Top 10 Configuration Risks in AWS

Remediation Begins with Discovery

Amazon Web Services (AWS®) is a flexible, agile cloud platform that is easy to set up and configure. Resources like repositories and EC2 instances can be set up quickly so workloads can immediately begin to take advantage of the cloud.

AWS applies the Shared Responsibility Model to distinguish the different aspects of security management. AWS owns the infrastructure, physical network, and hypervisor. The enterprise owns the workload OS, apps, virtual network, and access to its tenant environment/account and the data.

When you flip the switch and make it public, though, what doors are you leaving open?

Proper configuration can get tricky if you don't know what you don't know. Even experts can miss avoidable, high-risk vulnerabilities for their cloud instances.

Before any organization can be effective at fixing security issues, it must first understand the risks its cloud environment could likely face. What follow are the 10 most common security risks and misconfigurations found in AWS deployments.

Remediation begins with discovery.

PRISMA™
BY PALO ALTO NETWORKS

No. 1: Configuration Permits Too Much Network Access

An unsecured or invalid Network Access Control List is in use and present in the default configuration.

Why is this a Security Risk?

An unsecured NACL is allowing too much network access to your AWS Virtual Private Cloud (VPC).

The default NACL is too lazy to offer much protection, and a poorly constructed NACL won't be of much use, either. This is the most common high-level risk and should be one of the first things you fix to lock down access to your VPC and AWS services.

Why is this Alert Important?

Virtual Private Clouds are supposed to be private. With an unsecured NACL, you have no idea who's gaining access, and your VPC's data could be at risk. Keep access locked down, and only allow access to those devices and locations that need it.

An Unsecured VPC Puts Your Data in Danger

Unsecured networks can expose customer data and personal data as well as lead to legal and financial risks. New network-accessible vulnerabilities are discovered all the time, but even old vulnerabilities can lead to data breaches and open gates for bad actors. The best, most comprehensive defense is to secure your network with a strong NACL.

How is it Remediated?

You can mitigate this risk by configuring a non-default NACL and applying it to your VPC. Your NACL should be restrictive, only permitting the valid internet traffic required to operate your applications and services while delivering a high quality of service to your customers.

PRISMA™
BY PALO ALTO NETWORKS

No. 2: Administrative SSH Login is Accessible From Anywhere

This means the entire internet has access to connect to Transmission Control Protocol (TCP) port 22.

Why is this a Security Risk?

AWS defaults to this level of access. Since many users, especially those new to AWS, aren't aware of this out-of-the-box configuration and its potential security risks, this alert is quite common. In fact, Prisma™ Public Cloud (formerly RedLock) security and compliances triggers alerts for this SSH vulnerability almost as often as the risk at the top of the charts. With occurrence frequency three times that of the No. 3 risk in the top 10, this represents an avoidable, high-risk instance that requires immediate remediation by AWS users.

Why is this Alert Important?

If everyone can access and connect to TCP port 22, anyone can potentially be an attacker. Too much access increases the level of risk, especially when it comes to admin accounts. A breach of this nature opens the door to denial-of-service attacks and even irretrievable loss of data critical for sustaining operations. Such attacks can cause significant revenue loss and expensive legal challenges.

How are they Remediated?It's simple.

Reduce the access to TCP port 22. To do this, you can:

- Limit permitted IP addresses allowed to communicate to destination hosts on TCP port 22.
- Use the static office or home IP addresses of your employees as the permitted hosts.
- Deploy a bastion host with two-factor authentication.
- Make that host the only permitted IP to communicate with any other nodes inside your account.

Mitigation begins with discovery, so paying attention to and dealing with these alerts is critical to establishing reliable, continuous security for your assets deployed on AWS.

The Risks are real

In 2014, CodeSpaces.com was forced to shut down after its account on AWS Elastic Compute Cloud (EC2) was compromised and hackers deleted almost all of the company's digital assets. In a higher-profile incident in 2015, developers at Ashley Madison simply forgot to mitigate their AWS cloud security risk, exacerbating an already devastating breach.

PRISMA™ BY PALO ALTO NETWORKS

No. 3: You're Only Using Single-Factor Authentication

Multi-factor authentication is not enabled for your AWS user accounts.

Why is this a Security Risk?

You haven't configured your AWS user accounts to use MFA. This leaves your AWS accounts open to the simplest of hacks: bad passwords.

Why is this Alert Important?

MFA is one of the best ways to secure user accounts. It ensures that gaining access to the AWS control panel requires not only something the user knows a password but also something the user possesses, such as a hardware token. This additional layer of protection means you are not one stolen password away from a breach. If someone gains unauthorized access to your AWS user accounts, they might have access to sensitive parts of your AWS configuration, private data, and important services.

Single-factor authentication increases your vulnerability

Passwords are easy to crack. Sometimes, they don't even need to be cracked, such as when French TV network TV5Monde accidentally exposed important passwords on the air in 2015. If your user accounts only need a password to be accessed, it's possible for anybody with the password or the ability to brute-force the password to gain access.

How Is It Remediated?

Mitigation requires enabling MFA in your AWS account. You'll get to decide between a number of different hardware and software options for authentication token generation. AWS will walk you through the selection.

PRISMA™ BY PALO ALTO NETWORKS

No. 4: Unused Access Keys Are Available

Old and unused AWS access keys remain enabled in the system.

Why is this a Security Risk?

Sarah left the company two years ago. Part of her job involved AWS management, so her access keys open a lot of doors. Did anybody delete or deactivate her account when she left?

It's easy to have unused, old access keys laying around. People leave the company, applications and servers go into disuse, and old devices are replaced and forgotten.

Why is this Alert Important?

Old, unused credentials might still be stored in retired hardware or forgotten software, or retained by ex-employees. It's important to keep access to your AWS resources locked down to just known actors. Disabling or removing unnecessary credentials will reduce the window of opportunity for malicious use of compromised credentials.

Stale and unused access credentials can threaten your information security

Passwords and security credentials end up in unexpected places. This happens more often than you might think. In 2014, secondhand mobile phones were used to access AT&T customer data. Keeping strict control of access keys means they won't fall into the hands of attackers.

How Is It Remediated?

Prisma Public Cloud notifies you of each account that has old security credentials. It's then a simple matter to use the AWS Identity and Access Management (IAM) console to delete or deactivate the unnecessary keys.

PRISMA™ BY PALO ALTO NETWORKS

No. 5: Audit Logging is Not Tracking AWS Activity

No CloudTrail audit logs are being kept for AWS services in a region.

Why is this a Security Risk?

Great audit tools are available in AWS, but you don't have them enabled. This means all kinds of activity could be going on right under your nose, but you have no way to tell.

Why is this Alert Important?

Without audit logging, you may as well be flying blindfolded. If you don't know what's going on, how will you know if you're practicing good IT security? AWS offers a superior audit logging service called CloudTrail®, which provides information you'll need to know who's accessing your systems.

Ignorance is bliss, except in information security

There's nothing more embarrassing than being unaware of a security breach. In the massive 2014 eBay® data breach, the lag time before discovery gave hackers a huge head start. Audit logs can give you a leg up on noticing unusual AWS activity. Insufficient or absent audit logs endanger both your company's data and your customers' information.

How Is It Remediated?

o be as secure and auditable as possible, always enable AWS CloudTrail. CloudTrail offers audit-logging capabilities to AWS users. To maintain consistent best practices, enable it for every account and region.

PRISMA™ BY PALO ALTO NETWORKS

No. 6: Anybody Can Access Windows Remote Desktop

Permission to access the Windows Remote Desktop Protocol (RDP) has been granted to everybody.

Why is this a Security Risk?

Don't pile bricks in front of your Windows. If your AWS network configuration is too permissive, any device, anywhere, can access RDP on your systems. This can happen with a default configuration or by way of a later misconfiguration. Luckily, it's easy to mitigate.

Why is this Alert Important?

If everyone can access and connect to your RDP ports, anyone can potentially be an attacker. Too much access increases the level of risk, especially when it comes to management protocols like this one. A breach of this nature opens the door to password hacks, complete takeovers of your Windows servers, and even irretrievable loss of critical data and customer information. Such attacks can cause significant revenue loss, expensive legal challenges, and other serious consequences.

Protecting Your Windows Servers Is Vital

Microsoft Windows® has more reported security vulnerabilities than its competitors. The Windows RDP has had its share of crippling vulnerabilities in the past, and it's safe to say it will have more in the future. Lock this protocol down and only allow access from trusted devices and locations.

How Is It Remediated?

Restrict access to management protocols solely to specific devices and locations within your control. Unless there's a specific reason for somebody to gain access to Windows RDP on a server, keep it locked down.

PRISMA™
BY PALO ALTO NETWORKS

No. 7: Anybody Can Look Through Your Playbook

Internet Control Message Protocol (ICMP) is accessible by everybody, giving too much information to potential attackers.

Why is this a Security Risk?

The network configuration for your AWS infrastructure is allowing anybody to access Internet Control Message Protocol information.

Why is this Alert Important?

ICMP is a family of network protocols your IT team uses to make sure your network is working properly. When the network is open to everybody, important information could be leaked. Bad actors might discover things about your AWS infrastructure that they shouldn't know. Although this information might not constitute a direct threat, it makes an attacker's job much easier. It's like opening up your playbook and letting the opposing team learn all your tricks.

Your AWS infrastructure is not for prying eyes

Hackers can use ICMP to probe for all kinds of information, from port scanning to network topology and even OS fingerprinting. It gets worse: the teardrop attack could use ICMP to remotely reboot certain machines. Keep ICMP usage limited to those who really need it: your DevOps team.

How Is It Remediated?

We recommend you restrict ICMP solely to devices and locations within your organization. This can be done through AWS configuration.

PRISMA™ BY PALO ALTO NETWORKS

No. 8: Anybody Can Connect to Your MySQL Database

Your MySQL database is wide open—and anybody, anywhere can try to access it.

Why is this a Security Risk?

If your AWS configuration allows global access to MySQL®, this means that anybody, anywhere, can connect to your database and potentially access it.

Why is this Alert Important?

Let's assume you don't want to give the entire world access to your MySQL database. The wrong signature can leave your database wide open. MySQL has a robust security system built into it, but that doesn't mean a zero-day vulnerability won't give unprecedented access to a bad actor.

A compromised database can be crippling. Every piece of information stored in the database can be accessed, leading to a complete data breach.

Your MySQL Database Isn't For Everyone

Allowing global access to your MySQL server is a bad idea. There are literally tutorials available on methods of hacking MySQL. Lock this network access down tight to only trusted devices and locations. Better yet, make sure they are all local to the MySQL database and using encrypted connections.

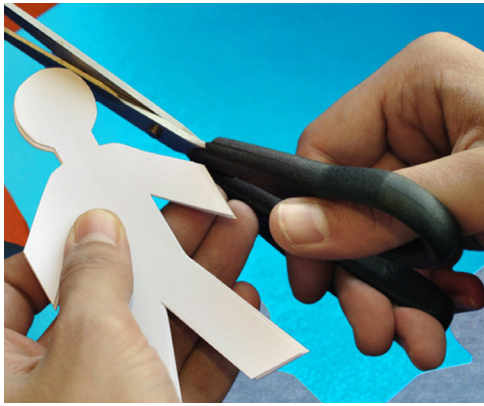
How Is It Remediated?

Restrict network access to MySQL solely to trusted devices. Do not let the entire galaxy connect to your database.

PRISMA™ BY PALO ALTO NETWORKS

No. 9: IAM User Has Policy Directly Assigned

Giving access to individual users, instead of groups and roles, can result in excessive and unnecessary privileges being granted.



Why is this a Security Risk?

In AWS, a policy is an entity that defines permissions. Policies can be attached to an identity or a resource, and are stored as JSON documents and attached as identity-based policies in IAM. If they are not assigned correctly to individuals, they will be broadly applied to too many users through their inclusion in groups, or to resources and the users who have access to those resources.

Why is this Alert Important?

Some Identity and Access Management policies are assigned to users, not groups or roles. By default, IAM users, groups, and roles have no access to AWS resources. Reducing access management complexity can reduce opportunity for users to inadvertently receive or retain excessive privileges.

Assign IAM Policies Appropriately

We recommended applying IAM policies to groups and roles, not directly to users. Assigning privileges at the group or role level reduces the complexity of access management as the number of users grow.

How Is It Remediated?

Create an IAM group, assign a policy to it, and add your users to the group. Finally, go into the IAM console and detach users from policies with which they should not be associated.connect to your database.

PRISMA™ BY PALO ALTO NETWORKS

No. 10: EBS Volume Encryption is Not Enabled

Ensure encryption at the host layer and in your EC2 instances.

Why is this a Security Risk?

Hackers can access threat models from unencrypted data left on unused resources or second-hand hardware. When data is not encrypted, it's easily accessible, which could result in a loss of data, including keys or other access data that could lead a hacker back to your environment with easy access.

Why is this Alert Important?

Elastic Block Store (EBS) volumes do not have volume encryption enabled. EBS volume encryption is a powerful capability that will help protect your data at rest on an EBS volume.

Encrypt. Always Encrypt.

Most auditors are going to require that data be encrypted at rest, so for that requirement alone, it's wise to encrypt. Even if that's not mandated, EBS volume encryption will provide protection against unintended access to your resources.

How Is It Remediated?

To enable EBS volume encryption, you need to create a new, encrypted EBS volume and migrate the old data to the new volume.

PRISMA™ BY PALO ALTO NETWORKS

Facing Security Risks with Open Eyes

Know what you need to know before you need it.

Undetected, these errors probably don't affect day-to-day operations. However, they leave the door open for potentially serious problems.

Prisma Public Cloud captures and analyzes tens of billions of events each month across AWS, Microsoft Azure®, and Google Cloud Platform (GCP™).

These events come from companies both large and small with a broad range of experience—from cloud veterans to first-timers.

Every event is analyzed, prioritized, and categorized using our risk engine.

Start your free trial today.

PRISMA™ BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com