Purpose SSD
Reserved EC2 Instances Not Fully Utilized
Unattached EBS Volumes
Unused AMIs
Unused DynamoDB Tables
Unused Elastic IP Addresses
Unused Elastic Load Balancers
Unused WorkSpace(s)

Availability Data

Auto Scaling Groups Not Utilizing Multiple Availability Zones
Automatic RDS Database Backups Disabled
CloudFormation Stack Failed Status
Current AWS Service Limits
Deprecated Oracle Version
DynamoDB Client Errors
DynamoDB System Errors
EBS Volumes With No Recent Snapshots (30 days)
EBS Volumes With No Recent Snapshots (7 days)
EBS Volumes Without A Snapshot
EC2 Errors In Console Output
EC2 Instance Status Checks Failed
EC2 Instances Not Utilizing Termination Protection
EC2 System Status Checks Failed
EC2 Volume Status Checks Failed

Elastic Load Balancers Not Utilizing Multiple Availability Zones
Elastic Load Balancers With Fewer Than Two Healthy Instances
Elastic MapReduce Clusters Terminated with Errors
Elastic MapReduce Clusters with Failed Jobs
Elastic MapReduce Clusters with Failed Steps
Elastic MapReduce Clusters without Termination Protection Enabled
Elastic MapReduce HBase Failed Backup
Instances for Elastic Load Balancer Unevenly Distributed Across Availability Zones
Maintenance Events Scheduled For EC2 Instances
Maintenance Events Scheduled For RDS DB Instances
No Availability Zone Distribution Of EC2 Instances
RDS DB Instance less than 1 GB Of Free Storage
RDS DB Instance less than 1 MB Of Free Storage
RDS DB Instance less than 10% Of Free Storage
RDS DB Instance With Failed Status
RDS DB Instance With Incompatible Parameters Status
RDS DB Instance With Incompatible Restore Status
RDS DB Instance With Storage Full Status
RDS DB Instances Running Out of Memory
RDS DB Instances With Failover Event
RDS Instance With No CloudWatch Alarm For RDS Disk Usage
RDS Instances Configured To Retain Backups For Fewer Than 30 Days
RDS Instances Not Running In Multiple Availability Zones
RDS MySQL DB Instances Nearing Deprecation
Redshift Cluster Less Than 1 GB Of Free Storage
Redshift Cluster Less Than 1 MB Of Free Storage
Redshift Cluster Less Than 10% Of Free Storage
Redshift Databases Without CloudWatch Alarm For Disk Usage
S3 Buckets With SNS Notifications Not Enabled
Services Nearing AWS Service Limits
SES Domains With Failure Status
SES Email Addresses With Failure Status
SQS Message Queue Appears To Be Backed Up
Uneven Availability Zone Distribution Of EC2 Instances
Unhealthy EC2 Instances Attached To Load Balancers
WorkSpace With Unhealthy State

Usage (over- and under-utilization) Data

Activities In RDS Events
Auto Scaling Groups Not Using Cooldown Period
Auto Scaling Groups Referencing Invalid Elastic Load Balancer
Auto Scaling Groups Using EC2 Health Check Instead Of ELB
Auto Scaling Groups with Notifications Not Enabled
Auto Scaling Launch Configuration Referencing Invalid AMI
Auto Scaling Launch Configuration Referencing Invalid Key Pair
Auto Scaling Launch Configuration Referencing Invalid Security Group
Auto Scaling Launch Configuration Using Previous Gen EC2 Instances
CloudFront Distributions With Logging Not Enabled
DB Instances With Excessive Number Of Rules
DB Security Groups With Excessive Number Of Rules
DB Security Groups With Excessive Number Of Rules (No Resources)
DB Security Groups without DB Instances

DynamoDB Throttled Requests
EBS Volumes With Excessive Snapshots
EC2 Auto Scaling Groups Not Being Utilized
EC2 Instance Stopped Due To Scheduled Retirement
EC2 Instances Encountered Internal Error
EC2 Instances Not Attached To An Auto Scaling Group
EC2 Instances Not Launched As EBS-Optimized Using IOPS EBS Volume
EC2 Instances With Excessive Number Of Rules
EC2 Instances With Source/Destination Check Set to False
EC2 Snapshots Of Deleted AMIs
EC2-Classic Security Groups With Excessive Number Of Rules
EC2-Classic Security Groups With Excessive Number Of Rules (No Resources)
EC2-Classic Security Groups With No EC2 Instances
EC2-VPC Security Groups with No Resources
Elastic Load Balancers With HTTP Errors
Elastic MapReduce Missing Blocks
Elastic MapReduce Open Map Slots
Elastic MapReduce Open Reduce Slots
Excessive Log Files
Failed Activities in Auto Scaling Logs
Failed Activities In RDS Events
Large Objects Being Stored Within S3
New Payee Accounts Discovered While Processing Your Detailed Billing Report
Over-Utilized DynamoDB Table Reads
Over-Utilized DynamoDB Table Writes
Over-Utilized EC2 Instances
Over-Utilized Elastic Load Balancers
Over-Utilized ElastiCache Nodes
Over-Utilized RDS DB Instances
Payee Account With No Credentials Added
RDS DB Instance Master Credentials Reset
RDS Instances With Class Limited to 500 Mbps For Provisioned IOPS Storage
RDS Instances With Class Not Optimized For Provisioned IOPS Storage
RDS Instances Without Notifications Enabled
RDS Micro Oracle DB Instances
RDS Read Replicas With Different Instance Class Than Source DB
RDS Read Replicas With No Source DB Instance
Redshift Clusters in Maintenance Mode
Redshift Security Groups without Redshift Clusters
S3 Buckets With Lifecycle Object Expiration Enabled
S3 Buckets With Website Enabled
S3 Writing Log Files To A Bucket That Has Logging Enabled
Server Access Logs in S3 Bucket
SES Domains Not Utilizing DKIM Signing
SES Email Addresses Not Utilizing DKIM Signing
Spot Request Terminated Because Spot Price Exceeds Max Bid
Suspended Auto Scaling Groups
Under-Utilized DynamoDB Table Reads
Under-Utilized DynamoDB Table Writes
Under-Utilized EC2 Instances
Under-Utilized Elastic Load Balancers
Under-Utilized ElastiCache Nodes
Under-Utilized RDS DB Instances

Unsupported RDS Instances Should Be Upgraded
Untagged Resources
Unused CloudWatch Alarms
Unused Elastic Network Interface
Unused Key Pairs

AWS Trusted Advisor Data

Amazon Aurora DB Instance Accessibility
Amazon EBS Provisioned IOPS (SSD) Volume Attachment Configuration
Amazon EBS Public Snapshots
Amazon EBS Snapshots
Amazon EC2 Availability Zone Balance
Amazon EC2 to EBS Throughput Optimization
Amazon RDS Backups
Amazon RDS Idle DB Instances
Amazon RDS Multi-AZ
Amazon RDS Public Snapshots
Amazon RDS Security Group Access Risk
Amazon Route 53 Alias Resource Record Sets
Amazon Route 53 Deleted Health Checks
Amazon Route 53 Failover Resource Record Sets
Amazon Route 53 High TTL Resource Record Sets
Amazon Route 53 Latency Resource Record Sets
Amazon Route 53 MX Resource Record Sets and Sender Policy Framework
Amazon Route 53 Name Server Delegations
Amazon S3 Bucket Logging
Amazon S3 Bucket Permissions
Amazon S3 Bucket Versioning
Auto Scaling Group Health Check
Auto Scaling Group Resources
Auto Scaling Groups
Auto Scaling Launch Configurations
AWS CloudTrail Logging
AWS Direct Connect Connection Redundancy
AWS Direct Connect Location Redundancy
AWS Direct Connect Virtual Interface Redundancy
CloudFormation Stacks
CloudFront Alternate Domain Names
CloudFront Content Delivery Optimization
CloudFront Custom SSL Certificates in the IAM Certificate Store
CloudFront Header Forwarding and Cache Hit Ratio
CloudFront SSL Certificate on the Origin Server
EBS Active Snapshots
EBS Active Volumes
EBS General Purpose SSD (gp2) Volume Storage
EBS Magnetic (standard) Volume Storage
EBS Provisioned IOPS (SSD) Volume Aggregate IOPS
EBS Provisioned IOPS SSD (io1) Volume Storage
EC2 Elastic IP Addresses
EC2 On-Demand Instances
EC2Config Service for EC2 Windows Instances
ELB Active Load Balancers
ELB Connection Draining

ELB Cross-Zone Load Balancing
ELB Listener Security
ELB Security Groups
Exposed Access Keys
High Utilization Amazon EC2 Instances
IAM Access Key Rotation
IAM Group
IAM Instance Profiles
IAM Password Policy
IAM Policies
IAM Roles
IAM Server Certificates
IAM Use
IAM Users
Idle Load Balancers
Kinesis Shards per Region
Large Number of EC2 Security Group Rules Applied to an Instance
Large Number of Rules in an EC2 Security Group
Load Balancer Optimization
Low Utilization Amazon EC2 Instances
MFA on Root Account
Overutilized Amazon EBS Magnetic Volumes
PV Driver Version for EC2 Windows Instances
RDS Cluster Parameter Groups
RDS Cluster Roles
RDS Clusters
RDS DB Instances
RDS DB Parameter Groups
RDS DB Security Groups
RDS DB Snapshots Per User
RDS Event Subscriptions
RDS Max Auths per Security Group
RDS Option Groups
RDS Read Replicas per Master
RDS Reserved Instances
RDS Subnet Groups
RDS Subnets per Subnet Group
RDS Total Storage Quota
Security Groups - Specific Ports Unrestricted
Security Groups - Unrestricted Access
Service Limits
SES Daily Sending Quota
Unassociated Elastic IP Addresses
Underutilized Amazon EBS Volumes
Underutilized Amazon Redshift Clusters
VPC Elastic IP Address
VPC Internet Gateways
VPN Tunnel Redundancy