National Cyber Security Centre

Securing Amazon Web Services

New Zealand's National Cyber Security Centre is hosted within the Government Communications Security Bureau

May 2020

Overview

1. This document contains guidance designed to help your organisation commence the process of securing cloud resources in Amazon Web Services (AWS). We provide advice on:
    a. important steps to take with AWS's Identity and Access Management (IAM) system;
    b. key security tools and services that will help you on your path to building a secure AWS environment.

Who is this advice for?

2. This advice has been produced for organisations who may be considering the use of AWS cloud services and resources for the first time, or those who are already using this technology and scaling it up at pace.
3. This advice is designed for organisation that have not yet carried out a full certification and accreditation (C&A) process on AWS due to the impact of COVID-19. However, organisations still need to have a plan in place to ensure that C&A can be carried out as soon as practicable. The full context for usage and risks associated with AWS services needs to be documented and understood.
4. This advice is not designed to supersede AWS instances which have been assessed and approved by an accreditation authority in your organisation for your own business use.

Making risk-based decisions in difficult times

5. We recognise that the COVID-19 pandemic presents a significant change to the way that many organisations function, and that fast-paced cloud adoption is a challenge some organisations are facing.
6. For government agencies, the NZ Information Security Manual (NZISM) states you should carry out C&A on platforms as a core part of your security assurance processes. It is prudent for all organisations to complete a security assessment before using a new platform. However, while you may have not had time to complete C&A before you start using AWS, you can conduct a basic risk assessment to clearly articulate:

a. the context for your use of AWS;

b. why you are using AWS services;

c. the security and privacy steps you are taking;

d. your plan for building out a robust security assurance programme for your AWS resources.

7. You should have a plan to complete C&A as soon as is practicable.

8. Public service organisations should contact the Government Chief Digital Officer's (GCDO) team. You can request the risk assessment and service security certificate they have produced for AWS Infrastructure as a Service (IaaS) resources.

Important Steps for AWS Identity and Access Management

9. When creating an AWS account, you specify an email address and password to sign in to the AWS Management Console. When you sign in using these credentials, you are accessing the console by using your *root account*. As per AWS guidance, you should not use your root account for day-to-day administration of your AWS resources. Following security best practices can help to prevent your root account from being compromised. This is vitally important because your root account has access to all the services and resources in your account.

10. Make sure you take the time to protect your root account by following the below advice and carefully managing your root account.

Create a strong password for your AWS resources

11. To help ensure that you protect your AWS resources, first set a strong password with a combination of letters, numbers, and special characters. You should build an AWS password policy that meets the password requirements of the NZISM.

12. For more information about password policies and creating strong passwords, see: Setting an Account Password Policy for IAM Users.

Use a group email alias with your AWS account

13. If for any reason you are unavailable to respond to an AWS notification or manage your AWS Cloud workloads, using a group email alias with your AWS account means other trusted members of your organisation can manage the account in your absence.

Enable multi-factor authentication

14. Multi-factor authentication (MFA) is a security capability that provides an additional layer of authentication on top of your username and password. When using MFA, after you sign in with your username and password you must also provide an extra piece of information that only you have physical access to, which can come from a dedicated MFA hardware device or an app on a phone.

15. You must select the type of MFA device you want to use from the list of supported MFA devices. If you choose a hardware MFA device, ensure that you keep it in a secure location. If you are using a virtual MFA device (such as a phone app), think about what might happen if your phone is lost or damaged. One approach is to keep the virtual MFA device you use in a safe place. Another option is to activate more than one device at the same time, or to use a virtual MFA that has options for device key recovery.

16. To learn more about MFA, watch this video and see also: Securing Access to AWS Using MFA and Enabling a Virtual Multi-Factor Authentication (MFA) Device.

Set up AWS IAM users, groups, and roles for daily account access

17. To manage and control access and permissions to your AWS resources, use AWS Identity and Access Management (IAM) to create users, groups, and roles. When you create an IAM user, group, or role, it can access only the AWS resources to which you explicitly grant permissions, which is also known as least privilege.

18. If you are the account owner, AWS recommends that you create a separate IAM user for yourself for daily use of your resources (separating your administrator and user accounts). See: Now Create and Manage Users More Easily with the AWS IAM Console.

Delete your account's access keys

19. You can allow programmatic access to your AWS resources from the command line or for use with AWS APIs. However, AWS recommends that you do not create or use the access keys associated with your root account for programmatic access. In fact, if you still have access keys, delete them. Instead, create an IAM user and grant that user only the permissions needed for the APIs you are planning to call. You can then use that IAM user to issue access keys. To learn more, see: Managing Access Keys for Your AWS Account.

Important Security Tools in AWS

20. While IAM is important, it is not the only security consideration when starting to use AWS. The points below contain high-level advice to get you started with using a number of AWS services that can help your security, monitoring and logging: CloudTrail, CloudWatch and Trusted Advisor. You may want to use some or all of these services depending on how well and how quickly you can ingest your AWS logs into your existing security monitoring and logging tools.

Enable CloudTrail for all AWS resources

21. You can track all activity in your AWS resources by using AWS CloudTrail. Even if you initially do not know how to use CloudTrail, turning it on now can help AWS Support and your AWS solutions architect later if they need to troubleshoot a security or configuration issue. To enable CloudTrail logging in all AWS regions, see: AWS CloudTrail Update – Turn On in All Regions and Use Multiple Trails. To learn more about CloudTrail, see: Turn On CloudTrail: Log API Activity in Your AWS Account.

Enable CloudWatch for all AWS resources

22. While CloudTrail is an important diagnostic and security tool, CloudWatch is a critical logging, monitoring and health tool for AWS resources.

23. We recommend you turn on CloudWatch for all of your AWS resources. As per our advice on moving to the cloud, you should be logging your cloud resources. We understand that it may not be possible to actively monitor all of your logs when you start using AWS. However, CloudWatch provides an easily implemented logging and alerting tool that you should be using either as–is, or ingesting its logs into your existing logging and security monitoring tools. We recommend you set up an alert whenever CloudWatch is disabled on a resource.

AWS Trusted Advisor

24. AWS Trusted Advisor is a reporting and monitoring tool you can use to provide additional checks on security settings and to confirm whether resources are complying with policies and are appropriately configured. For example, some of the basic security settings that Trusted Advisor can scan for include S3 bucket permissions (a number of data breaches in recent years have happened due to S3 buckets having loose permissions), checking your CloudTrail logging, security settings, searching for exposed access keys and IAM settings.

25. As a new user of AWS, Trusted Advisor can be a useful tool to help you keep visibility of your AWS resources and ensure that your policies and settings are being applied across your accounts.

Next Steps

26. As your AWS usage grows or you begin managing multiple AWS accounts, you may need to start diving deeper into security topics. For more information, see the following:

    - AWS Secure Initial Account Setup
    - Introduction to AWS Security whitepaper
    - AWS Cloud Security Resources
    - AWS Security Best Practices whitepaper
    - Security by Design
