Robel Michael Gebregergis

Supply Chain Risks From Cloud Security Posture Management Services

Master's thesis in Applied Computer and Information Technology
Oslo Metropolitan University
Faculty of Technology, Art and Design

Title:

Supply Chain Risks from Cloud Security Posture Management Services

By:
Robel Michael, Gebregergis

Supervisors:
Ebenezer Paintsil & Lothar Fritsch

Oslo Metropolitan University, Faculty of Technology, Art and Design
Oslo 2023

Supply Chain Risks from Cloud Security Posture Management Services

Robel Michael Gebregergis

May 2023

Abstract

Cloud security posture management services (CSPMSs) support security efforts in the industry by providing more convenient ways of detecting misconfigurations, threats, and vulnerabilities in the cloud. The capabilities of a CSPMS depend on the level of access assumed by these management tools or services. CSPMS may obtain access to everything including keys, secrets, environmental variables, certificates, and sensitive data or files because of the nature of the privileges they assume before they scan the cloud environment. CSPMS clients are often naive about the nature of the privileges these services or tools assume, the amount of sensitive data they collect, and the supply chain risks associated with the implementation of the service or tools. Consequently, they often rollout default configurations or policies prescribed by vendors with little or no regards to supply chain risks since they are sold to them as read only policies. This thesis investigates supply chain risks associated with CSPMS and how least privileged principles can be used to mitigate such risks using comparative studies, experimentation, and analysis of default permissions of some of the existing CSPM services.

Acknowledgments

I would like to begin by expressing my profound gratitude to my supervisors, Associate Professor Ebenezer Paintsil and Professor Lothar Fritsch. Their invaluable guidance, unwavering support, and extraordinary patience throughout my master's thesis study have been truly exceptional. Their profound expertise and extensive experience have consistently served as a source of inspiration and have been instrumental in guiding me throughout the research process.

Furthermore, I extend my deep appreciation to my sister, Ruta Michael, and my entire family for their unwavering presence and belief in my abilities have played a pivotal role in my academic journey. Their support has played a pivotal role in my academic journey, providing encouragement and motivation during this period.

Finally, I would like to express my sincere appreciation to Oslo Metropolitan University for granting me the opportunity to pursue and successfully complete this master's program.

Contents

List of Tables

List of Figures

List of Acronyms

CC Cloud Computing

PoLP Principle of Least Privilege

MAC Mandatory Access Control

DAC Discretionary Access Control

RBAC Role-Based Access Control

CSPMS Cloud Security Posture Management Service

CI/CD Continuous Integrations / Continuous Deployment

IaC Infrastructure as Code

API Application Programming Interface

GUI Graphical User Interface

RPA Robotic Process Automation

SOC Security Operation Center

ABAC Attribute-Based Access Control

AWS Amazon Web Services

IAM Identity and Access Management

Chapter 1

Introduction

Cloud computing (CC) offers numerous benefits such as increased performance, better flexibility, scalability and cost efficiency [1, 2, 3]. This has led to the widespread use of CC services across organizations [4, 5, 6] However, security threats and compliance violations in cloud environments remain major issues. Recent studies indicate that most cloud security breaches are caused by misconfigurations, poor access management, and inadequate audit logging [5, 1, 4, 7]. These breaches can result in the exposure of sensitive data and significant financial losses for organizations [5].

As a result, organizations are increasingly recognizing the importance of implementing cloud security auditing tools and services such as *Cloud Security Posture Management Services* (CSPMSs) [8]. CSPMS tools offer more effective and convenient methods of identifying misconfigurations and mitigating compliance violations by performing scans in your cloud environment [9, 10]. Moreover, these tools help automate the security and remediation processes while offering continuous real-time risk and threat monitoring capabilities in the cloud [2, 6]. This significantly enhances the overall security posture of cloud environments [6, 9].

However, CSPMS tools require specific permissions to perform their scans [6]. The extent of these permissions can vary, ranging from excessive to precise, depending on how the tools are implemented. Although most CSPMS tools rely on read-only access permissions to perform their scans, it is unclear whether this level of access permission aligns with the *principle of least privilege* (PoLP), which is essential for safeguarding sensitive data and mitigating risks such as supply chain risk.

CSPMS clients however, often relying on the recommendations of CSPMS vendors, deploy these permissions without considering their own security requirements

or adherence to the PoLP. Consequently, they overlook the potential implications of these read-only access permissions and may unknowingly provide excessive permissions to these tools. This oversight exposes them to significant risks including supply chain risks and the potential collection of sensitive data.

The aim of this study is to address this gap in scientific research by conducting comparative studies, experiments, and analyses in existing CSPMS tools. The research will investigate the supply chain risks associated with the default permissions of these tools. Moreover, the study also aims to examine whether the existing CSPMS tools rely on over-privileged permissions to perform their scans. Lastly, the effectiveness of implementing the PoLP as a mitigation strategy will be evaluated. The findings of this research will provide valuable insights to organizations utilizing CSPMS tools and shed light on the associated supply chain risks.

To the best of our knowledge, no prior studies have investigated the implications of supply chain risks in the context of CSPMS tools, despite the potential risks associated with granting these tools excessive permissions.

1.1 Problem Statement

The main aim of this thesis is to conduct a comprehensive analysis and evaluation of the potential supply chain risks associated with the default permissions in CSPMS tools. The research also aims to examine whether the existing CSPMS tools rely on over-privileged permissions for performing their scans in cloud environments. Furthermore, the study will explore whether adhering to the PoLP can mitigate the excessive permissions given to these tools while enabling effective security scans.

The problem statement of the thesis is defined by the following research questions:

Q1: Do the default permissions required for running the CSPMS scans pose any supply chain risk?

Q2: Do the existing CSPMS tools deploy over-privileged permissions to perform their scans?

Q3: Is it possible to reduce the permissions of these CSPMS tools while still ensuring their effective security scans?

These questions lay the foundation for the research, enabling an in-dept investigation into the potential supply chain risks associated with CSPMSs tools.

The findings of this study will contribute to a better understanding of the supply chain risks associated with implementing the default permissions in CSPMs within cloud environments. Additionally, the research will provide valuable recommendations for improving security practices for CSPMS tools, aiming to enhance overall security measures in cloud environments.

1.2 Thesis Outline

Thus far, we have discussed the introduction and problem statement of the thesis. This sub-chapter, we will briefly discuss the structure of the rest of the thesis, which will be as follows:

Chapter 2 provides a comprehensive background theory on essential concepts deemed necessary for understanding the thesis.

Chapter 3 discusses relevant literature related to the thesis topic.

Chapter 4 describes the methodology used for performing the study, including an in-depth description of the tools and technologies.

Chapter 5 presents the assessment results along with a comprehensive analysis of the findings.

Chapter 6 presents the conclusion of the thesis, summarizing the key findings and their implications. It also offers recommendations for further developments and potential avenues for future research in the field.

Chapter 2

Background Theory

This chapter provides a comprehensive background theory on essential concepts that are crucial for understanding the thesis. The chapter will cover a range of topics, including *Cloud Security Posture Management* (CSPM), *Access Control in Cloud Computing*, *Supply Chain risks*, the *Princliple of Least Privilege* (PoLP), and *Identity and Access Management in Cloud* (IAM).

2.1 Cloud Security Posture Management

Cloud Security Posture Management (CSPM) refers to cloud security audit tools and services that aim to identify and mitigate the various security risks inherent in cloud environments. These tools use various practices and technologies to perform scans in cloud environments, automate security assessments, and effectively mitigate the risks associated with the cloud [1, 6].

CSPM tools are used to identify and mitigate misconfigurations in cloud environments [9, 11]. This is achieved by scanning and analyzing the configurations of cloud resources across cloud workloads [2].

Moreover, CSPM tools provide organizations with compliance assurance by assessing their cloud environment against established security best practices and regulations, such as the CIS Benchmarks, ISO 27001, SOC 2, and PCI-DSS [12, 13]. This ensures the cloud environment is secure and complaint with industry's best security standards.

Furthermore, CSPM tools provide organizations with continuous real-time risk and threat monitoring capabilities [6, 10]. This facilitates the detection of misconfigurations, policy violations, and excessive privileges [2]. Additionally, by

integrating with cloud-native and DevOps tools such as *Continuous Integration and Continuous Deployment* (CI/CD) pipelines and *Infrastructure as Code* (IaC), CSPM tools offer security teams direct remediation guidance through explicit instructions to address the aforementioned risks [1]. Consequently, resulting to enhanced efficiency of the security operations center (SOC) [6].

In addition to the aforementioned features, advanced CSPM tools leverage *Robotic Process Automation* (RPA) systems to proactively address cloud risk concerns before breaches occur. These systems utilize enriched data sources and intuitive query tools to address any identified risks [12].

CSPM's automated risk assessment and mitigation processes are applicable across the different CC service models, including *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), and *Software as a Service* (SaaS). Additionally, they can also be deployed in various cloud environments, including hybrid, multi-cloud, and container deployment systems [8, 1].

In summary, CSPM tools and services offer several benefits and functionalities for organizations operating in cloud environments. These include continuous real-time monitoring capabilities, comprehensive visibility and control of cloud resources, automated detection of misconfigurations, automated remediation mechanisms for identified threats, and compliance assurance with industry's best standards and regulations. By providing these capabilities through a centralized platform, CSPM tools enable organizations to effectively manage, identify, and mitigate the security risks associated with their cloud environment. [2, 6, 8]

2.1.1 Cloud Security Posture Management Implementation: Agent-based and Agentless Approach

CSPM tools can be implemented using two methods, namely the *agent-based* approach and the *agentless* approach [12].

In the agent-based approach, software agents are installed and deployed directly on each client's endpoints and systems, such as servers, cloud computing (CC) instances or clusters. These agents are responsible for monitoring, analyzing, and reporting the security findings back to a centralized management system [14, 15, 16]. Although this approach offers granular and effective real-time monitoring and incident detection capabilities, it may introduce compatibility, performance, or vulnerability issues to the cloud environment due to the introduction of

additional components [14, 16, 17].

The agentless approach, on the other hand, does not require the installation or deployment of software agents on each client's endpoints [15, 16]. Instead, they rely on remote management protocols or *Application Programming Interfaces* (APIs) to access the client's system. The agentless approach operates by scanning and monitoring resources externally by taking snapshots rather than running utilities directly on each client's endpoints. Hence, this approach offers more flexibility and ease of management. However, limitations such as reduced level of detail, false positives and automation capabilities are major issues associated with this approach [14, 15, 17].

Table 2.1 below presents a comparison table between the Agent-based and Agentless CSPM implementation methods. To determine the most suitable implementation approach for CSPM tools, an organization should assess its prerequisites and carefully consider the trade-offs associated with each approach [14].

Table 2.1: A comparison table between the Agent-based and Agentless CSPM security implementation systems

Features	**Agent-based solutions**	**Agentless solutions**
Installation	Requires software agents to be installed on each client endpoints	Does not require software agents to be installed on client endpoints
Monitoring	Provides granular & effective real-time monitoring capabilities	Provides monitoring with reduced level of detail
Security	Less secure due to added components	Less intrusive, more secure
Visbility & control	Provide a higher level of control visibility of the system	Limited control & visibility capabilities
Resource usage	Requires more resources such as memory and CPU	Does not require many resources
Incident detection	Capable of detecting incidents with high accuracy	May generate false positives due to the external scanning approach
Performance	May impact system performance due to the installation of software agents	Minimal impact on system performance due to the absence of software agents

2.2 Access Control

Access control is a fundamental security concept in the fields of information security and computer systems [18, 19, 20, 21]. Access control mechanisms refers to the implementation of pre-defined set of security policies and permissions used to regulate access to various system objects (*i.e., data resources or services, assets, software applications, files, database etc.*) within computer systems, thereby ensuring only authorized access to these objects [20, 22].

The implementation of access control mechanisms has two primary objectives. Firstly, to prevent unauthorized entities (*i.e., individual users, groups, or processes*) from accessing the aforementioned objects. Secondly, to limit authorized entities to accessing only those objects that align with their designated roles,

thereby preventing potential misuse or abuse of privileges and permissions.

In the context of CC, access control focuses on controlling access to objects in the cloud [23]. According to [24], access control in CC is defined as "... *how subjects (i.e., users and processes) can access objects based on defined access control policies to protect sensitive data and critical computing objects in the cloud systems*".

Based on the definition above, we understand that access control in CC comprises of three main components: *subjects*, *objects*, and *access control models* [24]. The subject (i.e., individual user, group of users, or process) is the entity initiating the access action, usually request to an object. The object, on the other hand, refers to system resources or services that the subject is requesting access to. These objects can be a file, database or software application as stated above. Lastly, the access control model refers to the set of pre-defined rules and permissions that govern the subject's access to an object or vice versa. Thus, it determines how they interact within a system [21].

Figure 2.1 below illustrates the relationship and connection links among the three main components of the access control, which are subjects, objects, and access control model. Subjects are individual users, groups of users or processes, they are the ones initialing the access action in the model. Objects represent the diverse array of system resources and services available within the computer system, such as files, databases, and applications. Lastly, access control model refers to the set of pre-defined rules and permissions that govern subjects access permissions to objects or vice versa.

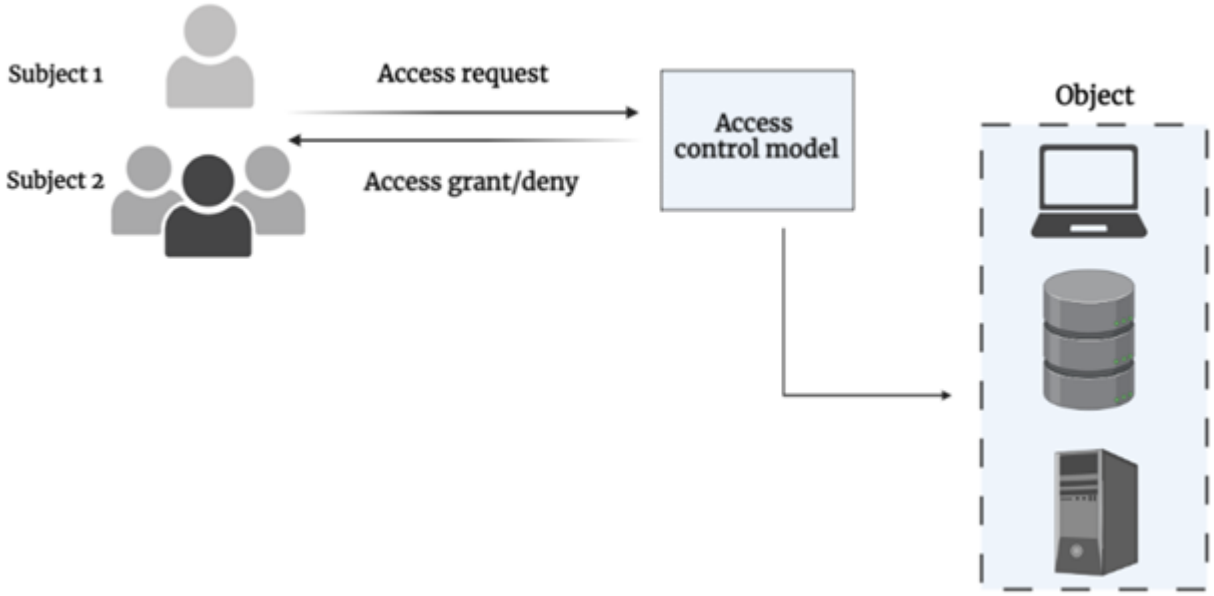


Figure 2.1: The relationship and connection between the three fundamental components of the AC model: subject, object, and access control model is illustrated in the figure. Figure created using Biorender.

A robust access control mechanism is one of key security controls in the cloud. Access control mechanisms should grant access only to authorized entities while simultaneously limiting unauthorized access [22, 25, 26]. Some well-known access control models utilized today are the *Mandatory Access Control* (MAC), *Discretionary access control* (DAC), *Role-Based Access Control* (RBAC), and *Attribute-Based Access Control* (ABAC). Each of these access control models possesses unique characteristics and features [25]. To implement an effective access control model, it is important to understand its main features and align them with the organization's objectives. However, when applied to cloud environments, the MAC and DAC models steadily encounter significant challenges [21, 22, 25].

The MAC model operates in a centralized manner, where a system administrator holds the authority to govern subjects permissions to objects [25, 27]. Although effective in ensuring data integrity and confidentiality, the MAC model does not ensure complete secrecy. Moreover, the MAC model can also be both costly and complex to implement. Furthermore, its lack of support for the PoLP and limited flexibility in large-scale and resource-intensive systems make it inefficient for cloud environments [22, 26].

In contrast, the DAC model grants object owners' complete authority over their respective resources, allowing them to establish the permissions granted to subjects accessing their objects [25, 27]. While DAC offers greater flexible and ease of implementation compared to MAC, it falls short in terms of security by failing to ensure data integrity and confidentiality. Another significant drawback of the DAC model is the scalability issue, particularly in distributed systems like the cloud, that involves multiple users and applications [18]. This can lead to significant management overhead, hindering the efficient management of cloud resources [25, 27].

Furthermore, the aforementioned access control models typically assume that data is stored on trusted data servers accessible to the client. However, this assumption is no longer applicable in CC as the data owner and the cloud servers may belong to distinct domains [28, 29]. Consequently, to overcome these challenges the RBAC and ABAC models were developed [25]. In the following subsections, we will discuss these two access control models in depth.

2.2.1 Role-Based Access Control

The Role-Based Access Control (RBAC) model is an access control model that assigns permissions to subjects based on their respective roles within an organization. The RBAC model is similar to the MAC model, in that it is a centralized access control model. This means that a central administrator is solely responsible for assigning and managing the access permissions to subjects [27].

In the RBAC model, the access permissions and privileges are pre-defined for each role prior to assigning subjects. Depending on the organization, subjects can have multiple roles or be assigned to multiple groups, which grants them additional access privileges and permissions [25].

Compared to other access control models such as DAC and MAC, the RBAC model is more flexible, scalable, and easier to implement. Moreover, it supports hierarchy and inheritance rights, duty separation and follows the PoLP , thus making it more suitable and appealing for cloud environments [18, 25, 27].

However, the RBAC model has some limitations. Limitations such as the lack of support for the delegation principle and its static, coarse-grained nature can make it challenging to manage and enforce access control policies effectively. Nevertheless, it remains a popular and widely used access control model [19, 27].

The RBAC model consists of five essential elements: *subject*, *role*, *permission*,

operation, and *object*. Subjects are entities, typically employees within an organization who interacts with the system. Roles represent the permissions and privileges associated with a specific task in an organization. Operations refer to actions that subjects can perform within the object. Permissions determine the access rights and privileges of subjects, while objects are the system resources and services that subjects can interact with [19, 27].

Figure 2.2 below illustrates the relationship link between the elements of the RBAC model. Subjects consists of individual users and groups, often employees of an organization. Roles represent the pre-defined set of permissions and privileges that are assigned based on specific tasks and responsibilities within an organization. Operations refer to the actions that subjects perform when interacting with objects. Permissions govern the access rights and privileges to users, while objects encompass the services and system resources that subjects can interact with.

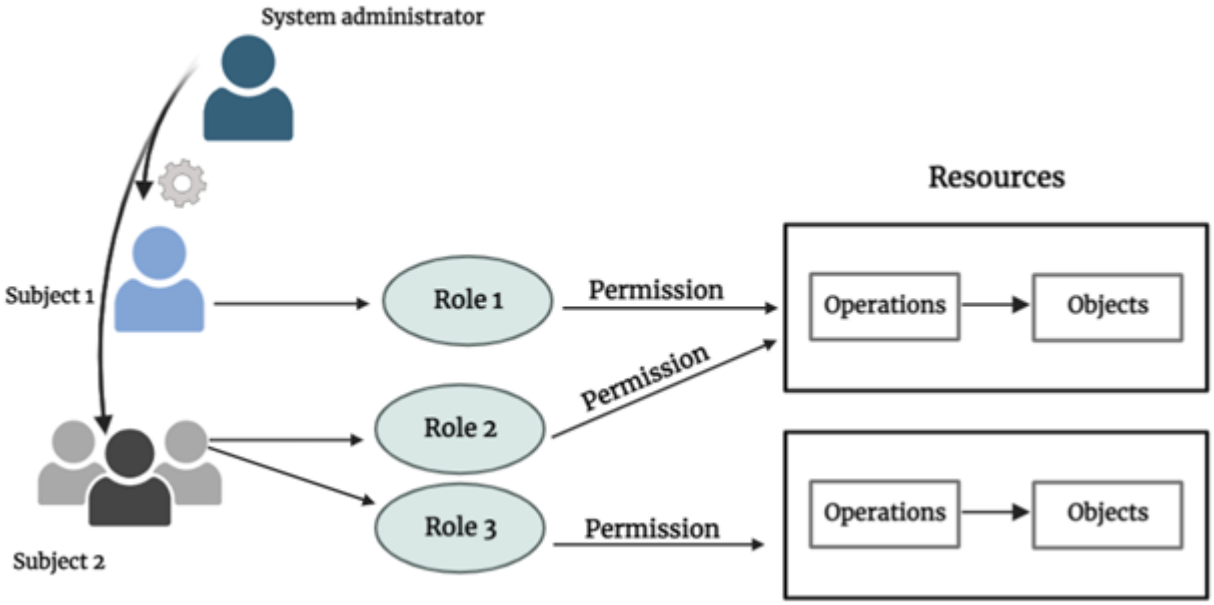


Figure 2.2: The interactions between the different elements in the RBAC model is illustrated in the figure. Figure created using Biorender

The RBAC model is composed of four conceptual models *RBAC0*, *RBAC1*, *RBAC2* and, *RBAC3*.

RBAC0 serves as the base model, and it is based on the PoLP and separation of roles [30].

RBAC1 and RBAC2 models are both extensions to the base model with additional features. RBAC1 introduces the use of role hierarchies, thus allowing for a more structured and hierarchical approach to access control. In contrast, RBAC2, introduces the use of constraints, enabling finer-grained control over resource access. With constraints, RBAC2 can manage more complex access control scenarios, enabling precise control over resource access [30].

Finally, RBAC3 is the consolidated model that incorporates the features of RBAC0, RBAC1, and RBAC2, providing the most advanced and flexible access control mechanism. RBAC3 is capable of handling complex access control scenarios in large organizations, by combining both role hierarchies and constraints to achieve precise and granular control over resource access.[30]. Figure 2.3 below shows the relationship link between the four RBAC models.

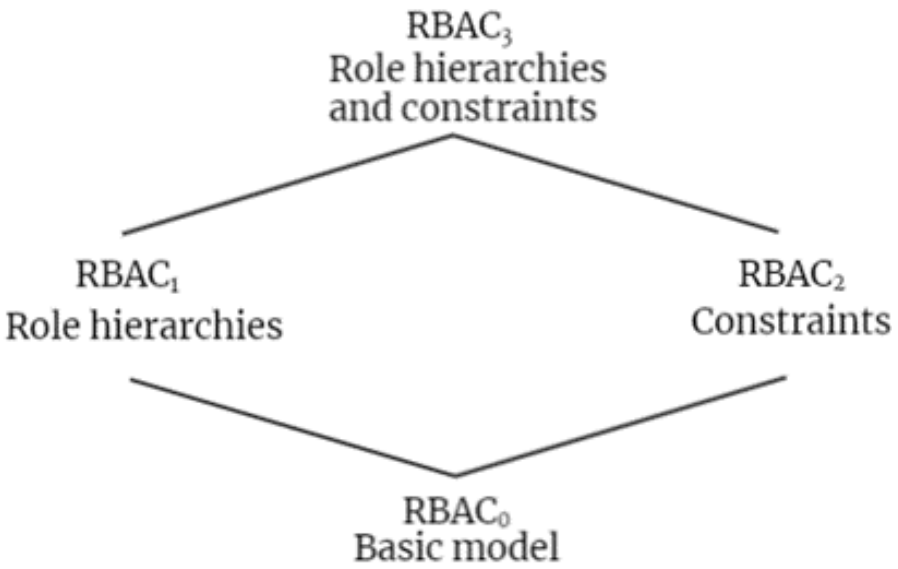


Figure 2.3:
The relationship model of the Role-Based Access Control system as presented by Sandhu in 1997. Figure created using Biorender.

2.2.2 Attribute Based Access Control

Unlike RBAC, Attribute-Based Access Control (ABAC) is an access control model that determines access permissions based on the attributes associated with subjects [25, 27, 31]. These attributes include "*the assigned attributes of the subject, the assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions*" as noted in [19, 32].

As explained above, the attributes in ABAC refer to the various properties associated with subjects, objects, and the environment. These attributes are typically represented as name-value pairs and play a crucial role in determining access decisions. Similiar to RBAC, subjects refers to individual users or groups, interacting with the system. Objects represent the system resources and services that are being accessed. Operations refer to the specific functions or actions performed on objects, typically at the request of subjects. Lastly, environment conditions encompass the contextual characteristics surrounding access requests and are independent of both subjects and objects. These conditions provide additional contextual information that helps inform the access control decisions, ensuring that access is granted or denied based on the relevant attributes and conditions present [19, 32].

The ABAC mode is an extension of the RBAC model in a way. This is done by incorporating additional features such as attribute delegation, attribute decentralization, and attribute interference [26, 33]. These features enhance the model's applicability and effectiveness in cloud environments, which are characterized by large amounts of data, dynamic users, and flexible network topologies [23, 33]. ABAC's advantages, including in granularity, flexibility, usability and support for data sharing, have contributed to its growing popularity in access control.[19]

2.2.3 Access Control in Cloud Security Posture Management

Having established a fundamental understanding of access control mechanisms, including their objectives, and different models, it is crucial to explore their application in the context of CSPM. The access control model utilized in CSPM tools is the RBAC model. As stated earlier, RBAC provides a systematic approach to governing permissions by assigning pre-defined roles to subjects. This ensures that access privileges are determined based on roles rather than individual subjects. By implementing RBAC, CSPM tools establish a structured and organized approach to managing access rights, enabling granular control over user actions within the

cloud environment [11].

2.3 Principle of Least Privilege

The *principle of least privilege* (PoLP) is a fundamental concept in information security that ensures effective access control systems, particularly in CC environments [19]. At its core, the PoLP emphasizes on granting subjects the minimum amount of access permissions necessary to complete their tasks [34].

By implementing the PoLP, organizations can mitigate the security risks associated with compromise of privileged credentials by malicious entities, accidental misuse by authorized users, or intentional misuse by so called "*insider threats*". This leads to a lower risk of unauthorized access, accidental modification, and abuse of sensitive data and resources, thus enhancing the overall security posture of a system [35, 36, 37]. Therefore, it becomes essential for organizations operating in CC environments to prioritize the PoLP in order to mitigate the aforementioned security risks effectively.

The implementation of the PoLP in CC environments however, is challenging due to three main factors [38]. Firstly, formulating policies that accurately align with the user permission needs is complex. Secondly, determining the necessary permissions can be uncertain, making it difficult to strike the right balance. Lastly, enforcing the PoLP becomes nearly impossible due to the large scale and dynamic nature of cloud environments. These factors collectively contribute to the difficulties organizations face in implementing and maintaining least privilege access control measures in the cloud [38].

Nevertheless, there are some solutions to achieve it. To comply with the PoLP in CC environments requires an effective utilization of *identity and access management* (IAM) policies, which will be discussed in the next subsection. This involves assigning IAM policies with minimal permissions required for specific tasks within the cloud services and resources. Additionally, instead of relying on wildcards and AWS managed policies to assign permissions to users in the cloud, explicitly defining the necessary permissions needed yourself in IAM policies enhances adherence to the PoLP [39].

Moreover, regular monitoring of user accesses and usage using services such as Amazon Web Services (AWS) Access Advisor is another important measure. Access Advisor allows user to regularly analyze users' usage patterns and recent accesses. This enables administrators to easily identify and revoke unnecessary

permissions for individual user. All these measures enable organizations to achieve a higher level of security in their cloud environments.

In summary, the PoLP emphasizes the importance of granting entities the minimum necessary permissions required for their tasks. Neglecting this principle may expose subjects to threats such as credential compromise by external malicious actors and the potential resource misuse by insiders, whether accidental or intentional. While challenging to achieve in CC environments, approaches such as avoiding wildcards, AWS managed policies and instead using explicit permission definitions are helpful help. Additionally, leveraging AWS services like Access Advisor can assist identify unused permissions so administrators can revoke them. As such, implementing the PoLP is crucial in mitigating security risks and preventing potential breaches in CC environments [5].

2.4 Identity Access and Management

Identity and Access Management (IAM) is a cloud service that offers cloud administrators a centralized management system for overseeing entities access permissions to resources and services within their cloud environment. With IAM, administratirs have the ability to define granular access permissions, enabling precise control over the level of access granted to entities to their AWS resources [40] . This service enables administrators to establish IAM entities, to which pre-defined policies containing specific permissions and privileges can be assigned [41, 42, 43].

The IAM framework in AWS consists of three types of entities: *IAM users*, *IAM user groups*, and *IAM roles*. IAM users represent individual users or applications, IAM user groups represent set of IAM users while IAM roles include linked IAM users and IAM user groups [41, 43]. Figure 4 below illustrates a visual representation of these IAM components.

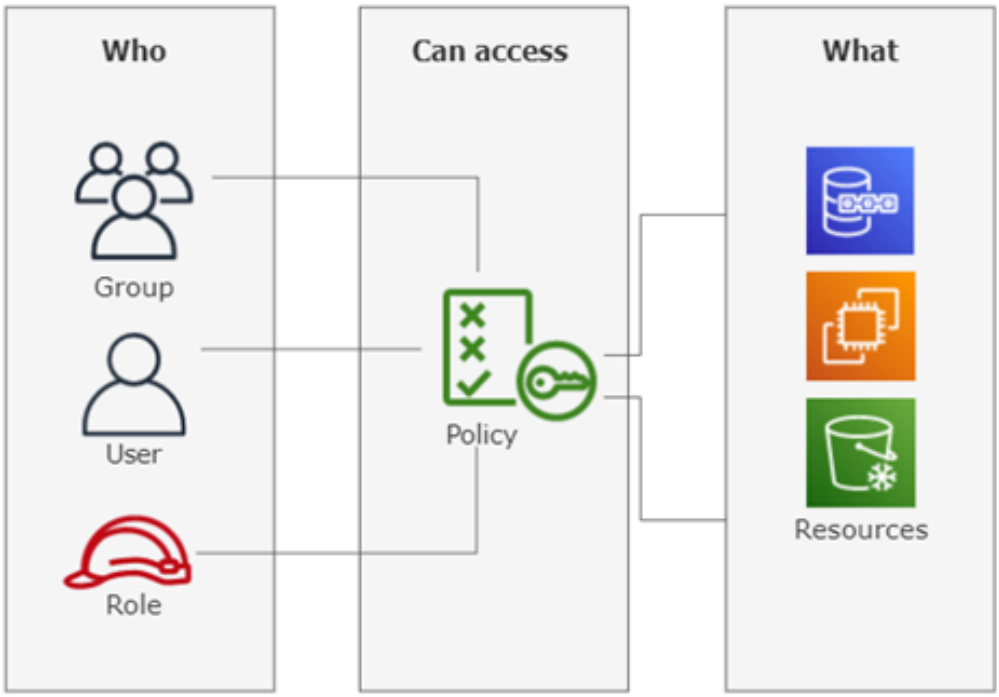


Figure 2.4: The AWS IAM entity is composed of three entities: IAM user, IAM user groups, and IAM role. Figure created by author.

The two fundamental aspects of IAM are the *authentication* and *authorization* process. In IAM, users authenticate their identity as IAM entities and are authorized based on assigned IAM policies. This ensures that only authenticated users with appropriate permissions can perform actions in the AWS environment. IAM's role is crucial in maintaining cloud security [39].

In AWS, IAM entities possess two types of credentials. The first type is the traditional username and password method, which grants access to the AWS Console but cannot be utilized for programmatic actions. The second type is the access key method which consists of an access key ID and a secret access key. Access keys serve the purpose of programmatically invoking AWS actions through the Software Development Kit (SDK) or Command Line Interface (CLI). An IAM entity may possess both username/password and access keys if they require both programmatic and console access [39].

It is worth nothing that although the implementation of the IAM policies may vary among the different CSPs, they are generally expressed in the JSON format [44, 41, 45, 39]

Figure 2.5 below provides illustrates an example of an AWS AdministratorAccess IAM policy. The policy consists of top-level elements, including Version and Statement, where the latter specifies the action and resource on which the action shall apply. The character (*) used in the policy represents a wildcard, and signifies to the word "all". Consequently, this policy allows all (*) actions on all (*) resources. However, it is worth noting that this policy must be attachment to an IAM entity before the actions can be implemented [39, 41, 42, 44, 46].

An important element to note in the figure is the use of the asterisk character (*) in the policy. This character is referred to as a wildcard, and it signifies the word "all". Consequently, the AdministratorAccess policy shown in the figure below allows all (*) actions on all (*) resources. Hence, users assigned with this policy possess unrestricted access to do whatever he/she wants in the cloud environment. However, it is worth noting that this policy must be attachment to an IAM entity before the actions can be implemented [38, 41, 44, 45, 46]

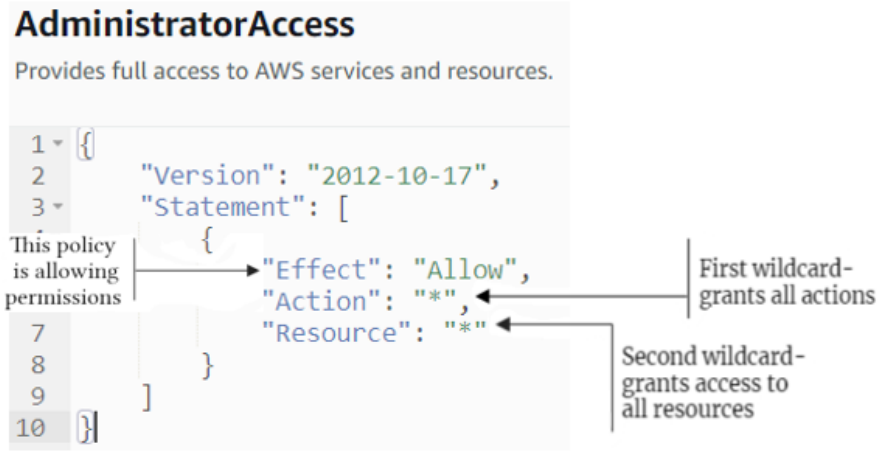


Figure 2.5: The figure illustrates an AWS AdministratorAccess IAM policy. The policy grants entities permission to perform all (*) actions on all (*) resources. Screenshot from AWS console.

In summary, the implementation of IAM in cloud enables cloud administrators to securely manage the access permissions and privileges of entities in their cloud environment. This approach ensures that only authorized identities have access to the appropriate resources and actions [47].

2.4.1 Identity-based and Resource-based policies

AWS IAM includes two types of policies: *identity-based policies* and *resource-based policies*. Identity policies are directly applied and attached directly to IAM entities such as IAM user, IAM user group, or IAM roles. Resource Policies, on the other hand, are attached to resources rather than entities [39, 46, 48].

In the upcoming subsections, we will delve into both types of policies in-dept.

Identity-based policy

As mentioned above, Identity policies are directly attached at IAM entities. Identity policies can be further categorized into three different types: *AWS managed policies*, *customer managed policies* and *inline policies* [38, 46].

AWS managed policies, also referred to as standalone policies, can be attached to multiple IAM entities within the same AWS account or across different accounts. Thus, enabling policy reusability. These policies are created and maintained by AWS. This means that they are regularly kept up-to-date by AWS to accommodate the ever-emerging array of new services. This proactive approach minimizes the requirement for manual maintenance efforts and helps prevent potential errors. Additionally, these policies provide users with a library of predefined policies, enabling them to save time by avoiding the need to create policies from scratch [39, 49].

However, it's important to note that AWS managed policies offer limited customization options, as users cannot modify the permissions of the policies [46]. Despite this limitation, they remain popular among organizations due to their ease of use and reduced maintenance effort.

Figure 2.6 below illustrates three examples of AWS managed policies: AdministratorAccess policy, PowerUserAccess policy, and AWSCloudTrailReadOnlyAccess policy. In the figure, we can observe that a single AWS managed policy is attached to entities across different AWS accounts, and within a single AWS account, showcasing their versatility and wide applicability.

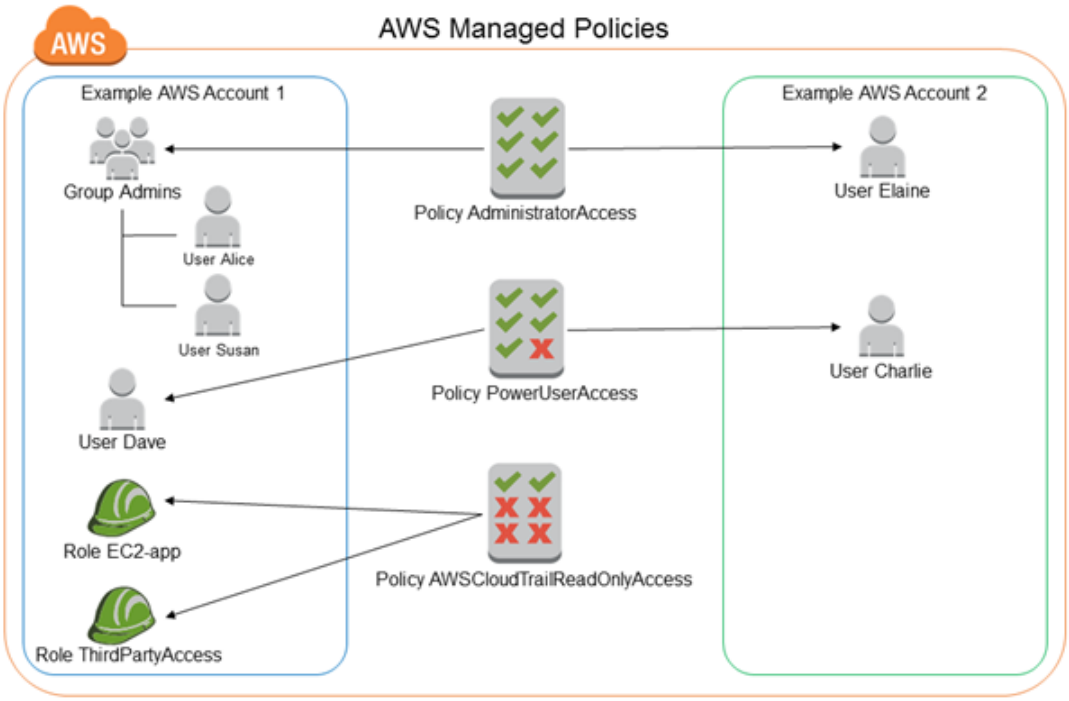


Figure 2.6: The figure illustrates the implementation of AWS managed policies. Figure from AWS official documentation

Customer managed policies offer similar capabilities to AWS managed policies in terms of being attachable to multiple IAM entities within the same AWS account. However, a key distinction is that customer managed policies cannot be attached across different organizations [38]. Furthermore, customer managed policies are created and managed by the customers themselves. This grants users greater flexibility to customize the policy permissions to meet their specific needs and requirements. This level of control allows for more granular customization compared to AWS managed policies [38, 49].

However, with this increased control and customization capability, customers also assume the responsibility of policy maintenance, including regular updates, revisions, and monitoring of policy usage to ensure compliance with organizational

and regulatory requirements[38, 49].

Due to this, customer-managed policies require a higher level of effort and attention compared to AWS managed policies. Nonetheless, the ability to customize and have greater control over the policies make them an attractive option for users who require a more tailored approach to policy management[38, 49].

Figure 2.7 below illustrates customer managed policies in AWS. In the figure we see that a single customer managed policy can be attached to multiple IAM entities within the same organizations. For example, the DynamoDB-books-app policy is attached to two distinct IAM roles [49].

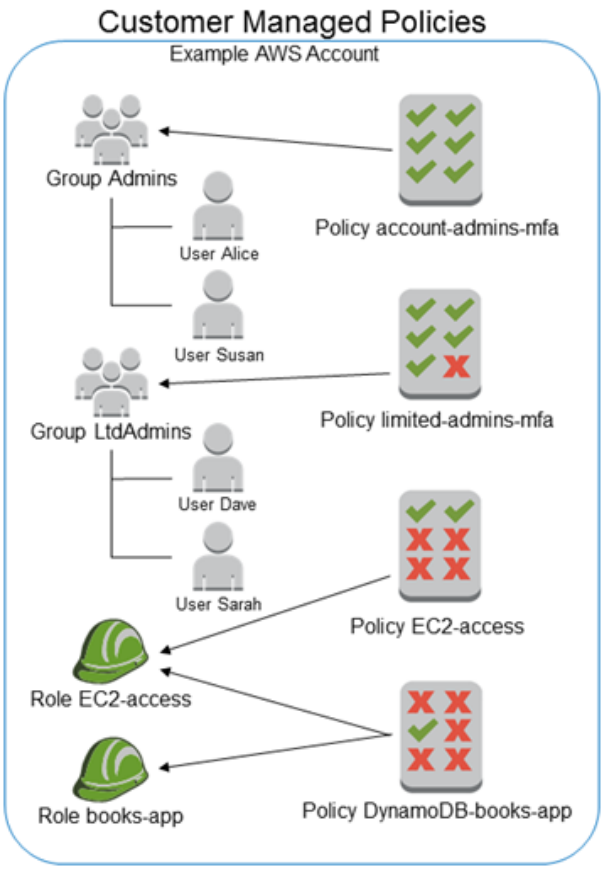


Figure 2.7: The figure illustrates customer managed policies in AWS. Figure from AWS official documentation

Inline policies are type of policies created for a specific IAM entity and as such, they maintain a strict one-to-one relationship with that entity. This means that when the entity is deleted, the policy attached to it also gets deleted with it. This approach ensures that the defined permissions are exclusively assigned to that particular user, group, or role, providing a high level of control and granularity [49].

However, AWS generally recommends using managed policies over inline policies in most cases. Managed policies offer greater flexibility and ease of management, as they can be attached to multiple entities and can be centrally maintained

and updated [50].

Figure 2.8 below illustrates inline policies in AWS. It demonstrates that even though two roles contain the same inline policy, the DynamoDB-books-app policy, they each have their own individual copy of the policy attached to them. This highlights the unique and independent nature of inline policies [38, 49].

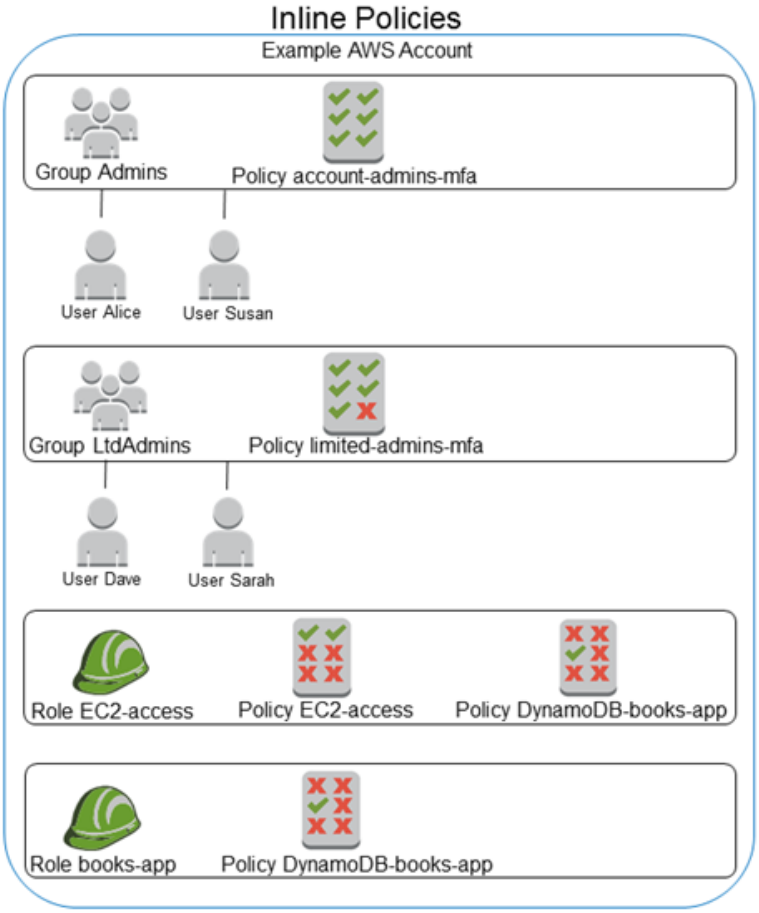


Figure 2.8: The figure illustrates incline policies in AWS. Figure from AWS official documentation

Resource policies

Resource policies are policies that are attached to specific resources, such as an Amazon S3 bucket. Unlike identity policies that are attached directly to specific IAM entities, resource policies define permissions at the resource level rather than the identity level. This means that these policies enable the control of which entities can access a specific resource [38, 49].

2.5 Access Advisor

Access Advisor is a service within the AWS IAM console that offers users valuable insights into the access patterns of IAM entities, including the policies and permissions associated with their access. This service helps identify the frequently accessed resources and permissions, as well as those that were never utilized, thereby facilitating the detecting and removal of unused permissions . As such, Access Advisor is instrumental in implementing the PoLP for resource permission assignment and for mitigating the risks of over privilege [50, 51].

For cloud administrators, Access Advisor serves as an essential tool for monitoring and optimizing user and role permissions. By analyzing the access patterns, they can effectively reduce the risk caused by unauthorized access. Furthermore, this service contributes to maintaining integrity and confidentiality of sensitive data in the AWS environment [50, 51].

2.6 Supply chain risks in Cloud Computing

Supply chain risks refers to the potential harm or compromise that arises from interactions with partner suppliers or third-party vendors. These risks stem from vulnerabilities associated with the products, services, software applications, or hardware provided by these external entities. Malicious actors exploit these vulnerabilities within the third party's organization to gain unauthorized access to other organizations.

When organizations depend on suppliers or third-party vendors for critical components or services, a level of dependency is introduced that poses them to such risks. These risks can manifest in different ways, such as security vulnerabilities in the products or services, compromised data integrity, or disruptions in the supply chain itself [52, 53, 54, 55].

Categorically, supply chain risks can be classified into three main types. The first type involves attacks on primary suppliers or third-party vendors, resulting in disruptions to product or service delivery. A prominent illustration of this risk is the 2017 cyberattack on shipping giant Maersk, which significantly impacted global supply chains [56] .

The second type occurs when organizations fall victim to breaches caused by vulnerabilities within their supply chain's network. In such cases, the malicious actors exploit the security weaknesses in the supplier's network, thereby gaining unauthorized access to the organization's systems. The Kaseya cyberattack is an example of this type of breach, where attackers utilized a vulnerability to infiltrate over 1,000 organizations [56] .

The third type of supply chain risk refers to organizations being compromised due to reliance on and vulnerability present within the third-party product or service used in their own operations. A notable example of this type of risk is the Log4j vulnerability in 2021, which exposed weaknesses in widely adopted software [56] .

In our research study, we specifically focus on the aforementioned supply chain risk. Our primary concern revolves around the dependence and resilience of the CSPM tool, which, if exploited, could leave us vulnerable to future attacks. Such exploitation could grant unauthorized access to our systems and data, emphasizing the importance of addressing supply chain risks in our context.

Chapter 3

Literature Review

This chapter presents literature review related to the thesis topic.

CSPMS tools are a relatively new technology that have recently gained attention due to their effective ability to identify and mitigate security risks in cloud environments. Therefore, there is a research gap concerning the examination of supply chain risks specifically associated with these tools.

The research methodology involved utilizing databases like Google Scholar and IEEE Xplore to gather relevant articles. The search criteria were refined to include only peer-reviewed articles and conference proceedings, while excluding non-peer-reviewed articles and those older than 10 years. Specific search terms related to "Least Privilege in Cloud Computing", "Supply chain risks in Cloud Computing," "Supply chain risks in CSPM tools," and "Least privilege in CSPM tools" were employed to ensure recent and credible sources were included. A total of 19 papers were collected, and after a narrowing down process, 9 papers were selected for further analysis. Due to time limitations, a structured literature review was not employed.

3.1 CSPMS

In a recent study conducted by Bulut and Hwang, they introduced NL2Vul, a framework that utilizes deep neural networks and transfer learning to automate vulnerability assessment in cloud security posture management (CSPM) [8]. The objective of the framework is to minimize human intervention and provide an automated approach to vulnerability assessment. By leveraging natural language processing techniques and transfer learning, NL2Vul predicts vulnerability scores, improving the efficiency of CSPM processes. The evaluation of the framework

demonstrated its effectiveness in accurately predicting the severity of vulnerability descriptions. It is important to note that while the paper discusses various aspects of CSPM, it does not specifically address the topic of supply chain risks associated with CSPM tools, which is the focus of our thesis.

3.2 Least Privilege

In recent years, several approaches have been proposed to address the challenges of implementing least privilege in CC environments. For instance, Puyang et al. (56) presented *LPCloud*, a framework that minimizes the privileges of cloud administrators using an algorithm based on API call dependencies to mitigate insider threats. LPCloud included a Policy Generator service and Policy Enforcer component for policy production and enforcement, respectively.

Similarly, Sanders & Yue [19, 57] conducted two studies focusing on mitigating the over- and under-privilege assignment issues in cloud environments. One study introduced a rule mining algorithm that generated least privilege in ABAC policies while minimizing the assignment errors [19]. The other study presented two frameworks to reduce the over- and under-privilege in cloud services [57]. The effectiveness of these approaches was evaluated with real-world datasets, although further research was suggested to enhance the accuracy from the study in 2018. The practical implementation of over and under-privilege detection is implemented in cloud services such as AWS Access Advisor and recommender by Google cloud platform (GCP).

In the context of smart homes, Goutam et al. [58] developed Hestia, a system designed to generate least privilege network policies to mitigate the risk of compromise. The system was evaluated on 40 smart home devices and showed its effectiveness in reducing the attack surface while maintaining usability. Additionally, Rastogi et al. [59] presented CIMPLIFIER, a tool that enforces privilege separation and least privilege principle in container-based applications such as Docker, by eliminating unnecessary resources. Evaluation of the tool on real-world container applications demonstrated its capability image size while preserving functionality.

To address the challenges associated with detecting least privilege on IaC templates, Shimizu & Kanuka [60] developed a test-based algorithm that automates the process. The algorithm generates the least privilege based on the results of the tests conducted. The effectiveness of this approach was evaluated using real-world IaC templates. The findings demonstrated its ability to effectively detect the least

privilege.

While the literature reviewed focuses on the implementation and effectiveness of the least privilege principle in cloud and container environments, to the best of our knowledge there is no current study that aims to investigate supply chain risks associated with CSPMS tools.

3.3 Supply chain risks

Two studies have examined risk mitigation in supply chain management but their focus and relevance to CSPMSs differ. Akinrolabu et. al.[61] introduced a quantitative risk assessment model called CSCCRA, which evaluates risks faced by CSPs based on existing standards and methodologies. They applied the model to a Customer Relationship Management (CRM) application and presented the risk value in dollar terms for cost-effective risk mitigation [61] .

On the other hand, Mani et al. [62] explored the potential of big data analytics to reduce social risks in the manufacturing supply chain and achieve sustainability. Their case study demonstrated that big data analytics can mitigate risks related to environmental and social factors. While the papers provided discuss supply chain risks in the context of CC, they focus on different aspects of risk assessment and mitigation that may not relate to supply chain risks associated with CSPMSs.

Another relevant paper is the one by Razaque et al. [63] which provides a survey of privacy preservation models for third-party auditor tools (TPAs) in CC. The authors highlight the importance of TPAs in ensuring data integrity and confidentiality in the cloud but also discuss the trust issues of TPAs and the security risks that they can pose to data owners due to their access to sensitive data. To address these risks, they proposed secure multi-party computation-based and differential privacy-based models, that limit TPAs' data access and require collaboration data verification. However, while this paper addresses the role of TPAs in CC, it does not directly relate to the investigation of supply chain risks associated with CSPMS tools.

Chapter 4

Methodology

This chapter presents the research methodology used in the study and outlines the technologies and tools utilized to establish the experimental environment for the thesis.

4.1 Research Methodology and Objectives

A well-defined research methodology is crucial for ensuring the collection and analysis of data in a study. A robust research methodology not only ensures the validity and reliability of the study's findings but also guides the researcher throughout the process. The three main approaches to research are *qualitative*, *quantitative*, and *mixed methods* [64].

Qualitative research involves exploring the subjective experiences of individuals or groups, through methods such as interviews, observations, ethnography, or case studies [64].

Quantitative research, on the other hand, focuses on the collection and analysis of numerical data through surveys and experiments. Surveys utilize structured questionnaires, such as multiple-choice questions, to gather information on a specific topic or issue from a representative sample of the target population. In contrast, experimental approaches involve manipulating variables to observe their effect on an desired outcome.

Lastly, mixed methods research combines both qualitative and quantitative approaches to provide a comprehensive understanding of the research topic [64].

For the thesis, the primary objectives are: 1) analysis the supply chain risks

associated with the default permissions in CSPMS tools; 2) assess whether the existing CSPMS tools deploy over-privileged permissions to conduct their security scans; and 3) explore the use of the PoLP access to mitigate the potential supply chain risks these tools may pose.

To address these objectives, a quantitative research method utilizing experiments will be utilized. The experiment will involve creating a private cloud environment to establish a controlled test environment for data collection and analysis. Additionally, two Amazon Elastic Compute Cloud (EC2) instances will be deployed in the cloud in order to simulate a real-world scenario.

After establishing our private cloud and deploying two EC2 instances, we will proceed to select three CSPMS tools for the evaluation of their default permissions. In addition to that, we will examine whether these tools deploy over-privileged permissions for conducting their scans and whether it is possible to reduce these permissions without affecting their capabilities.

This comprehensive analysis will enable us to gain insights into the initial risk levels associated with the default permissions used by CSPMS tools. By examining the extent of over-privileged permissions and exploring possibilities for permission reduction, we aim to identify potential contribution of the CSPM tools to supply chain risks. The findings from this analysis will provide valuable insights into the risk levels posed by default permissions in CSPMS tools and inform the development of strategies to mitigate these risks effectively.

4.2 Tools

This section presents the tools used in the research study:

- Ubuntu 20.04.2 LTS
- Amazon Web Services (AWS) cloud platform
- CloudSploit
- Prowler
- Scoutsuite

4.3 Test Environment

This section provides an overview of the selected CSPMS tools and their respective default permissions. It will be followed by a high-level description of the cloud environment implemented for the assessment.

4.3.1 CSPMS tools

The selection process for the CSPMS tools in this study was conducted meticulously to ensure alignment with the research objectives. Considering the limitations in terms of time and resources, three prominent open-source CSPMSs will be evaluated: *CloudSploit*, *Prowler*, and *Scoutsuite*. These tools are chosen based on their proven effectiveness and widespread adoption within the industry. Additionally, the decision to prioritize open source solutions brings several advantages such as cost-efficiency, a huge community for support and collaboration, and customization options [65].

To ensure accurate evaluation and comparison, separate AWS accounts will be created for each CSPMS tool. This will involve accessing the IAM console and managing IAM user accounts. Dedicated user accounts will be established for each tool, specifically for the scanning process. The necessary default policies will be attached to their respective user accounts to grant the required permissions for their functionality. This approach will ensure distinct and controlled environments, facilitating reliable experimentation and assessment. By maintaining isolation, the research outcomes are enhanced in terms of accuracy and reliability. After creating the user accounts in AWS, the tools will be deployed and assessed on Ubuntu server.

Table 4.1 below provides an overview of the default permissions required by each CSPMS tool. The table shows that all tools utilize the SecurityAudit policy. Prowler adds the ViewOnlyAccess policy and Scoutsuite utilizes the ReadOnlyAccess policy. Additionally, CloudSploit requires an additional customer managed policy, CloudSploitSupplemental.

Table 4.1: The table shows the policies required for each of the CSPMS tools to perform its scans

	CloudSploit	**Prowler**	**Scoutsuite**
AWS managed policy	SecurityAudit N/A	SecurityAudit ViewOnlyAcess	SecurityAudit ReadOnlyAccess
Customer policy	CloudSploitSupplemental	Optional	Optional

In Table 4.2 below, a concise description is provided for each of the policies. The SecurityAudit policy is designed to grant read access to security configuration metadata. On the other hand, the ViewOnlyAccess policy provides permissions for viewing resources and basic metadata across all AWS services. Lastly, the ReadOnlyAccess policy is specifically designed to provide read-only access to AWS services and resources [66, 67, 68].

Table 4.2: Policies utilized by the CSPMS tools and a brief policy description on each of them

Policy name	**Policy Description**
SecurityAudit	Grants read access to security configuration metadata
ViewOnlyAccess	Grants permissions to view resources and basic metadata across all AWS services.
ReadOnlyAccess	Provides read-only access to AWS services and resources.

4.3.2 Amazon Web Services

This chapter provides a high-level overview of the cloud test environment utilized in AWS cloud platform.

Cloud test environment

The assessment's cloud test environment will be hosted on AWS cloud platform, which is recognized as the world's leading cloud platform offering a wide range of services and resources. AWS is chosen for its robustness, scalability, and comprehensive service offerings, making it an ideal choice for simulating a realistic cloud environment [45]. Figure 4.1 below provides a high-level overview of the created cloud infrastructure for the assessment.

In order to establish secure connections between the cloud resources and external network resources while preventing unauthorized access, a virtual private cloud (VPC) will be implemented.

Then two subnets will be created created within the VPC: a public and a private subnet. The public subnet will be designed to allow public accessibility through an internet gateway and routing table, while the private subnet remains accessible only within the VPC, ensuring enhanced security.

Following the creation and configuration of the VPC and subnets, two EC2 instances will be deployed within the respective subnets. One EC2 instance will be deployed in the public subnet, while the other EC2 instance will be deployed in the private subnet. This setup is commonly referred to as a bastion host, where the public instance serves as the entry point for accessing the private network from outside the VPC. Implementing a bastion host is a recommended security practice that effectively reduces the attack surface.

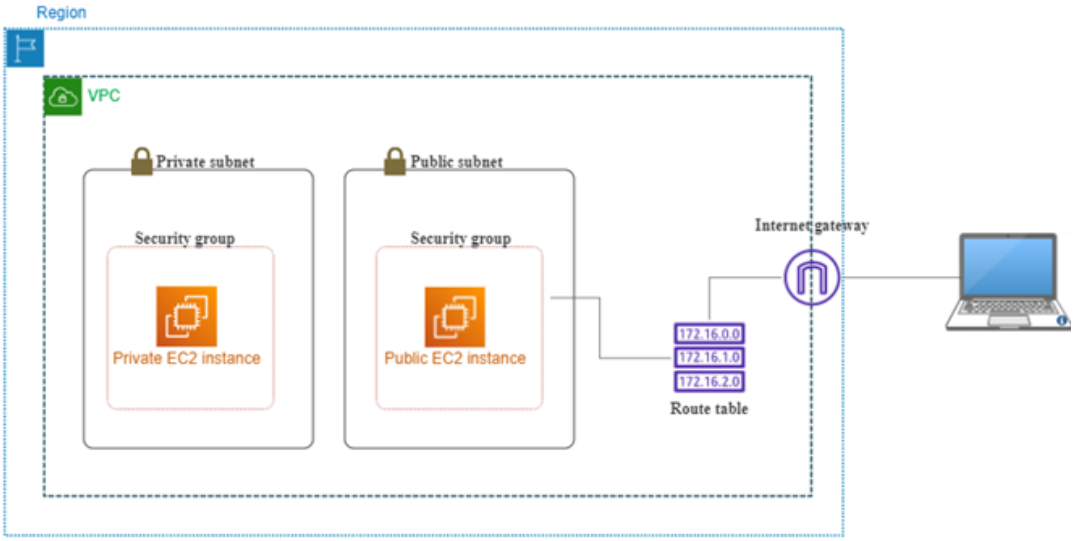


Figure 4.1: The figure illustrates a high level of the experimental test environment created in AWS. Figure created by author

For detailed instructions and configuration steps of the lab environment, including the setup of the Virtual Private Cloud (VPC), Elastic Compute Cloud (EC2) instances, and other relevant components, please refer to the Appendix section. The Appendix provides comprehensive instructions and screenshots to guide you through each component's setup process mentioned in this section. Following

these instructions will enable you to accurately replicate the lab environment for your own testing and experimentation needs.

4.4 Experiments

This section presents the experiment phases conducted as part of the study.

4.4.1 Experiment 1

The first experiment in the study will aim to identify the potential supply chain risks associated with the default permissions in CSPMS tools. This will involve a thorough analysis and examination of each policy's default permissions assigned to the CSPMS tools. The specific list of permissions utilized by each CSPMS tools can be viewed in Table 4.1. Additionally, in Table 4.2, we can observe that the policies heavily rely on read-only access permissions. The implications of these read-only access permissions will be thoroughly examined during the experiment. The objective is to understand the potential risks and consequences that arise from granting such permissions to CSPMS tools in terms of supply chain security.

4.4.2 Experiment 2

The second experiment in this study will focus on investigating whether the CSPMS tools deployed over-privileged permissions to perform their scans of cloud environments. To conduct this experiment, scans will be performed multiple times a day, and the access patterns of these tools will be tracked using AWS Access Advisor. As described in section 2.5, Access Advisor is a service provided by AWS that enables users to track and log the access patterns of IAM entities, thus providing valuable insight into the permissions that were utilized and those that remained unused.

By carefully analyzing the results obtained from Access Advisor and comparing them with the scanning outcomes of the CSPMS tools, it was possible to determine whether the tools deployed permissions that exceeded what was actually necessary. This investigation aimed to identify any instances of over-privileged permissions, where the tools were granted more access than required for conducting their scans.

4.4.3 Experiment 3

The final experiment of this study will aim to assess the capability of the CSPMS tools to perform their scans effectively with reduced permissions. To achieve this, inline policies will be created, which establish a direct and strict one-to-one relationship with the entities involved. These new inline policies will be designed to include only the permissions needed to scan what is provisioned in the cloud environment. The objective is to test whether the CSPMS tools could effectively conduct their scanning's effectively with these limited permissions.

Chapter 5

Results and Discussion

This chapter presents the results obtained from the experiments and analysis on the results.

The first experiment results will show the supply chain risks associated with the default permissions required for running the CSPMS tools. The second experiment results will present the excessive permissions upon which CSPMS tools rely on for conducting their assessments. Lastly, the final experiment results will show the outcomes achieved by reducing the permissions of CSPMS tools while ensuring their continued effectiveness in performing assessments.

5.1 Experiment 1: Supply chain risks associated with default permissions

This subsection will first present the results of the analysis of the default permissions required by all three CSPMS tools: *CloudSploit*, *Prowler*, and *Scoutsuite*. It is followed by a discussion on the potential supply chain risks associated with these permissions.

Supply chain risks, as stated in *section 2.6*, refers to the potential harm or compromise that arises from suppliers or third-party vendors [69]. These risks stem from vulnerabilities associated with the products, services, software applications, or hardware provided by these external entities. In our context, we aim to investigate whether the third-party tools or service, which in this case are the CSPMS tools (CloudSploit, Prowler, and Scoutsuite), pose supply chain risks. Specifically, we aim to determine whether the default permissions granted to these tools can potentially lead to supply chain risk when deployed in cloud platforms.

5.1.1 Results

The examination of access permissions used by the CSPMS tool revealed the common utilization of AWS managed policies, as shown in Table 4.1. A concise description into each policy is given in Table 4.2.

Among the examined tools, the SecurityAudit policy was consistently utilized, granting access to over 450 services through the inclusion of wildcard (*) characters. Figure 5.1 below illustrates a subset of these permissions for reference purposes.

In addition to SecurityAudit, Scoutsuite deployed the ReadOnlyAccess policy, and Prowler made use of the ViewOnlyAccess policy, both of which employed wildcards as well, as shown in Figure 5.2 and Figure 5.3.

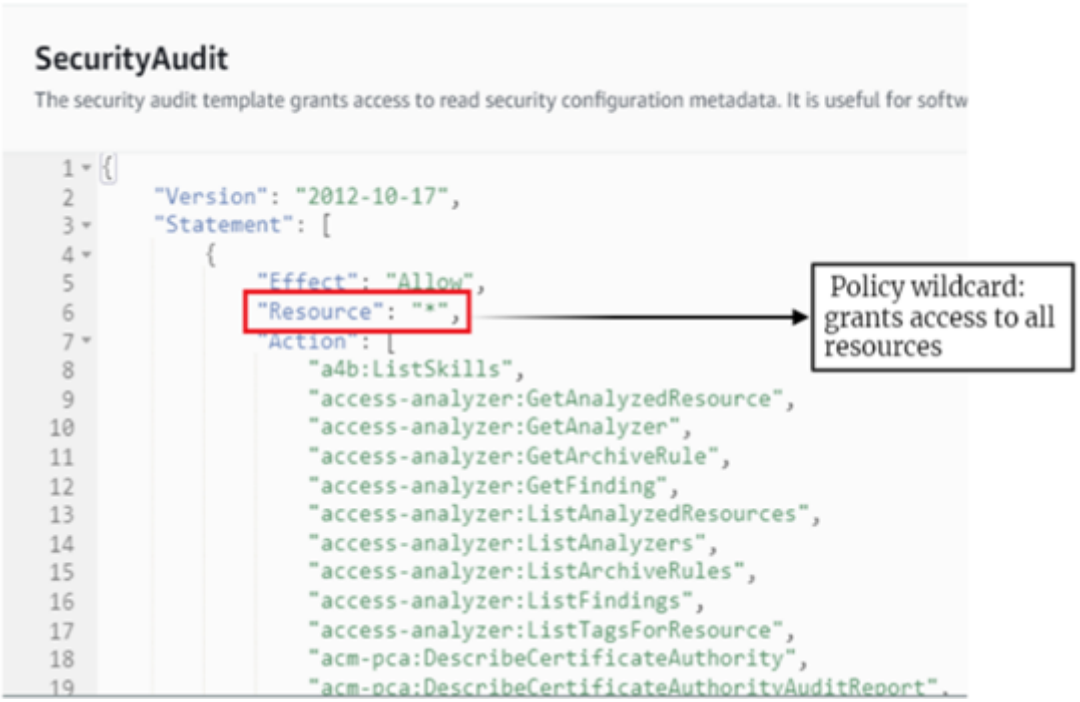


Figure 5.1: illustrates the SecurityAudit policy utilized by all CSPMS tools.

Figure 5.2: illustrates the ReadOnlyAccess policy used by Scoutsuite.

Figure 5.3: illustrates the ViewOnlyAccess policy used in Prowler.

5.1.2 Discussion

All three examined tools rely on AWS managed policies. These policies provide pre-defined permission sets, offering convenience and reducing the likelihood of errors compared to custom policies. However, upon examining these policies, we find that they do not fully align with the PoLP, which is crucial for mitigating supply chain risks [38].

The analysis reveals that the utilization of AWS managed policies for read-only access permissions may by default present inherent risks. Notably, the ReadOnlyAccess policy, where extensive access to data storage and database services such as Amazon S3 and DynamoDB was given. Similar concerns arise with the other two policies, namely SecurityAudit and ViewOnlyAccess. These observations give rise to apprehensions since these tools have the potential to gather and store sensitive information either locally or on third-party SaaS platforms. Consequently, this exposes organizations to unauthorized access and risks associated with the supply chain, particularly in instances where the tool is compromised or a malicious insider intends to exploit them for malicious purposes.

Furthermore, the ReadOnlyAccess policy grants access to Amazon S3, a widely used object storage service for data storage and retrieval. Developers commonly utilize S3 buckets to store various files, including terraform state files. These state files contain sensitive information about the state of the managed infrastructure and may contain sensitive data like access keys, and secret keys. *Figure 5.4* illustrates that the policy enables access to the s3:Get* service, again the use of wildcard is evident there. This means access to all services within the S3:Get service, including the S3:GetObject service. This service allows users to retrieve and download objects from an S3 buck to local environment. Thus, by granting the CSPMS tools to such unrestricted read access to S3 bucket introduces significant supply chain risks. This can potentially lead to unauthorized access to sensitive data either through third-party compromise or malicious insider within the CSPMS.

Similarly, the provision of access permissions to DynamoDB services as shown in *Figure 5.5*, particularly DynamoDB:Get*, raises significant concerns. DynamoDB is commonly used in systems such as e-commerce shops to store sensitive data, including customer details like addresses, phone numbers, and credit card information. Breaching access permissions to DynamoDB can lead to unauthorized access and data breaches, jeopardizing the privacy and security of individuals.

Moreover, the presence of wildcards in these policies grants access permissions to all resources within the services. While beneficial for specific service scans, providing access to all service resources is unnecessary and introduces potential supply chain risks if exploited as described above.

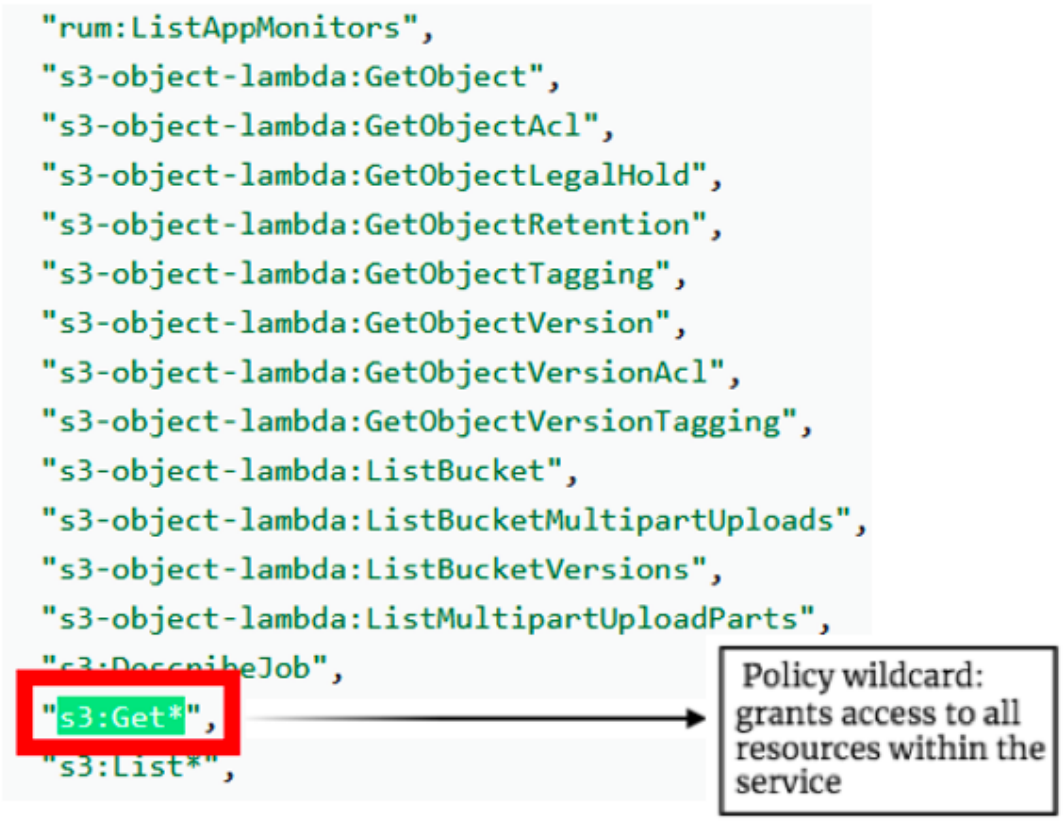


Figure 5.4: illustrates a snippet of permissions from the ReadOnlyAccess policy utilized by Prowler. Permission s3:Get* grants access to s3 bucket.

Figure 5.5: illustrates a snippet of permissions from the ReadOnlyAccess policy utilized by Prowler.

5.2 Experiment 2: Do the CSPM tools rely on over-privileged permissions

This subsection will first present the results of our investigation into whether the existing CSPMS tools deploy over-privileged permissions to perform their scans on cloud environments. Subsequently, a discussion will be provided to evaluate whether these tools adhere to the PoLP or not.

As explained in *section 2.3*, the PoLP advocates granting the minimum necessary permissions required to complete a task, considering anything beyond as over-privileged [38]. In our analysis, we focus on examining whether the permissions assigned to the CSPMS tools align with this principle. If they deviate from it, we can conclude that they are over-privileged in nature.

5.2.1 Results

The section presents the results obtained from the report generated by AWS Access Advisor. As described in *section 2.5*, AWS Access Advisor is a service designed to track and log the access patterns of IAM entities. Its purpose is to identify the frequently accessed resources and permissions as well as those that have never been utilized. Essentially, it provides an auditing mechanism for permissions.

To provide an overview of the findings, we present Table 5.1 below, which outlines the number of services that were not accessed by the three specific CSPMS tools. The table reveals that CloudSploit had 55 unaccused services, Prowler had 99 unaccused services, and Scoutsuite had 225 unaccused services

Table 5.1: Presents the tools that were not accessed during the scanning period of the tools

CSPMS tools	Policies utilized	Services not used
CloudSplout	SecurityAudit CloudSploitSupplemental	55 services
Prowler	SecurityAudit ViewOnlyAccess	99 services
ScourSuite	SecurityAudit ReadOnlyAccess	255 services

5.2.2 Discussion

The analysis conducted using Access Advisor has revealed interesting findings. Table 5.1 presents the results, showcasing the number of unused services for each CSPMS tool. Specifically, CloudSploit had 55 unused services, Prowler had 99 unused services, and Scoutsuite had 225 unused services.

To better understand the significance of these unaccessed services, it is important to explore their relationship with the associated permissions. For further insights, let's shift our attention to *Figure 5.6* below which provides a valuable glimpse into the services that were not accessed during the scanning period. The Access Advisor report on the SecurityAudit policy highlights notable services such as Amazon Cloud Directory, Cloud9, and CloudHSM that remained unaccessed.

To gain a more comprehensive understanding of the permissions tied to these services, we can refer to *Figure 5.7*. Within this figure, we can observe that Cloud9 possesses access permissions for two services, Cloud Directory has access permissions for one service, and CloudHSM holds access permissions for three services. This detailed breakdown offers a clearer picture of the permissions associated with each unaccessed service.

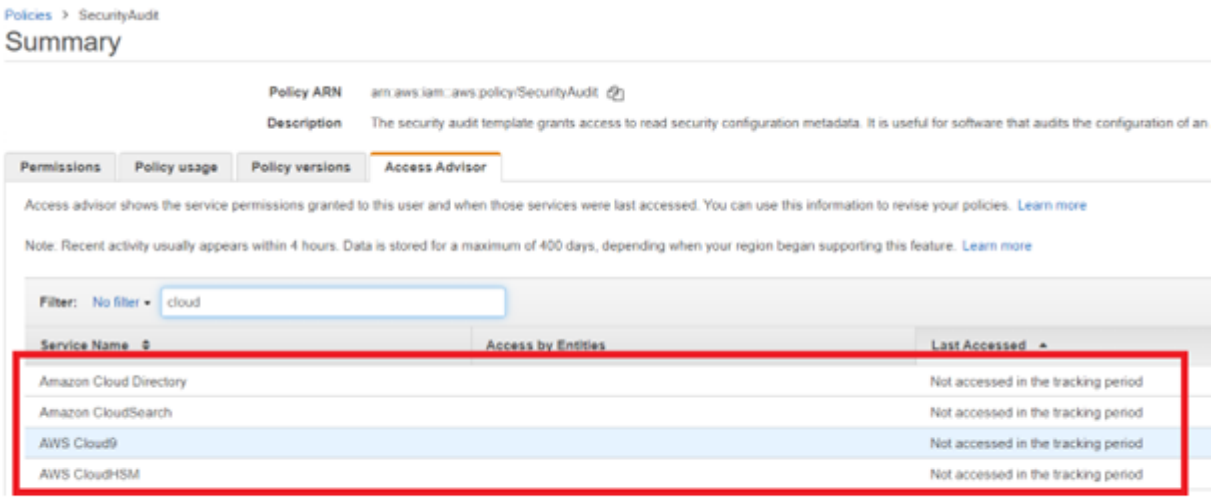


Figure 5.6: illustrates the Access Advisor report from the SecurityAudit policy showing the services that were not accessed during the scanning period of the CSPMS tool.

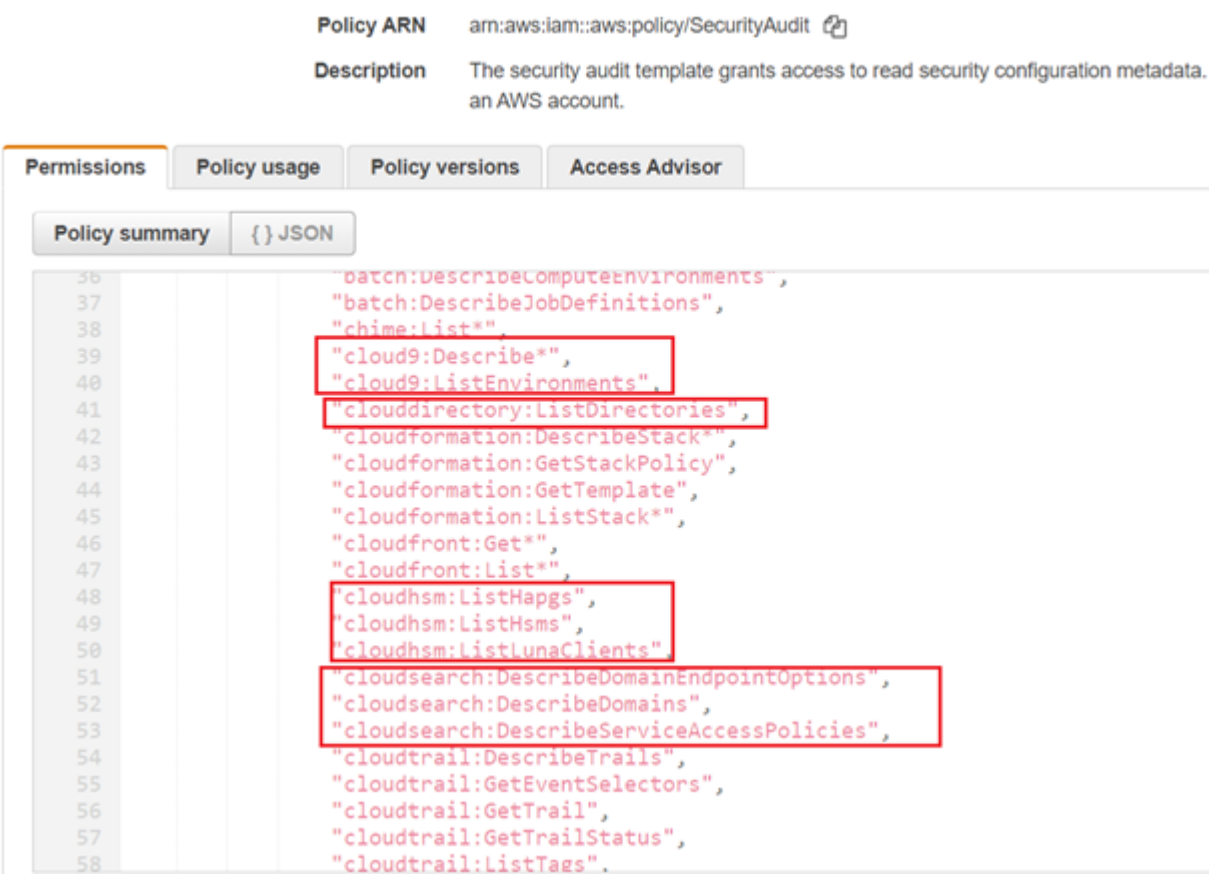


Figure 5.7: illustrates the permissions each service utilizes in the policyr.

Considering the SecurityAudit policy where 55 services were not accessed, it becomes crucial to recognize that these unaccessed services encompass a significant number of permissions that were not utilized. This observation does not aligns with the PoLP, which advocates granting only the minimum necessary permissions to perform a specific task. It is crucial to acknowledge that each additional permission introduces a potential liability, and over-privilege can lead to various security risks.

For instance, users with excessive permissions, such as managers and administrators, are at a higher risk of credential compromise. Additionally, the misuse of privileges, whether intentional or unintentional, can create potential security threats.

5.3 Experiment 3: Reduced permissions

This subchapter presents the results of an analysis which aimed at determining whether the permissions granted to CSPMS tools can be reduced while still maintaining their effectiveness in conducting security scans.

5.3.1 Result

The primary object of this experiment was to assess the feasibility of reducing the permissions of the CSPMS tools' while ensuring their ability to perform effective scans of the targeted services.

The experiment involved the creation and deployment of an incline policy specific to each CSPMS tools, with a focus on limiting permissions to EC2 instances. Prior to implementing the inline policies, default policies were removed to pave the way for a streamlined permission structure. The inline policy was designed to grant permissions exclusively for scanning the services relevant to the cloud environment, particularly the EC2 instances.

Figure 5.8 below provides an overview of the permissions included in the inline policy, for CloudSploit. The figure demonstrates that the policy was designed to grant scanning and accessing permissions exclusively for the EC2 service. Subsequently, figure 19 displays the results obtained after implementing the new inline policy, showcasing the outcomes achieved with the reduced overall permissions. Additionally, figure 20 illustrates the report obtained from Access Advisor.

5.3.2 Discussion

The experiment's findings reveal the possibility of reducing the permissions of CSPMS tools without compromising their scanning capabilities. his was achieved by implementing inline policies specific to each tool, with a focus on limited permissions for EC2 instances.

The analysis as shown in figure 5.10 confirms the effective implementation of the inline policy in granting permissions exclusively for the EC2 service. This targeted approach ensured that the CSPMS tools focused their scanning efforts on the relevant services, thereby mitigating unnecessary access to unrelated resources. The scanning results, as shown in Figure 5.9, demonstrate the effectiveness of the reduced permissions. The CSPMS tools were able to scan the intended services, validating their ability to conduct comprehensive security assessments with the limited permissions granted by the inline policy.

The results obtained from Access Advisor further support the experiment's findings. As illustrated in Figure 20, the report indicates that the CSPMS tools successfully reduced their permissions while maintaining their scanning capabilities. This alignment between the inline policy's granted permissions and actual usage patterns highlights the potential for optimizing permissions according to the principle of least privilege. By reducing unnecessary permissions, CSPMS tools can enhance security and compliance without compromising their scanning effectiveness.

The consistent results observed across all CSPMS tools further strengthen the validity of the experiment's findings. The successful reduction of permissions without sacrificing the effectiveness of security scans highlights the potential for enhancing security posture by implementing fine-grained permissions.

However, it is important to note that this experiment focused on a specific set of services and the EC2 instances in the cloud environment. Further research is required to explore the applicability of this approach to a wider range of services and cloud configurations. Additionally, considerations should be given to potential trade-offs between security and convenience, as reducing permissions may impact certain functionalities or user experiences.

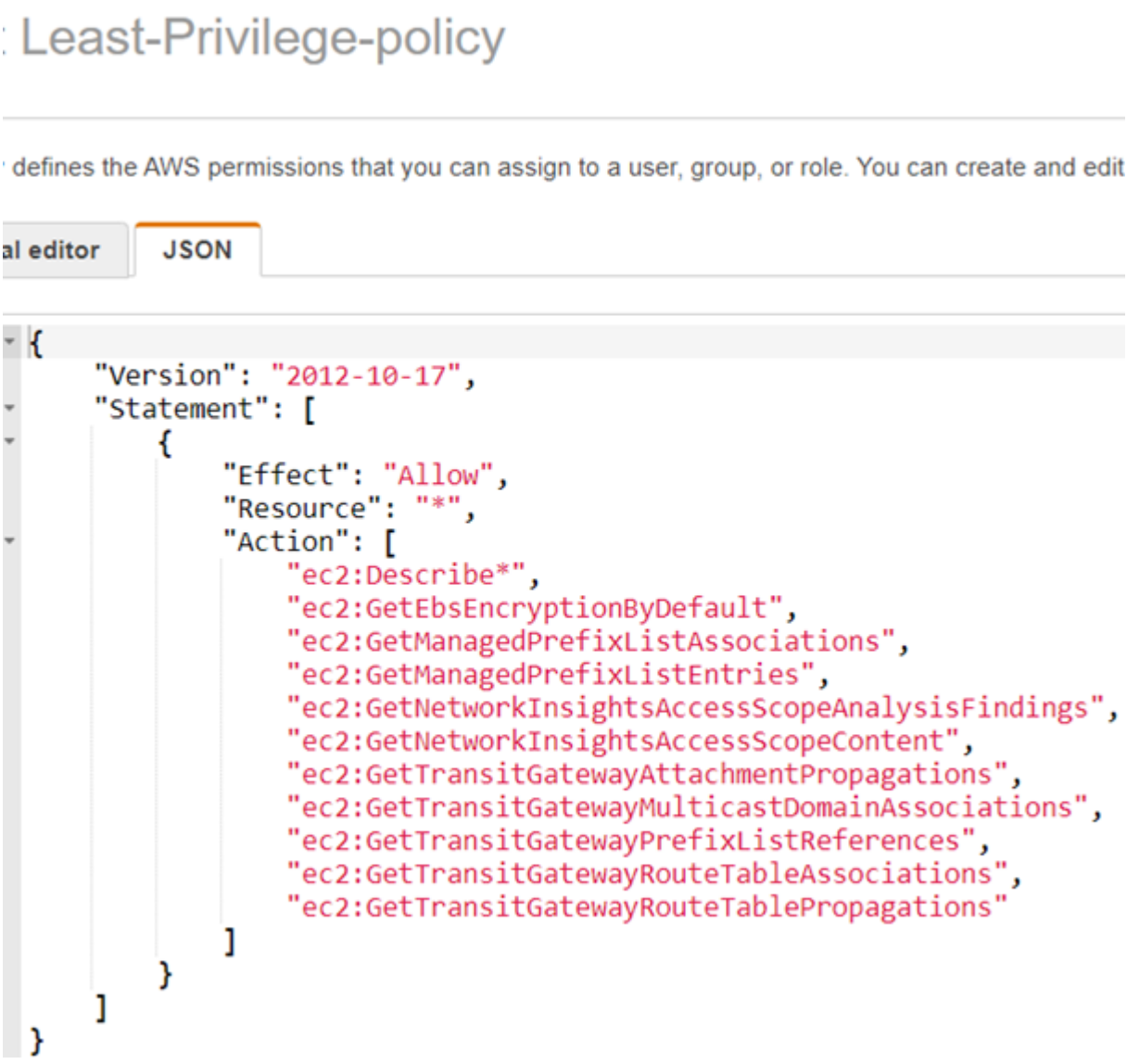


Figure 5.8: The figure shows a restricted permission version where only EC2 instances are scanned in CloudSploit.

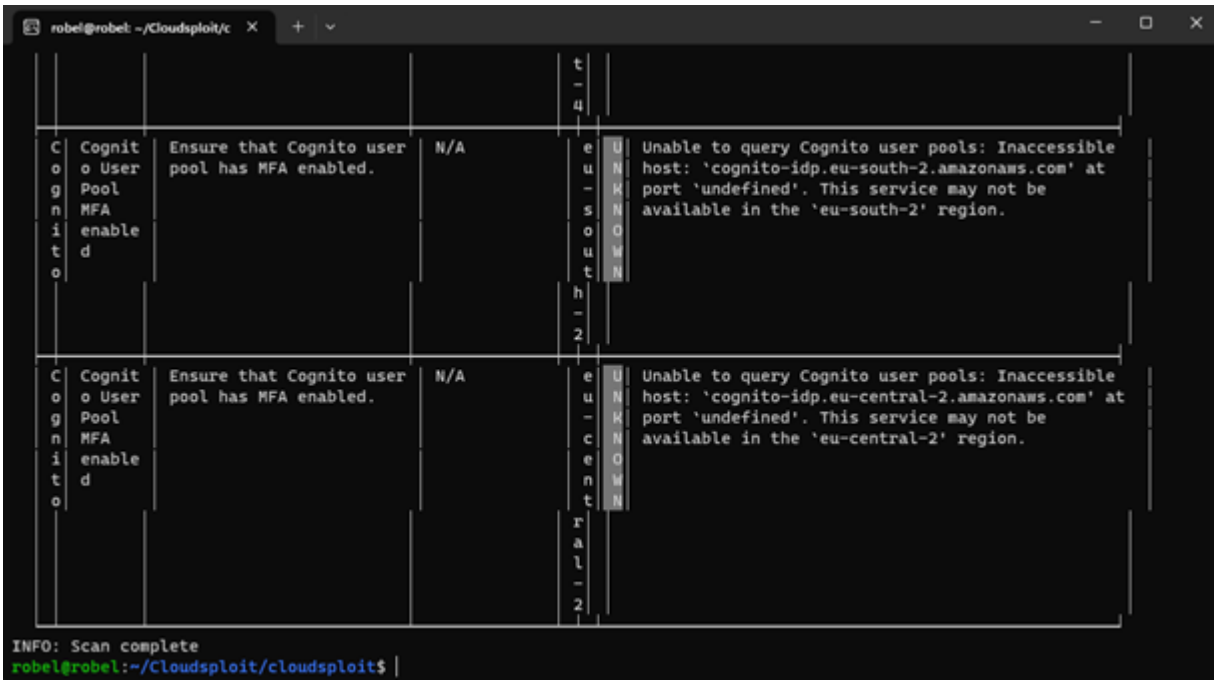


Figure 5.9: The figure illustrates the scanning process in Ubuntu after the permissions of CloudSploit have been reduced.

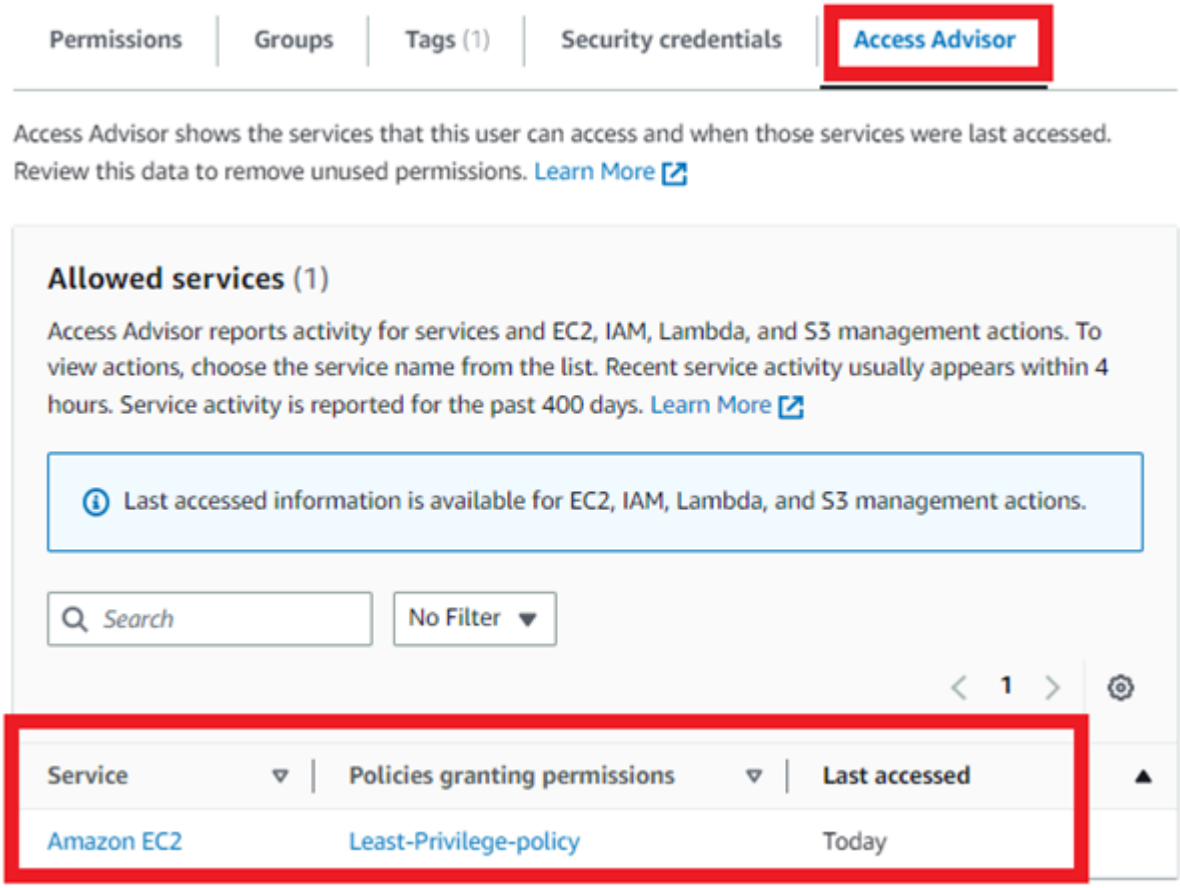


Figure 5.10: lThe figure displays the Access Advisor report after effectively reducing the permissions.

Chapter 6

Conclusion and Future Work

CSPMS tools have emerged as a novel technology renowned for their effectiveness in identifying misconfigurations, ensuring cloud compliance, and providing real-time risk monitoring capabilities in cloud environments. Thereby, enhancing the overall cloud security posture management. Despite their significance, the existing literature on CSPMS tools remains limited, prompting this research to fill the gap by conducting experiments, analyses, and investigations into the supply chain risks associated with these tools.

The research study aimed to address three main objectives. Firstly, it sought to identify whether the default permissions assigned to the CSPMS tools introduced any supply chain risks. Secondly, it aimed to assess whether these tools relied on over-privileged permissions to carry out their assessments. Lastly, the study aimed to explore the possibility of reducing the permissions granted to the tools while still maintaining their ability to perform their assessments effectively, aligning with the PoLP.

The findings of the research shed light on potential supply chain risks stemming from default permissions. Notably, the use of policy wildcards and AWS managed policies deviated from the PoLP, which is crucial in mitigating supply chain risks. Furthermore, the analysis revealed the presences of the s3:Get* in the ReadOnlyAccess policy, particularly the s3:GetObject permission that grants users the ability to read and retrieve data. This raised concerns about the potential risks associated with unauthorized access to these permissions.

Additionally, the study uncovered that CSPMS tools relied on over-privileged default permissions. However, when the permissions were reduced, the tools still demonstrated the capability to conduct successful audit scans, ensuring effective risk monitoring and compliance assessment.

The research findings open several interesting directions for future research. One potential area is the development of an auto-discovery service. This service would perform a preliminary scan of the cloud environment prior to conducting its audit scanning. This service would allow CSPMS tools to dynamically adjust their permissions based on the identified resources and services within the environment.

Another potential research direction involves the integration of a graphical user interface (GUI) within CSPMS tools, enabling users to define their local environment and deployment by selecting the specific resources and services present. Based on this information, the CSPMS tool would automatically generate the necessary permissions required for scanning the designated resources and services. This approach would provide clients and CSPMS vendors with improved management capabilities and enhanced control, allowing for customization of permission levels and scanning comprehensiveness. By implementing adaptive approaches like these, the risk of over-audit scanning can be mitigated while still adhering to the PoLP, thereby increasing the overall efficiency of compliance and security assurance.

In conclusion, this study addresses the knowledge gap surrounding CSPMS tools and their associated risks. By uncovering potential supply chain risks, identifying over-privileged permissions, and proposing strategies for permission reduction, this research contributes to the advancement of CSPMS technology. Furthermore, the proposed direction for future research, such as the development of an auto-discovery service, presents opportunities for further exploration and refinement in this evolving field.

Bibliography

[1] S. Aiello, "5g cloud-native network functions security risks in public clouds," *Social Science Research Network Electronic Journal*, Aug 2022.

[2] R. Loaiza Enriquez, "Cloud Security Posture Management /CSPM) in Azure," 2021. Accepted: 2021-06-29T07:44:07Z.

[3] A. BALCIOĞULLARI and M. MAVAŞOĞLU, *Current Studies in Social Sciences V*. Akademisyen Kitabevi, Sept. 2022. Google-Books-ID: U_6lEAAAQBAJ.

[4] D. K. Saini, K. Kumar, and P. Gupta, "Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions," *Security and Communication Networks*, vol. 2022, p. e4943225, Apr. 2022. Publisher: Hindawi.

[5] M. Sanders and C. Yue, "Automated least privileges in cloud-based web services," in *Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies*, HotWeb '17, (New York, NY, USA), pp. 1–6, Association for Computing Machinery, Oct. 2017.

[6] G. SAWHNEY, G. KAUR, and R. Deorari, "CSPM: A secure Cloud Computing Performance Management Model," in *2022 International Conference on Cyber Resilience (ICCR)*, pp. 1–5, Oct. 2022.

[7] K. Torkura, M. I. Sukmana, F. Cheng, and C. Meinel, "Continuous auditing and threat detection in multi-cloud infrastructure," *Computers and Security*, vol. 102, Mar. 2021.

[8] M. F. Bulut and J. Hwang, "NL2Vul: Natural Language to Standard Vulnerability Score for Cloud Security Posture Management," in *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, pp. 566–571, Sept. 2021. ISSN: 2159-6190.

[9] M. V. Reddy, P. S. Charan, D. Devisaran, R. Shankar, and P. M. Ashok Kumar, "A Systematic Approach towards Security Concerns in Cloud," in

2023 Second International Conference on Electronics and Renewable Systems (ICEARS), pp. 838–843, Mar. 2023.

[10] A. N. J. Vassilenko, *Comparative Study Of Implementing The On-Premises and Cloud Business Intelligence On Business Problems In a Multi-National Software Development Company*. PhD thesis, 2023.

[11] A. Kumar and G. Somani, "Security Infrastructure for Cyber Attack Targeted Networks and Services," in *Recent Advancements in ICT Infrastructure and Applications* (M. Chaturvedi, P. Patel, and R. Yadav, eds.), Studies in Infrastructure and Control, pp. 209–229, Singapore: Springer Nature, 2022.

[12] M. J. Haber, B. Chappell, and C. Hills, "Mitigation Strategies," in *Cloud Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Cloud Resources* (M. J. Haber, B. Chappell, and C. Hills, eds.), pp. 221–296, Berkeley, CA: Apress, 2022.

[13] J. Lloyd, "Additional Workload Architectural Considerations," in *Infrastructure Leader's Guide to Google Cloud: Lead Your Organization's Google Cloud Adoption, Migration and Modernization Journey* (J. Lloyd, ed.), pp. 279–314, Berkeley, CA: Apress, 2023.

[14] "Agentless vs. Agent Based Security & Monitoring: How to Choose?."

[15] C. Tozzi, "Agent-Based vs Agentless Security: Which Approach is Better?," Feb. 2023.

[16] M. Carle, "Key Benefits of Agentless Cloud Security," Oct. 2022.

[17] M. Brattstrom and P. Morreale, "Scalable Agentless Cloud Network Monitoring," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, pp. 171–176, June 2017.

[18] N. Meghanathan, *Review of Access Control Models for Cloud Computing*, vol. 3. Sept. 2013. Journal Abbreviation: Computer Science & Information Technology Pages: 85 Publication Title: Computer Science & Information Technology.

[19] M. W. Sanders and C. Yue, "Mining least privilege attribute based access control policies," in *Proceedings of the 35th Annual Computer Security Applications Conference*, ACSAC '19, (New York, NY, USA), pp. 404–416, Association for Computing Machinery, Dec. 2019.

[20] Y. Xia, L. Kuang, and M. Zhu, "A Hierarchical Access Control Scheme in Cloud using HHECC," *Information Technology Journal*, vol. 9, pp. 1598–1606, Aug. 2010.

[21] F. Cai, N. Zhu, J. He, P. Mu, W. Li, and Y. Yu, "Survey of access control models and technologies for cloud computing," *Cluster Computing*, vol. 22, pp. 6111–6122, May 2019.

[22] P. G. Shynu and K. J. Singh, "A Comprehensive Survey and Analysis on Access Control Schemes in Cloud Environment," *Cybernetics and Information Technologies*, vol. 16, pp. 19–38, Mar. 2016.

[23] P. K and J. Priya S, "Analysis of Different Access Control Mechanism in Cloud," *International Journal of Applied Information Systems*, vol. 4, pp. 34–39, Sept. 2012.

[24] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations," Tech. Rep. NIST SP 800-162, National Institute of Standards and Technology, Jan. 2014.

[25] Y. A. Younis, K. Kifayat, and M. Merabti, "An access control model for cloud computing," *Journal of Information Security and Applications*, vol. 19, pp. 45–60, Feb. 2014.

[26] M. Mulimani and R. Rachh, "Analysis of Access Control Methods in Cloud Computing," July 2016.

[27] R. El Sibai, N. Gemayel, J. Bou Abdo, and J. Demerjian, "A survey on access control mechanisms for cloud computing," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, p. e3720, 2020. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/ett.3720.

[28] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "A data outsourcing architecture combining cryptography and access control," in *Proceedings of the 2007 ACM workshop on Computer security architecture*, CSAW '07, (New York, NY, USA), pp. 63–69, Association for Computing Machinery, Nov. 2007.

[29] R. Aluvalu and L. Muddana, "A Survey on Access Control Models in Cloud Computing," in *Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1*

(S. C. Satapathy, A. Govardhan, K. S. Raju, and J. K. Mandal, eds.), Advances in Intelligent Systems and Computing, (Cham), pp. 653–664, Springer International Publishing, 2015.

[30] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models,"

[31] G. Karataş and A. Akbulut, "Survey on Access Control Mechanisms in Cloud Computing," *Journal of Cyber Security and Mobility*, vol. 7, pp. 1–36, July 2018. Publisher: River Publishers.

[32] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-Based Access Control," *Computer*, vol. 48, pp. 85–88, Feb. 2015. Conference Name: Computer.

[33] A. R. Khan, "Access control in cloud computing environment," *ARPN Journal of Engineering and Applied Sciences*, vol. 7, no. 5, pp. 613–615, 2012.

[34] K. Popović and Hocenski, "Cloud computing security issues and challenges," in *The 33rd International Convention MIPRO*, pp. 344–349, May 2010.

[35] G. S. Mahmood, D. J. Huang, and B. A. Jaleel, "A Secure Cloud Computing System by Using Encryption and Access Control Model," *Journal of Information Processing Systems*, vol. 15, pp. 538–549, June 2019.

[36] U. Lang and R. Schreiner, "Implementing Least Privilege for Interconnected, Agile SOAs/Clouds," in *ISSE 2012 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2012 Conference* (H. Reimer, N. Pohlmann, and W. Schneider, eds.), pp. 89–102, Wiesbaden: Springer Fachmedien, 2012.

[37] J. Saltzer and M. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, pp. 1278–1308, Sept. 1975. Conference Name: Proceedings of the IEEE.

[38] D. Shields, "Chapter 4: Policies & procedures for secure access p. 62-70," in *AWS Security*, p. 312, Manning Publications Co. LLC, Sept. 2022.

[39] D. Shields, "Chapter 2: Identity and Access Management p. 17-43," in *AWS Security*, p. 312, Manning Publications Co. LLC, Sept. 2022.

[40] "Giving Third Parties Limited Access to your AWS Account," Aug. 2020.

[41] N. Khasuntsev, "Automatic Detection of Misconfigurations of AWS Identity and Access Management Policies,"

[42] "What is IAM? - AWS Identity and Access Management."

[43] "IAM Identities (users, user groups, and roles) - AWS Identity and Access Management."

[44] T. van Ede, N. Khasuntsev, B. Steen, and A. Continella, "Detecting Anomalous Misconfigurations in AWS Identity and Access Management Policies," in *Proceedings of the 2022 on Cloud Computing Security Workshop*, (Los Angeles CA USA), pp. 63–74, ACM, Nov. 2022.

[45] "What is AWS."

[46] "Policies and permissions in IAM - AWS Identity and Access Management."

[47] I. A. Mohammed, "CLOUD IDENTITY AND ACCESS MANAGEMENT - A MODEL PROPOSAL," *SSRN Electronic Journal*, vol. 6, pp. 1–8, Oct. 2019.

[48] P. Gill, "Least-Privilege Identity-Based Policies for Lambda Functions in Amazon Web Services (AWS)," Master's thesis, University of Waterloo, Dec. 2020. Accepted: 2020-12-21T17:29:01Z.

[49] "Managed policies and inline policies - AWS Identity and Access Management."

[50] "Access Advisor - Mastering AWS Security [Book]." ISBN: 9781788293723.

[51] "IAM Access Analyzer vs Access Advisor," Dec. 2022.

[52] W. Wang, J. Han, M. Song, and X. Wang, "The design of a trust and role based access control model in cloud computing," in *2011 6th International Conference on Pervasive Computing and Applications*, pp. 330–334, Oct. 2011.

[53] A. Coufalíková, I. Klaban, and T. Šlajs, "Complex strategy against supply chain attacks," in *2021 International Conference on Military Technologies (ICMT)*, pp. 1–5, IEEE, 2021.

[54] J. Huddleston, P. Ji, S. Bhunia, and J. Cogan, "How VMware Exploits Contributed to SolarWinds Supply-chain Attack," in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 760–765, Dec. 2021.

[55] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, "Solar winds hack: In-depth analysis and countermeasures," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–7, IEEE, 2021.

[56] M. Malecki and R. Hannigan, "Stopping the domino effect: Cyber resilience in the supply chain," 2022.

[57] M. W. Sanders and C. Yue, "Minimizing Privilege Assignment Errors in Cloud Services," in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, CODASPY '18, (New York, NY, USA), pp. 2–12, Association for Computing Machinery, Mar. 2018.

[58] S. Goutam, W. Enck, and B. Reaves, "Hestia: simple least privilege network policies for smart homes," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '19, (New York, NY, USA), pp. 215–220, Association for Computing Machinery, May 2019.

[59] V. Rastogi, D. Davidson, L. De Carli, S. Jha, and P. McDaniel, "Towards least privilege containers with cimplifier," *arXiv preprint arXiv:1602.08410*, 2016.

[60] R. Shimizu and H. Kanuka, "Test-Based Least Privilege Discovery on Cloud Infrastructure as Code," in *2020 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 1–8, Dec. 2020. ISSN: 2330-2186.

[61] O. Akinrolabu, S. New, and A. Martin, "Cyber supply chain risks in cloud computing – bridging the risk assessment gap," *Open Journal of Cloud Computing*, vol. 5, no. 1, 2017. Publisher: RonPub.

[62] V. Mani, C. Delgado, B. T. Hazen, and P. Patel, "Mitigating Supply Chain Risk via Sustainability Using Big Data Analytics: Evidence from the Manufacturing Supply Chain," *Sustainability*, vol. 9, p. 608, Apr. 2017. Number: 4 Publisher: Multidisciplinary Digital Publishing Institute.

[63] A. Razaque, M. B. H. Frej, B. Alotaibi, and M. Alotaibi, "Privacy Preservation Models for Third-Party Auditor over Cloud Computing: A Survey," *Electronics*, vol. 10, p. 2721, Jan. 2021. Number: 21 Publisher: Multidisciplinary Digital Publishing Institute.

[64] J. W. Creswell, *Research design: qualitative, quantitative, and mixed methods approaches*. Thousand Oaks: SAGE Publications, 4th ed ed., 2014.

[65] A. Ghebrehiwet Ghebremedhin, "Combining static source code analysis and threat assessment modeling for testing open source software security," Master's thesis, Universitetet i Agder / University of Agder, 2012. Accepted: 2012-10-03T11:19:50Z Publication Title: 121.

[66] "Security Audits of AWS Accounts - Roles, Policies and equivalents on GCP and Azure," Jan. 2020. Section: AWS.

[67] "ReadOnlyAccess - AWS Managed Policy."

[68] "ViewOnlyAccess - AWS Managed Policy."

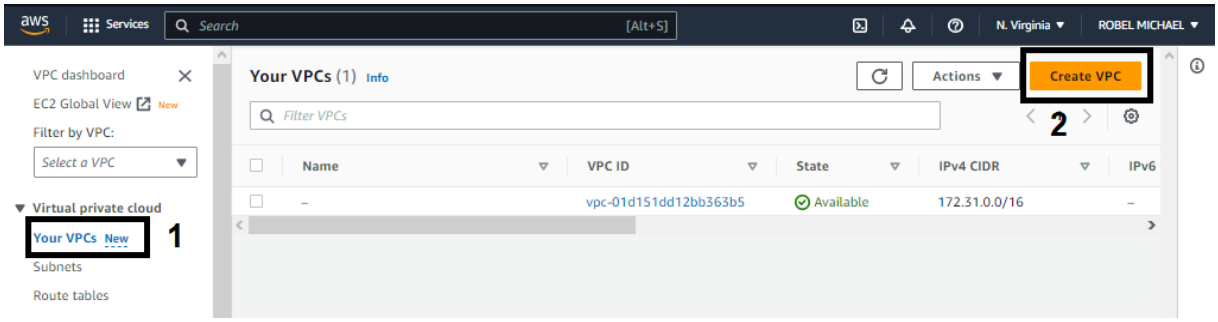
[69] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," Tech. Rep. NIST SP 800-30r1, National Institute of Standards and Technology, Gaithersburg, MD, 2012. Edition: 0.

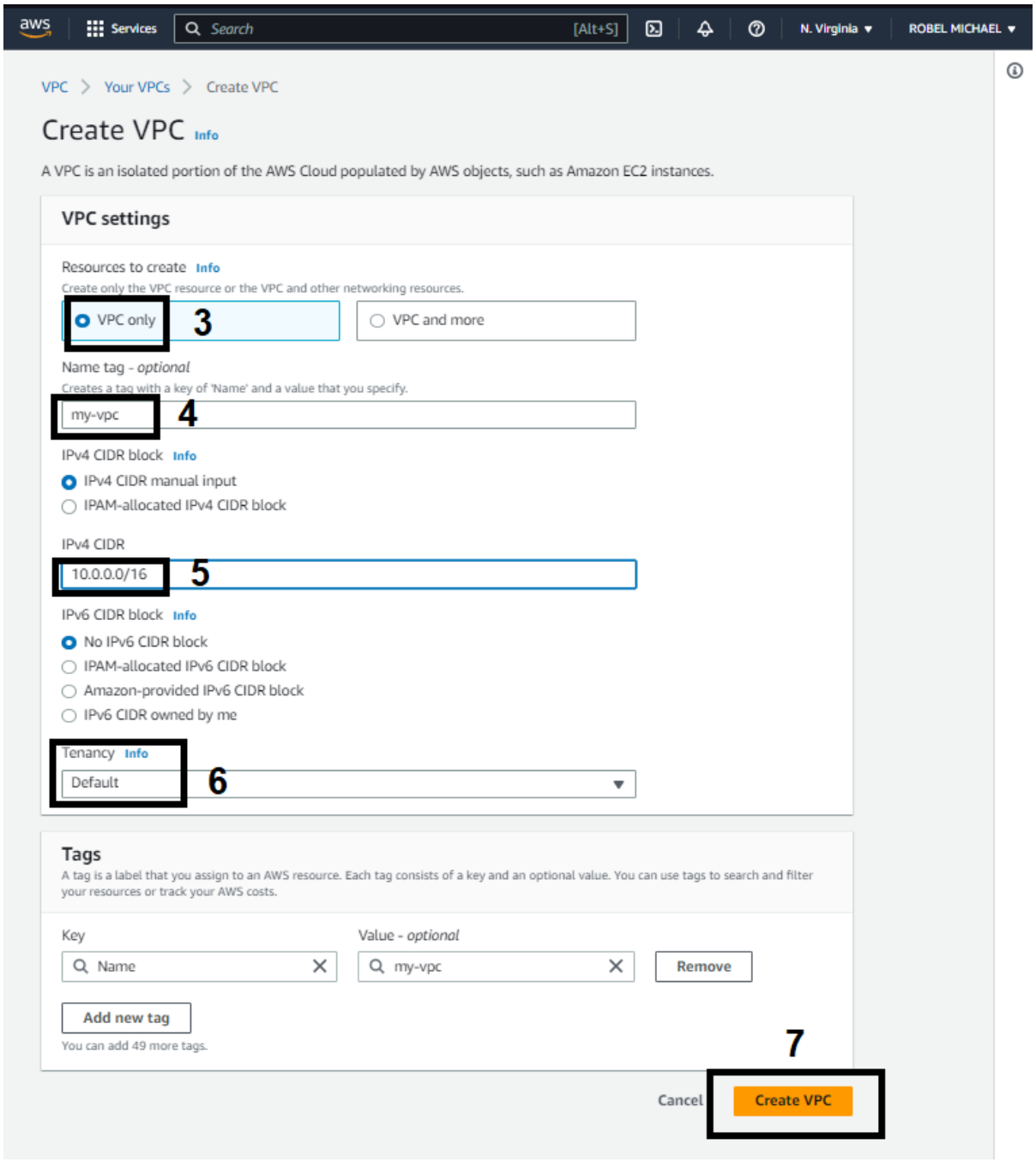
Appendix A

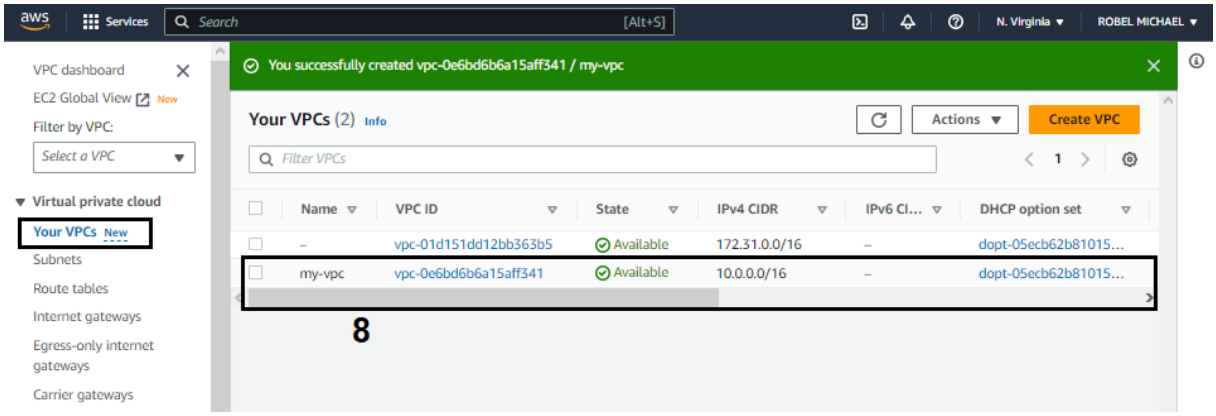
Appendix

Part 1: AWS - Lab environment VPC setup

1. Creating the virtual private cloud (VPC) in AWS console

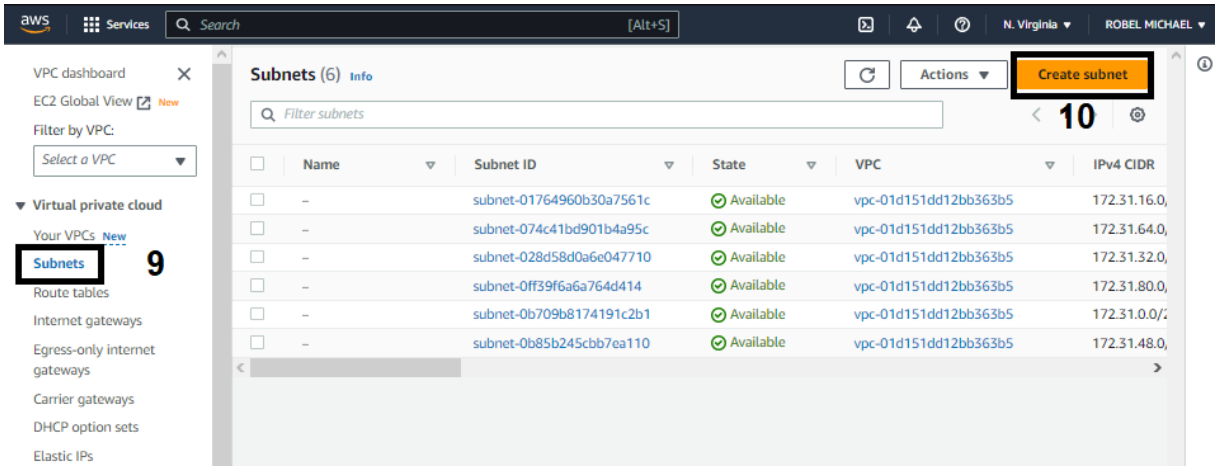


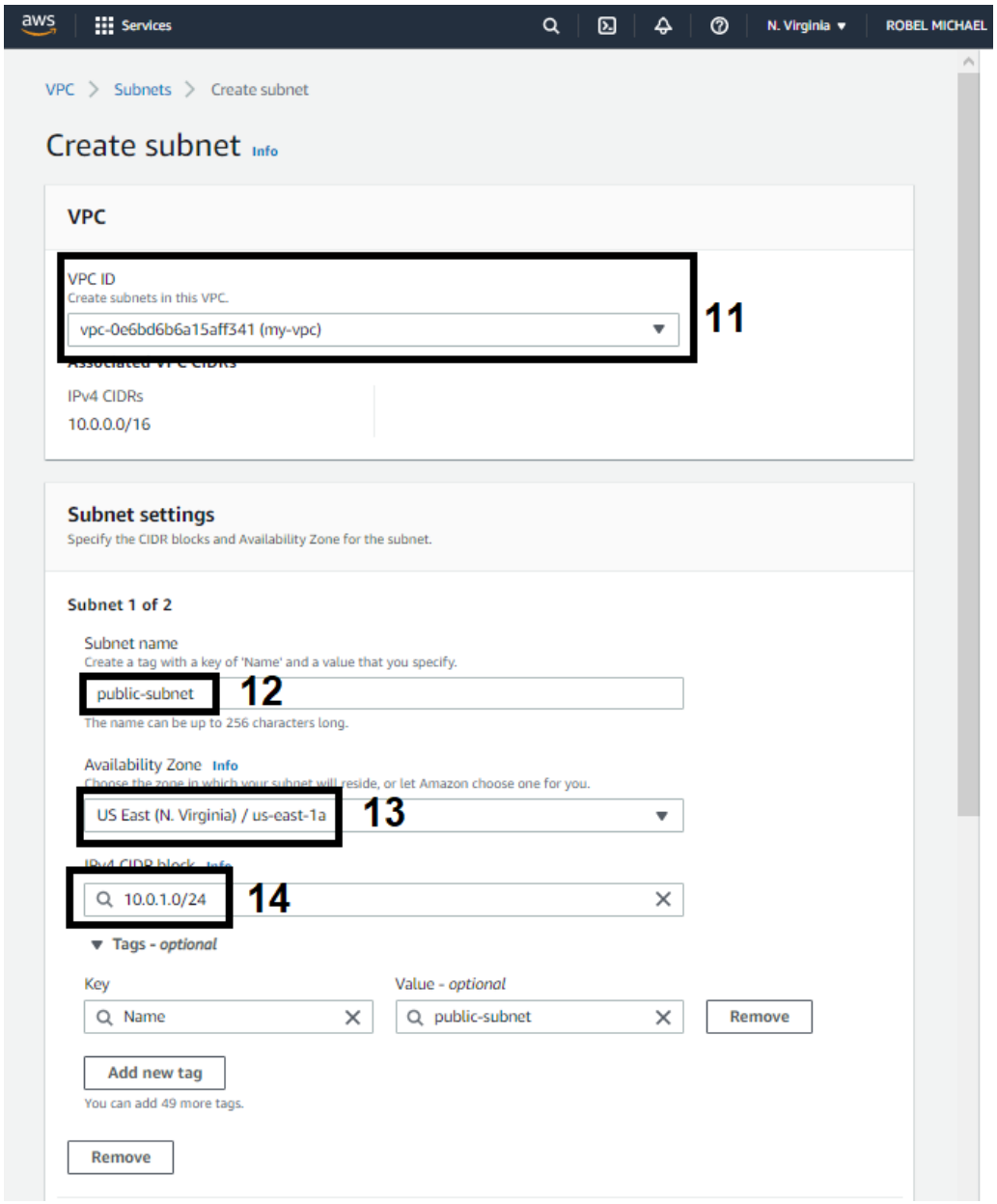


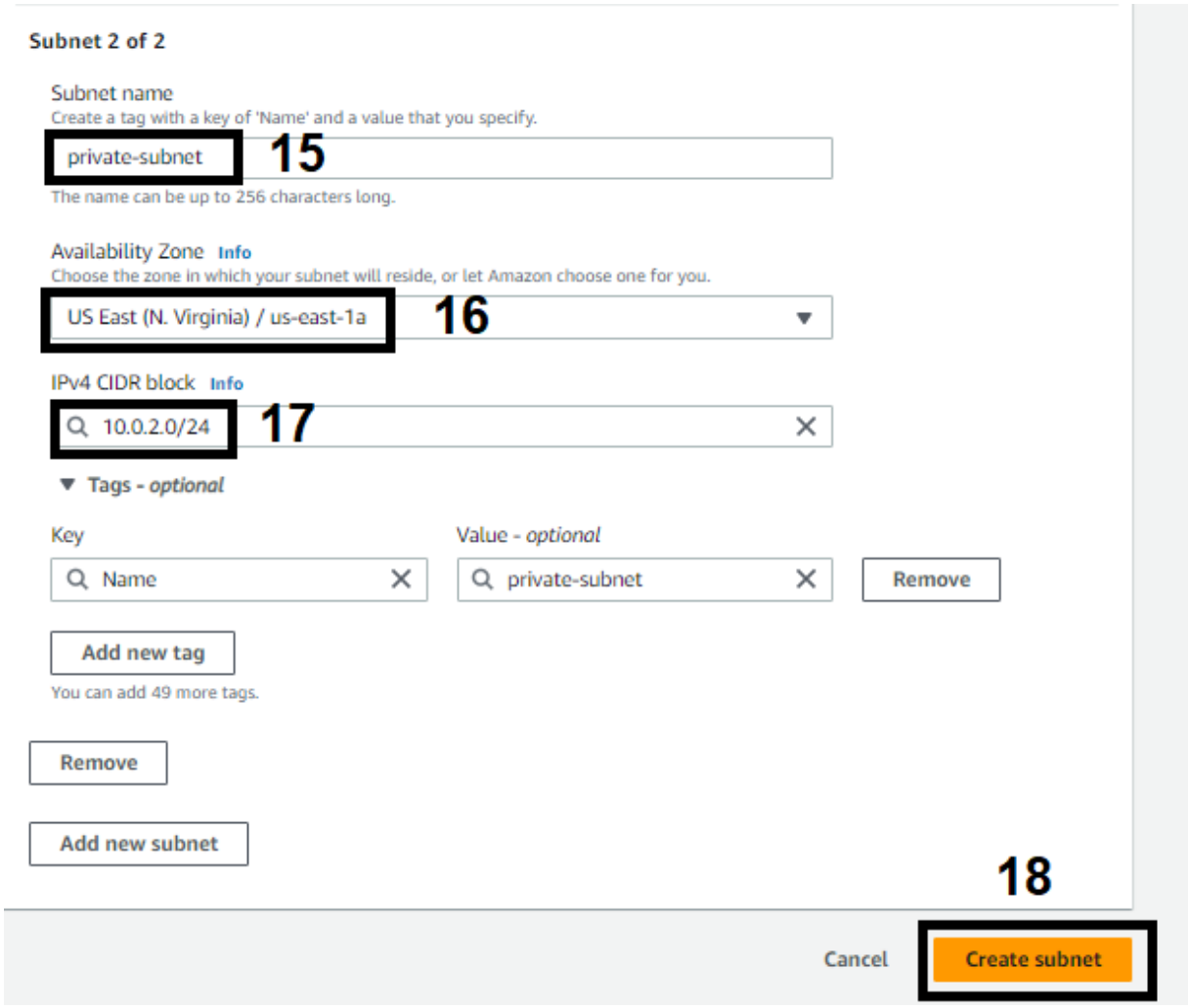

aws
Services
Search
[Alt+S]
N. Virginia
ROBEL MICHAEL
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs New
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
You successfully created vpc-0e6bd6b6a15aff341 / my-vpc
Your VPCs (2) Info
Actions
Create VPC
Filter VPCs
1
Name
VPC ID
State
IPv4 CIDR
IPv6 CI...
DHCP option set
–
vpc-01d151dd12bb363b5
Available
172.31.0.0/16
–
dopt-05ecb62b81015...
my-vpc
vpc-0e6bd6b6a15aff341
Available
10.0.0.0/16
–
dopt-05ecb62b81015...

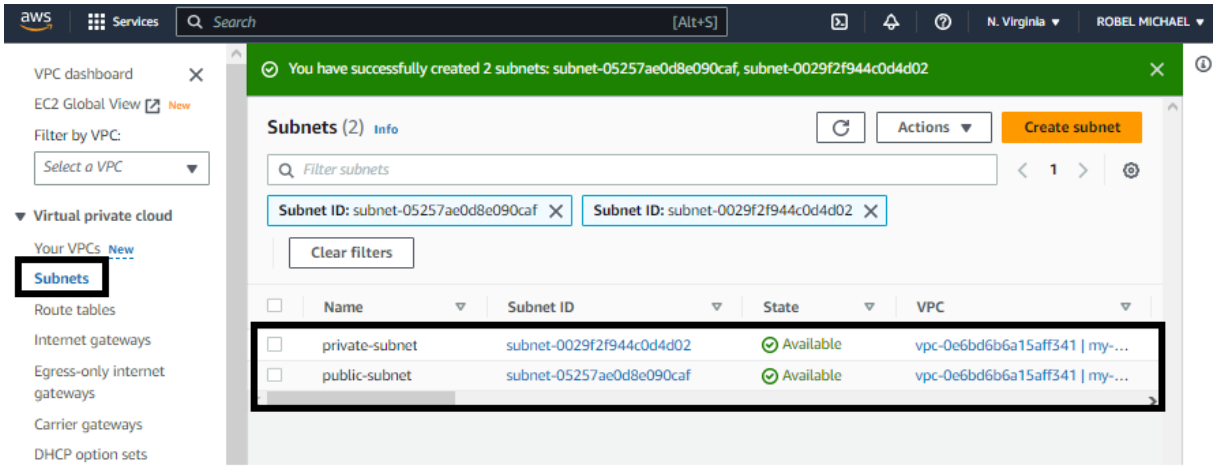
8

2. Setting up the public & private subnets

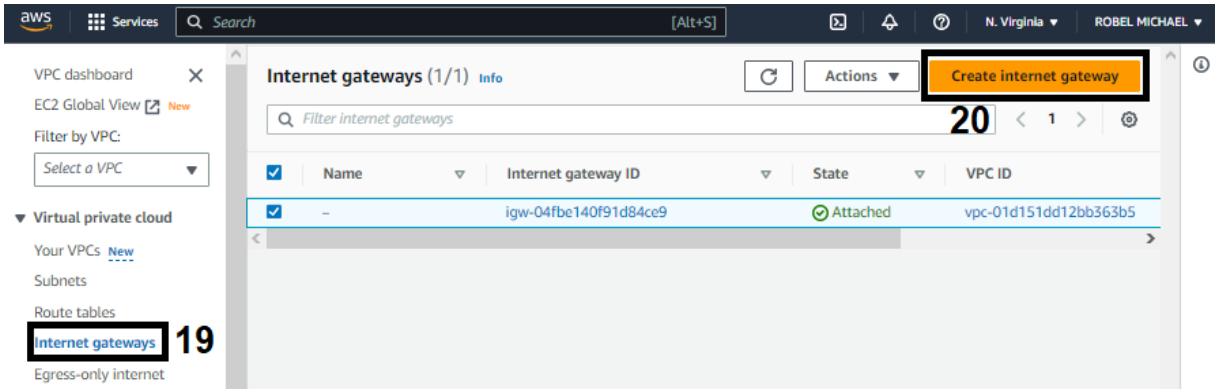


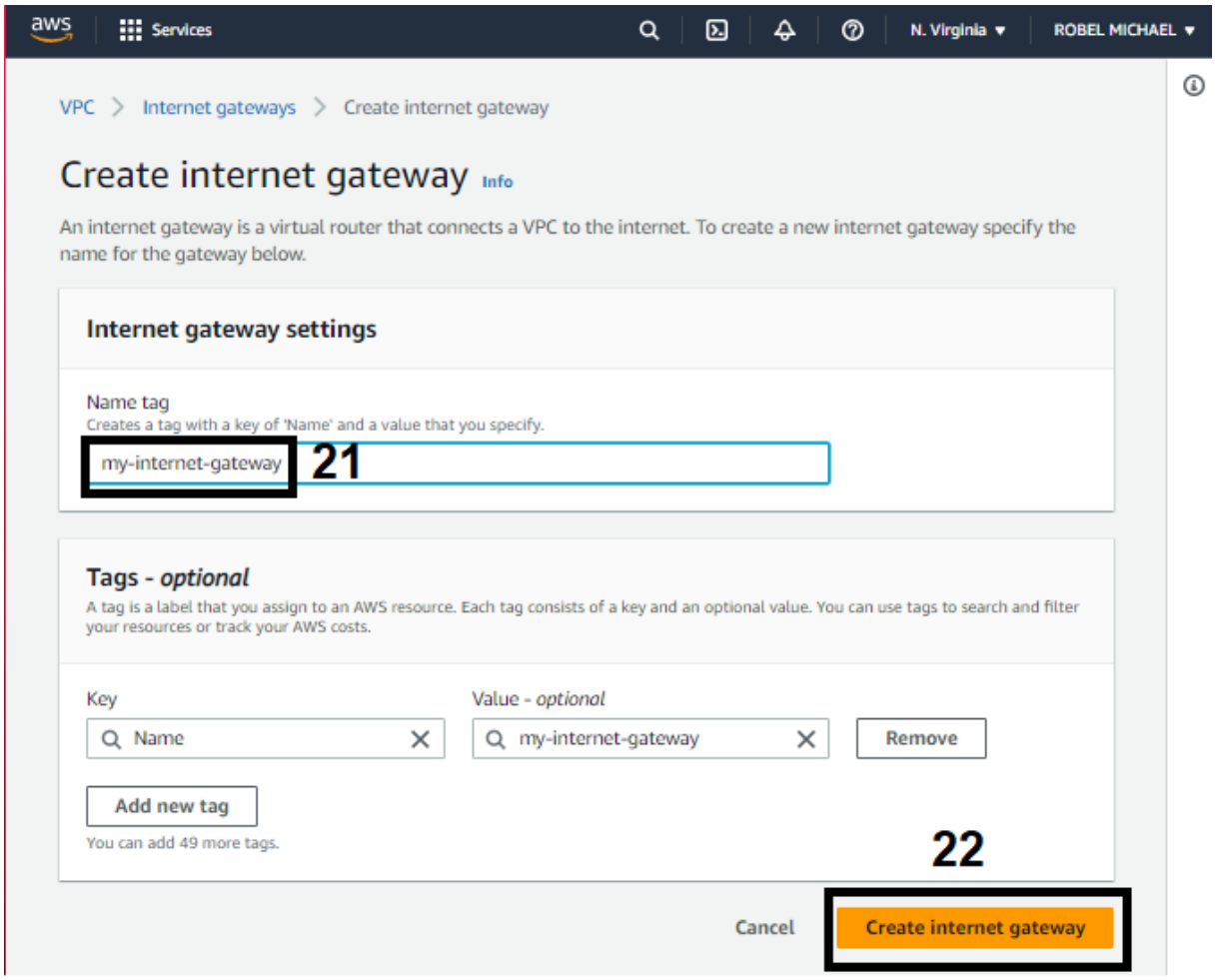


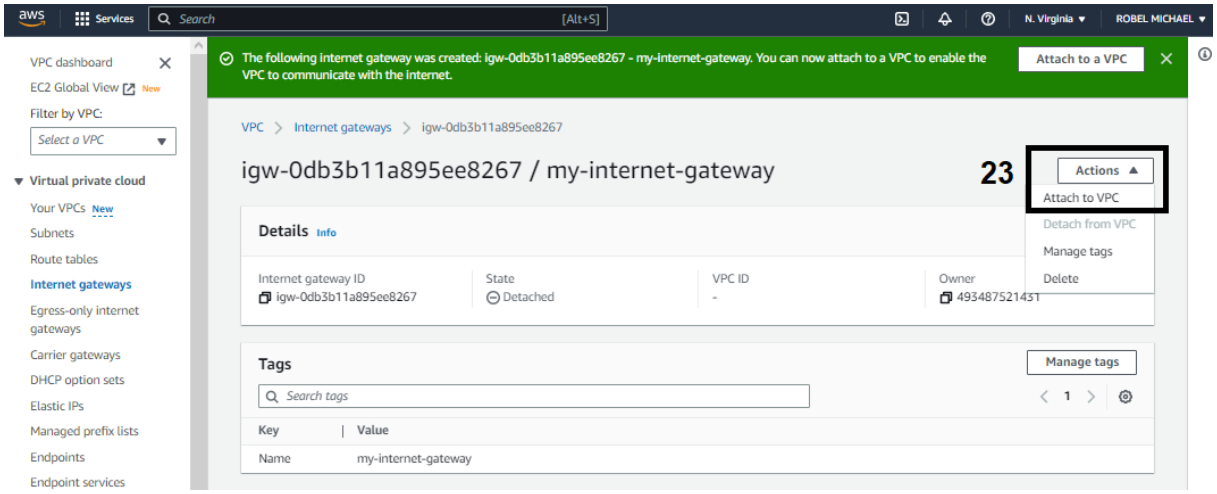

Subnet 2 of 2
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private-subnet
15
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a
16
IPv4 CIDR block Info
10.0.2.0/24
17
Tags - optional
Key
Name
Value - optional
private-subnet
Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet
18
Cancel
Create subnet

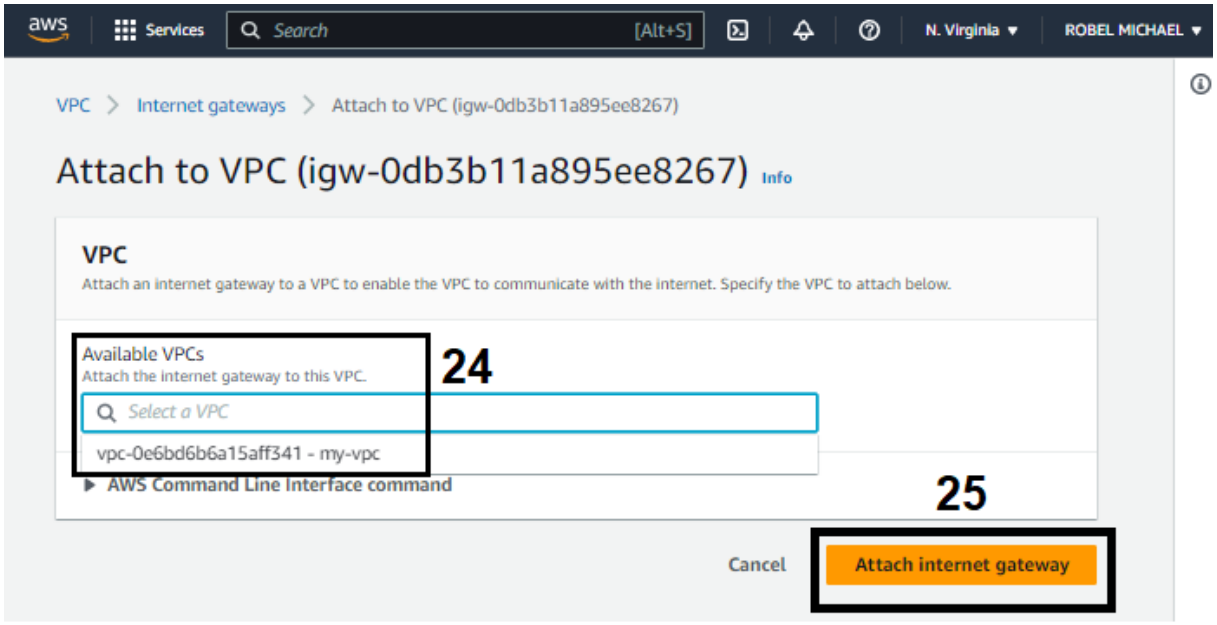

aws
Services
Search
[Alt+S]
N. Virginia
ROBEL MICHAEL
VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs New
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
You have successfully created 2 subnets: subnet-05257ae0d8e090caf, subnet-0029f2f944c0d4d02
Subnets (2) Info
Actions
Create subnet
Filter subnets
Subnet ID: subnet-05257ae0d8e090caf
Subnet ID: subnet-0029f2f944c0d4d02
Clear filters
Name
Subnet ID
State
VPC
private-subnet
subnet-0029f2f944c0d4d02
Available
vpc-0e6bd6b6a15aff341 | my-...
public-subnet
subnet-05257ae0d8e090caf
Available
vpc-0e6bd6b6a15aff341 | my-...

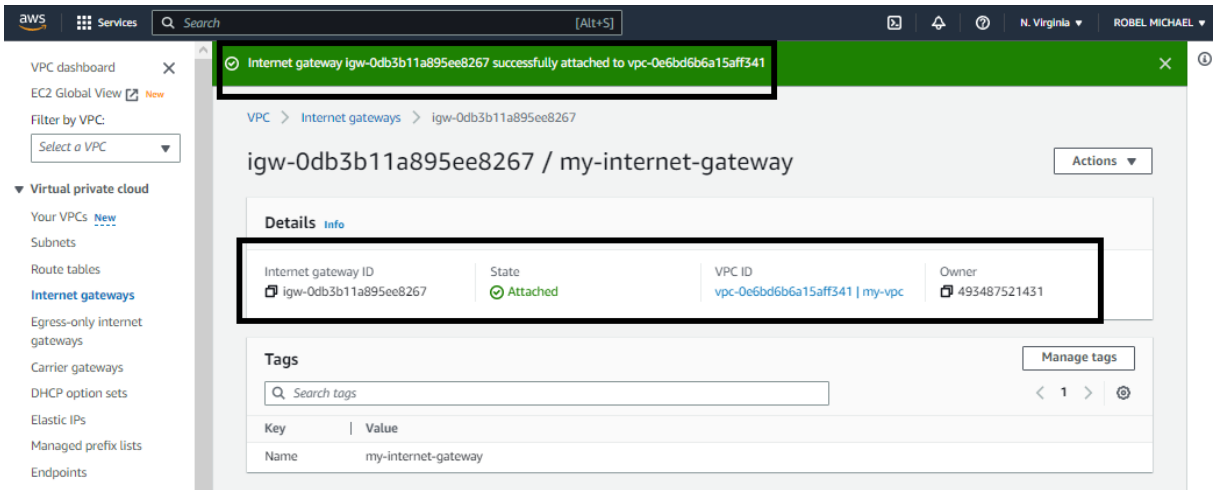
3. Creating Internet gateway & Routing table

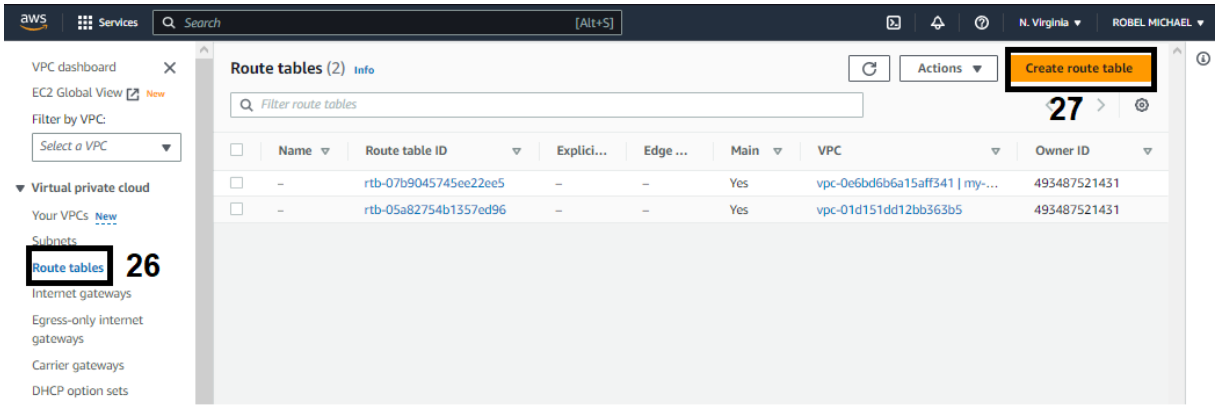


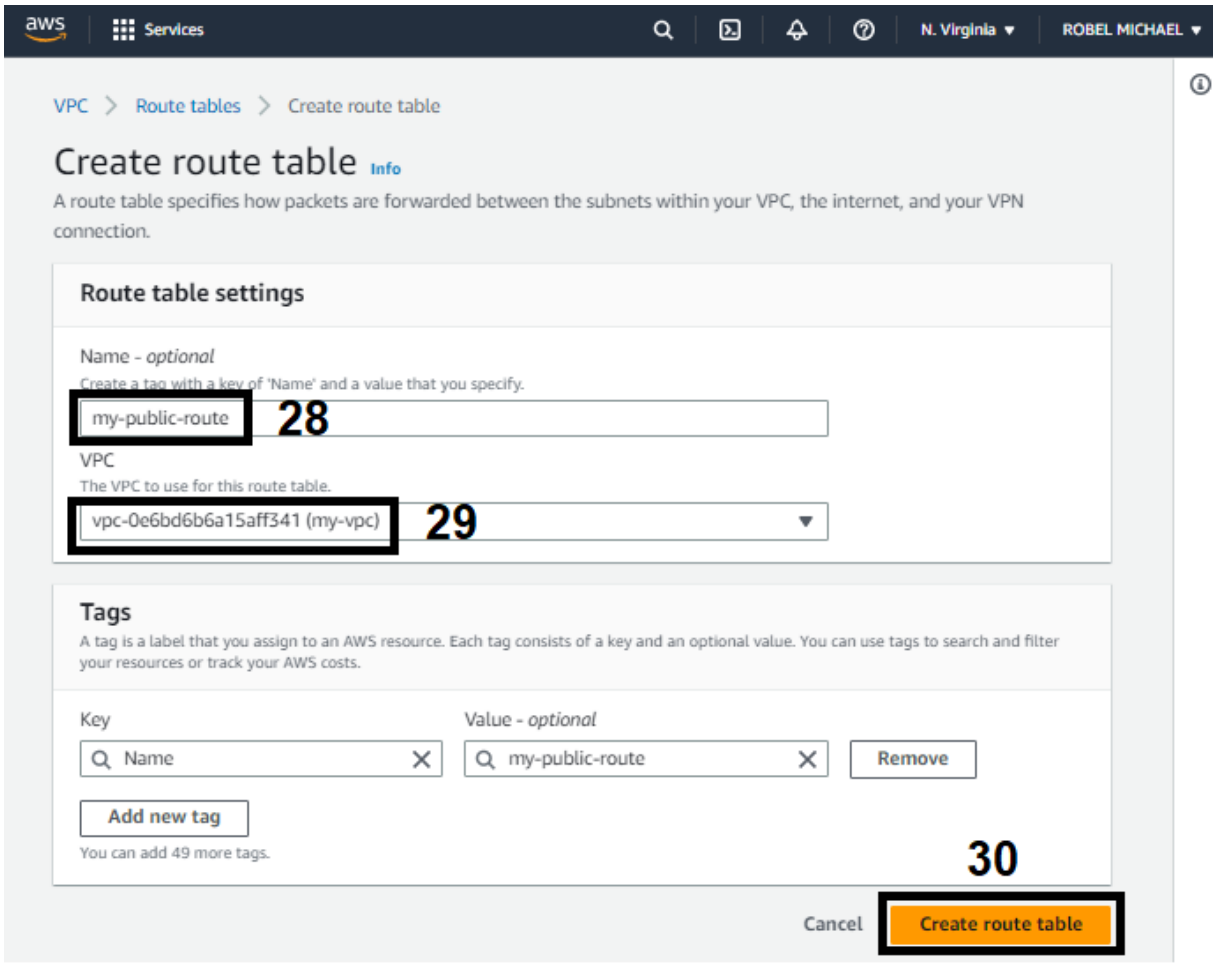


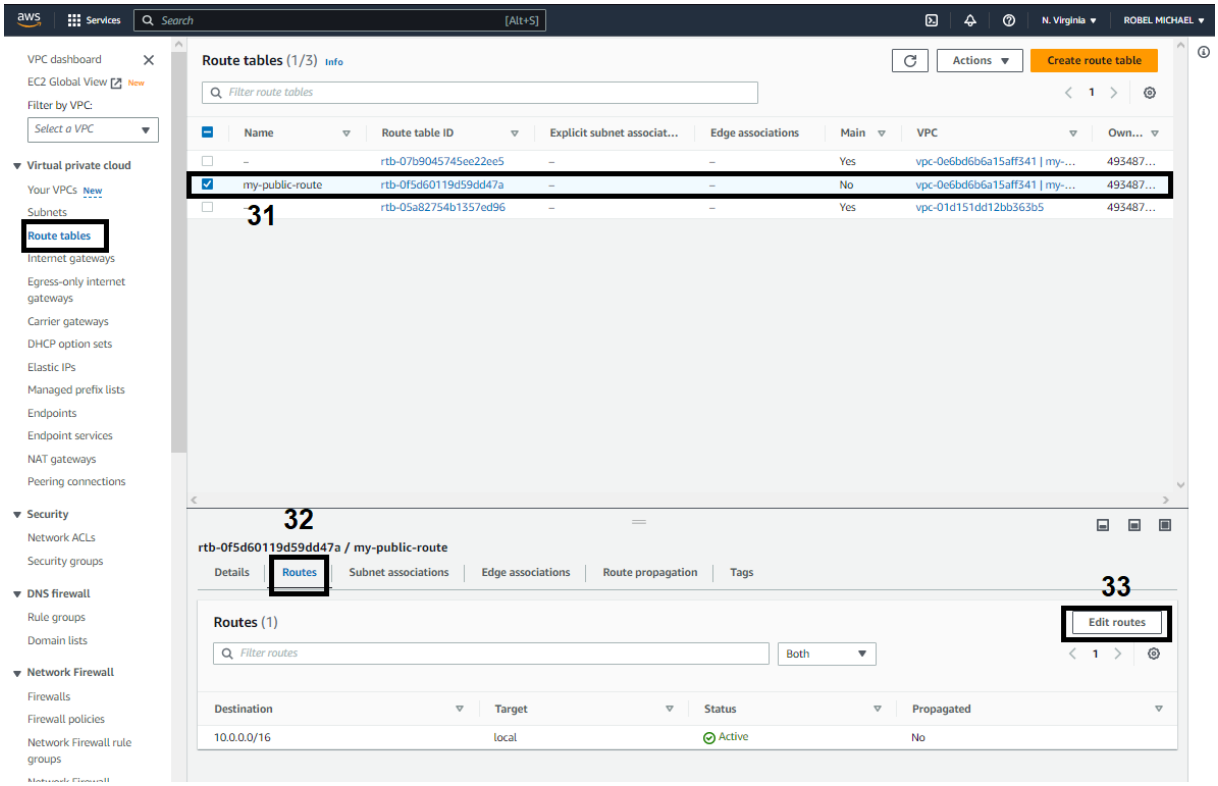

aws
Services
Search
[Alt+S]
N. Virginia
ROBEL MICHAEL
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
New
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
The following internet gateway was created: igw-0db3b11a895ee8267 - my-internet-gateway. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
VPC > Internet gateways > igw-0db3b11a895ee8267
igw-0db3b11a895ee8267 / my-internet-gateway
23
Actions
Attach to VPC
Detach from VPC
Manage tags
Delete
Details Info
Internet gateway ID
igw-0db3b11a895ee8267
State
Detached
VPC ID
-
Owner
493487521431
Tags
Manage tags
Search tags
1
Key
Value
Name
my-internet-gateway

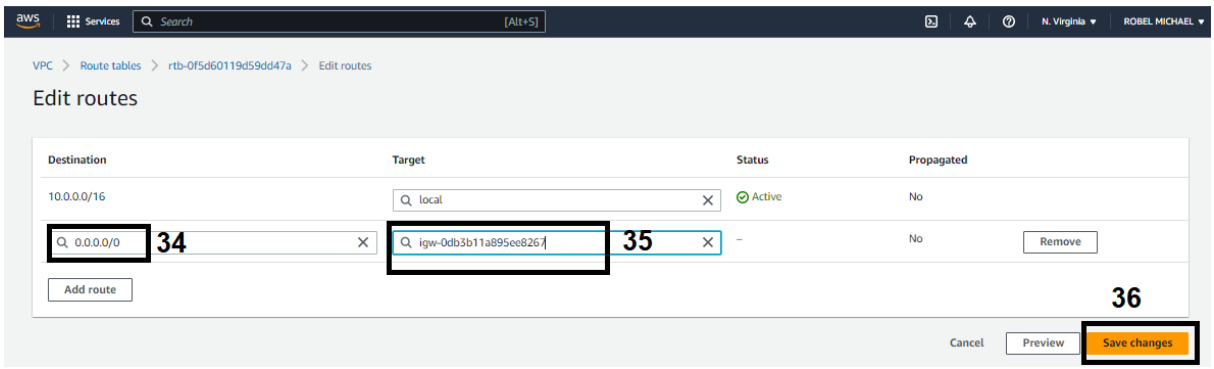

aws
Services
Search
[Alt+S]
N. Virginia
ROBEL MICHAEL
VPC > Internet gateways > Attach to VPC (igw-0db3b11a895ee8267)
Attach to VPC (igw-0db3b11a895ee8267) Info
VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.
Available VPCs
Attach the internet gateway to this VPC.
24
Select a VPC
vpc-0e6bd6b6a15aff341 - my-vpc
AWS Command Line Interface command
25
Cancel
Attach internet gateway

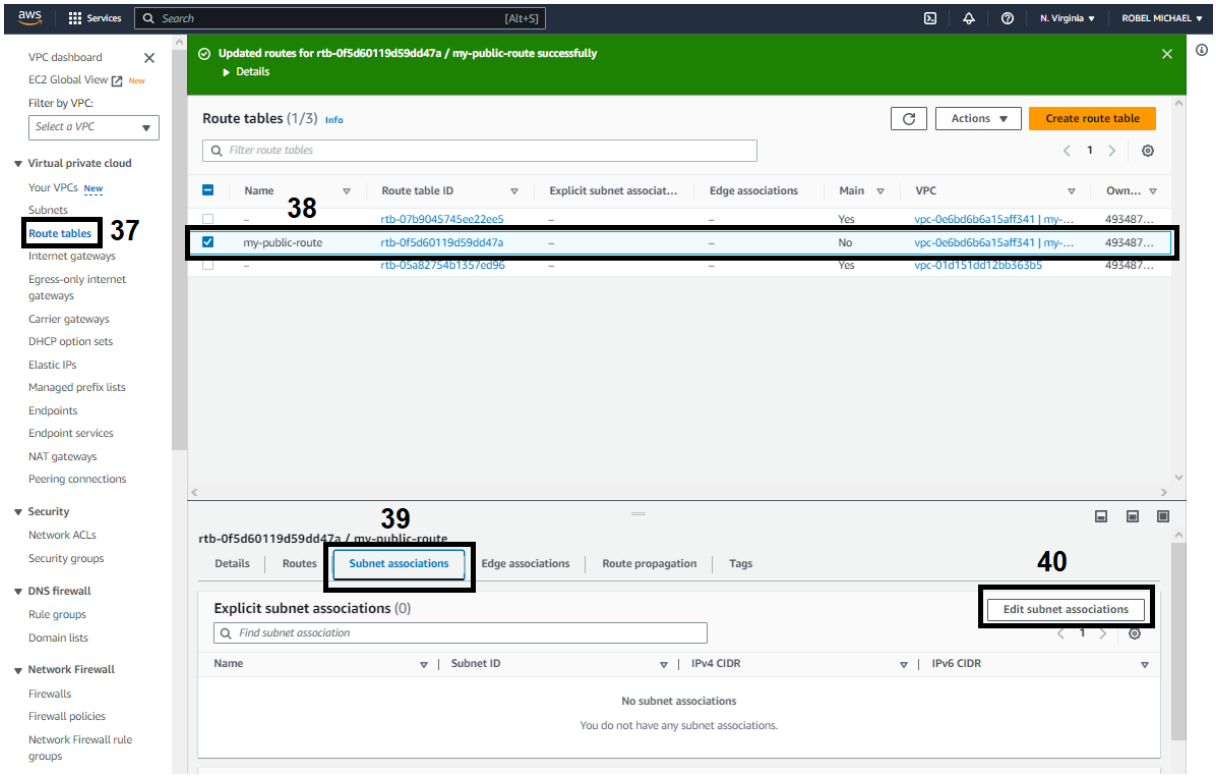

aws
Services
Search
[Alt+S]
N. Virginia
ROBEL MICHAEL
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
New
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Internet gateway igw-0db3b11a895ee8267 successfully attached to vpc-0e6bd6b6a15aff341
VPC > Internet gateways > igw-0db3b11a895ee8267
igw-0db3b11a895ee8267 / my-internet-gateway
Actions
Details Info
Internet gateway ID
igw-0db3b11a895ee8267
State
Attached
VPC ID
vpc-0e6bd6b6a15aff341 | my-vpc
Owner
493487521431
Tags
Manage tags
Search tags
1
Key
Value
Name
my-internet-gateway

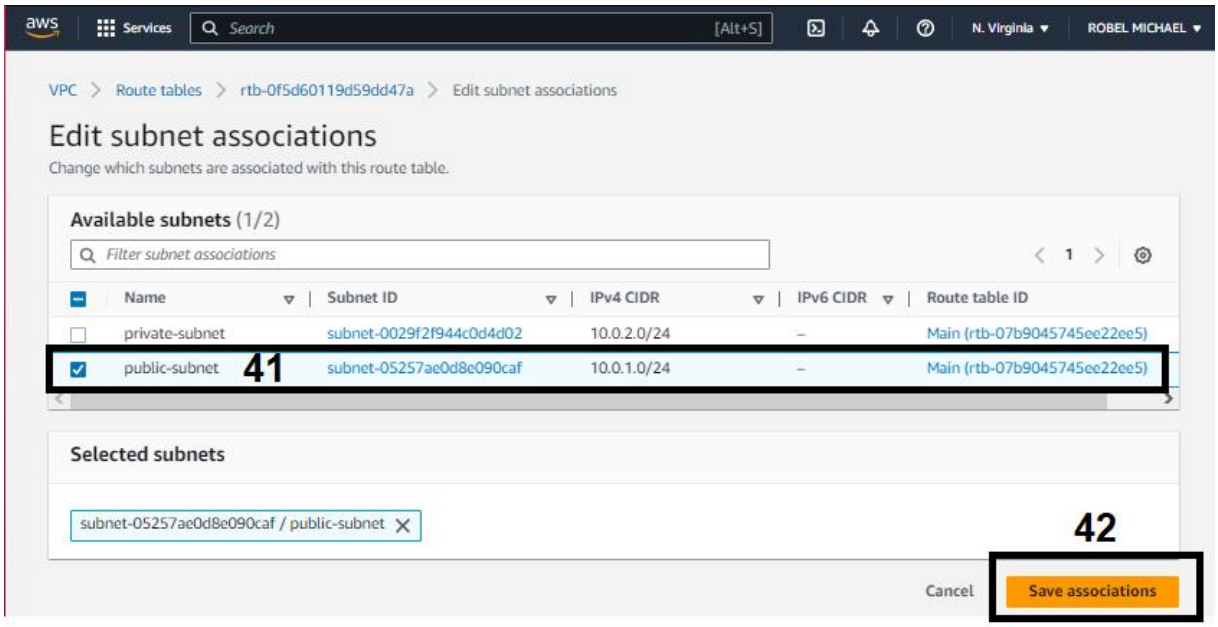

aws
Services
Search
[Alt+S]
N. Virginia
ROBEL MICHAEL
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
New
Subnets
Route tables
26
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Route tables (2)
Info
Actions
Create route table
27
Filter route tables
Name
Route table ID
Explici...
Edge ...
Main
VPC
Owner ID
rtb-07b9045745ee22ee5
Yes
vpc-0e6bd6b6a15aff341 | my-...
493487521431
rtb-05a82754b1357ed96
Yes
vpc-01d151dd12bb363b5
493487521431

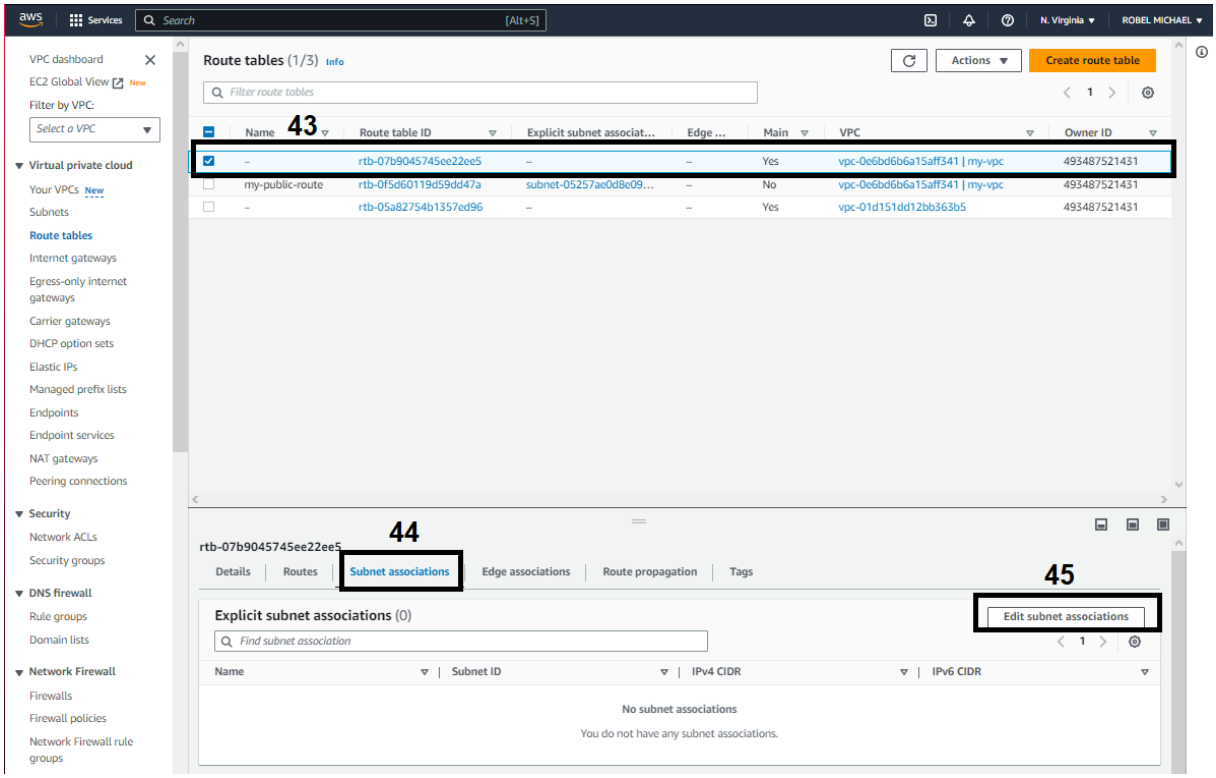

aws
Services
N. Virginia
ROBEL MICHAEL
VPC
Route tables
Create route table
Create route table
Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
my-public-route
28
VPC
The VPC to use for this route table.
vpc-0e6bd6b6a15aff341 (my-vpc)
29
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
my-public-route
Remove
Add new tag
You can add 49 more tags.
30
Cancel
Create route table

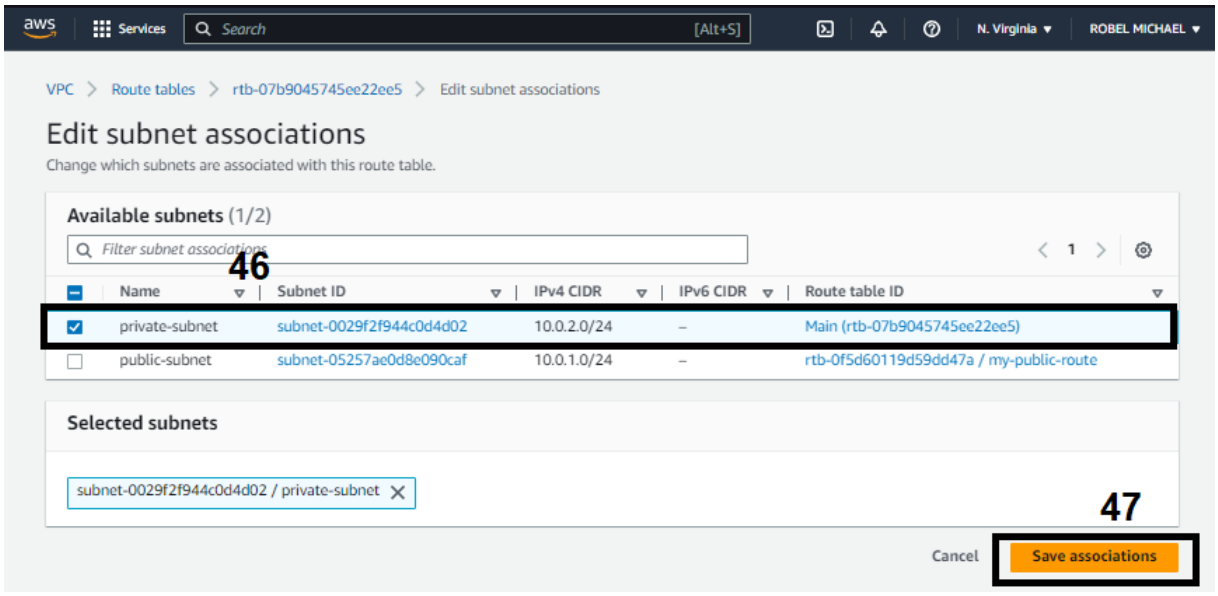

Route tables (1/3) Info
Actions
Create route table
Name
Route table ID
Explicit subnet associat...
Edge associations
Main
VPC
my-public-route
rtb-0f5d60119d59dd47a
31
32
rtb-0f5d60119d59dd47a / my-public-route
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
33
Edit routes
Routes (1)
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No


VPC > Route tables > rtb-0f5d60119d59dd47a > Edit routes
Edit routes
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No
0.0.0.0/0
34
igw-0db3b11a895ee8267
35
No
Remove
Add route
36
Cancel
Preview
Save changes

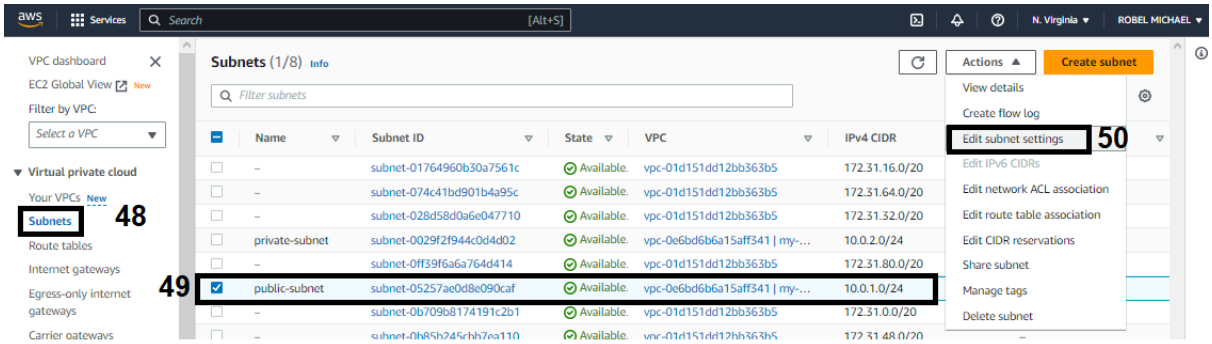

Updated routes for rtb-0f5d60119d59dd47a / my-public-route successfully
Details
Route tables (1/3) Info
Actions
Create route table
Filter route tables
Name
Route table ID
Explicit subnet associat...
Edge associations
Main
VPC
38
rtb-07b9045745ee22ee5
Yes
vpc-0e6bd6b6a15aff341 | my-...
my-public-route
rtb-0f5d60119d59dd47a
No
vpc-0e6bd6b6a15aff341 | my-...
rtb-05a82754b1357ed96
Yes
vpc-01d151dd12bb363b5
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
37
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
39
rtb-0f5d60119d59dd47a / my-public-route
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
40
Explicit subnet associations (0)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
No subnet associations
You do not have any subnet associations.

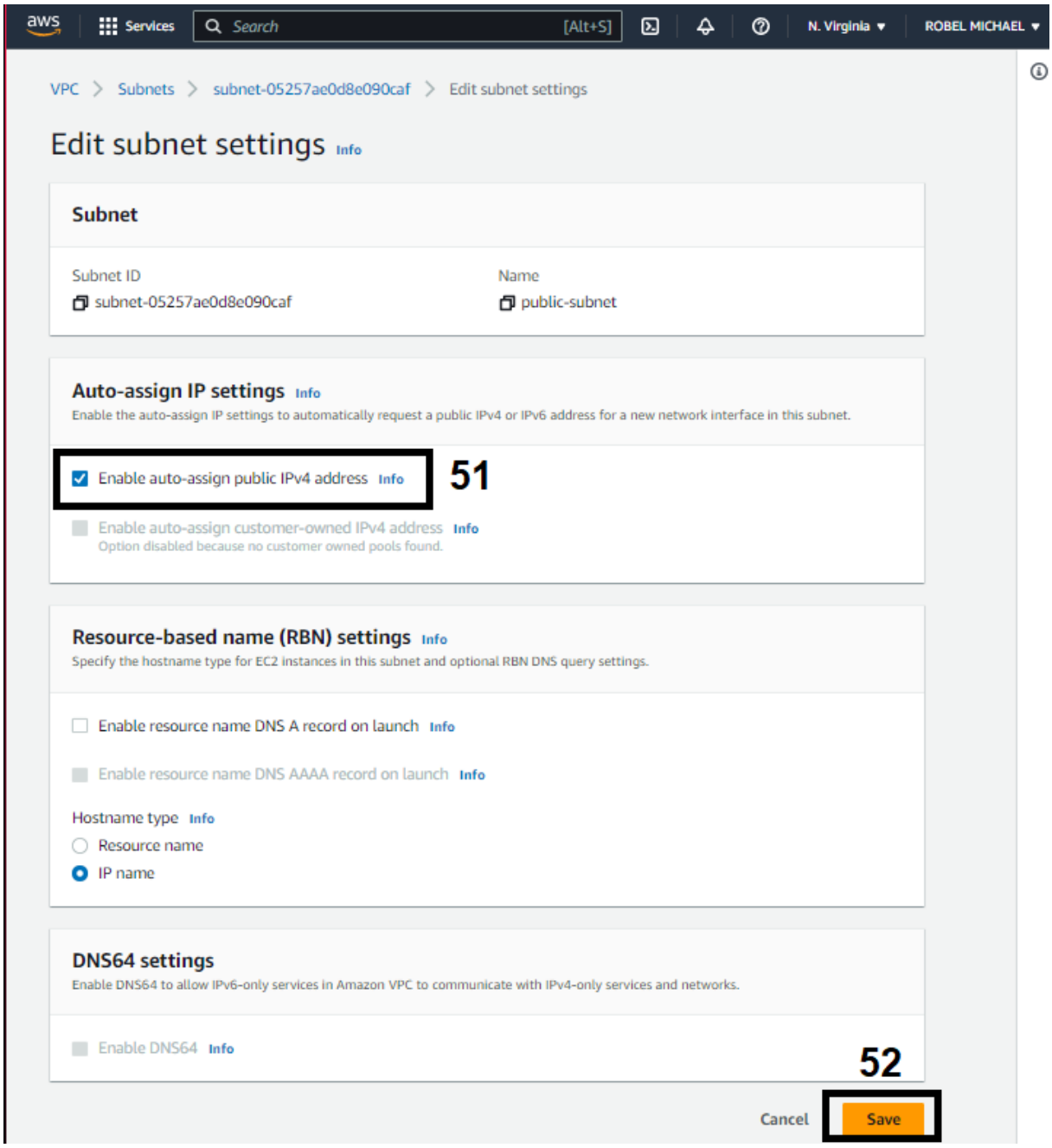

VPC > Route tables > rtb-0f5d60119d59dd47a > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/2)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
private-subnet
subnet-0029f2f944c0d4d02
10.0.2.0/24
Main (rtb-07b9045745ee22ee5)
public-subnet
41
subnet-05257ae0d8e090caf
10.0.1.0/24
Main (rtb-07b9045745ee22ee5)
Selected subnets
subnet-05257ae0d8e090caf / public-subnet
42
Cancel
Save associations


aws
Services
Search
[Alt+S]
N. Virginia
ROBEL MICHAEL
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
New
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
Route tables (1/3)
Info
Actions
Create route table
Filter route tables
1
43
Name
Route table ID
Explicit subnet associat...
Edge ...
Main
VPC
Owner ID
rtb-07b9045745ee22ee5
Yes
vpc-0e6bd6b6a15aff341 | my-vpc
493487521431
my-public-route
rtb-0f5d60119d59dd47a
subnet-05257ae0d8e09...
No
vpc-0e6bd6b6a15aff341 | my-vpc
493487521431
rtb-05a82754b1357ed96
Yes
vpc-01d151dd12bb363b5
493487521431
rtb-07b9045745ee22ee5
44
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
45
Edit subnet associations
Explicit subnet associations (0)
Find subnet association
1
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
No subnet associations
You do not have any subnet associations.

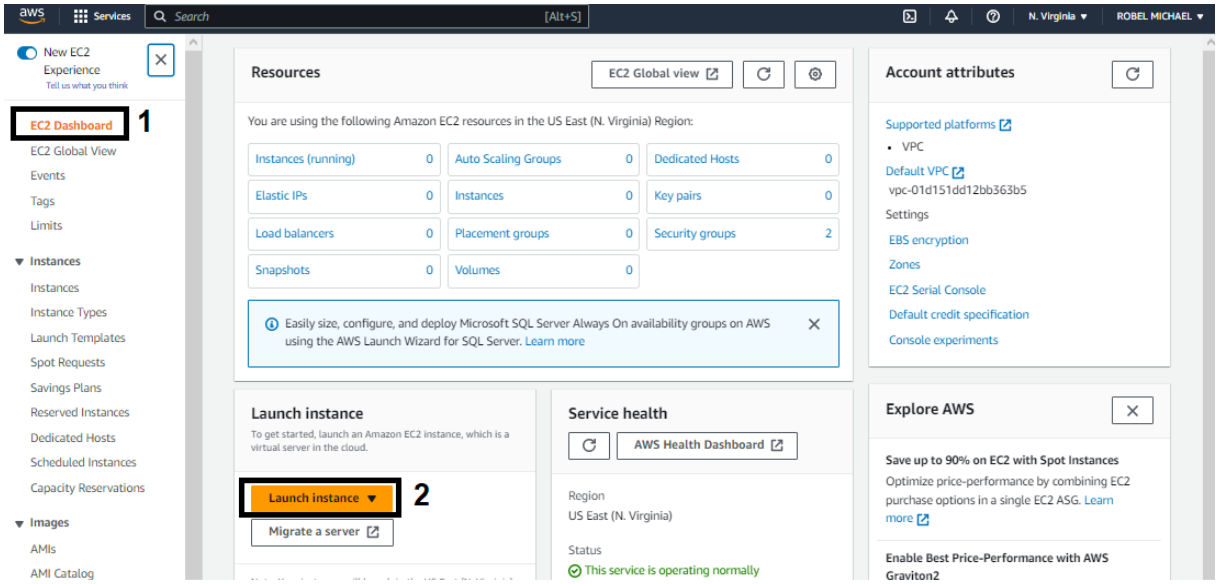

aws
Services
Search
[Alt+S]
N. Virginia
ROBEL MICHAEL
VPC
Route tables
rtb-07b9045745ee22ee5
Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/2)
Filter subnet associations
1
46
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
private-subnet
subnet-0029f2f944c0d4d02
10.0.2.0/24
–
Main (rtb-07b9045745ee22ee5)
public-subnet
subnet-05257ae0d8e090caf
10.0.1.0/24
–
rtb-0f5d60119d59dd47a / my-public-route
Selected subnets
subnet-0029f2f944c0d4d02 / private-subnet
47
Cancel
Save associations

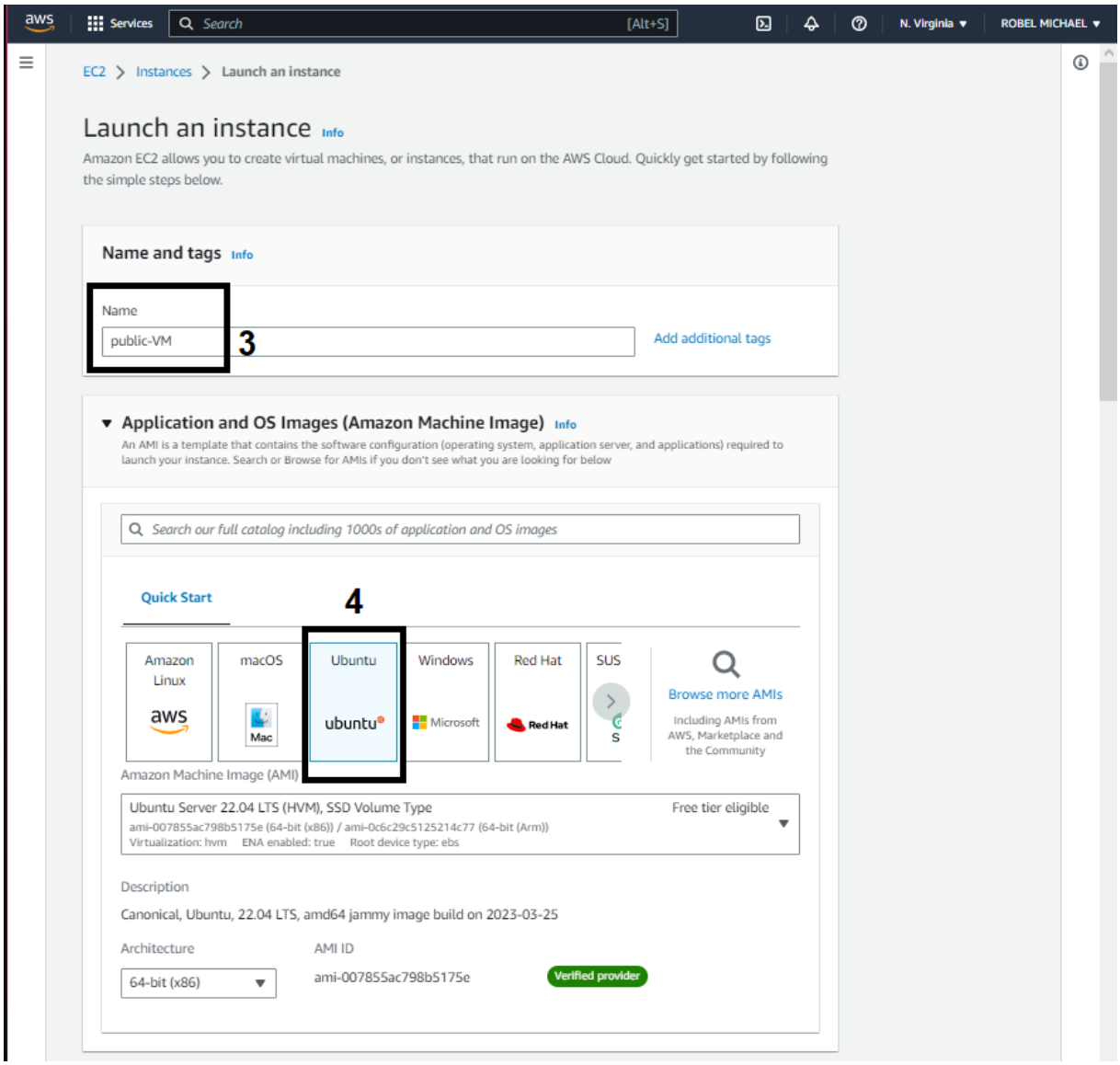
4. Enabling IPv4 on the public subnet

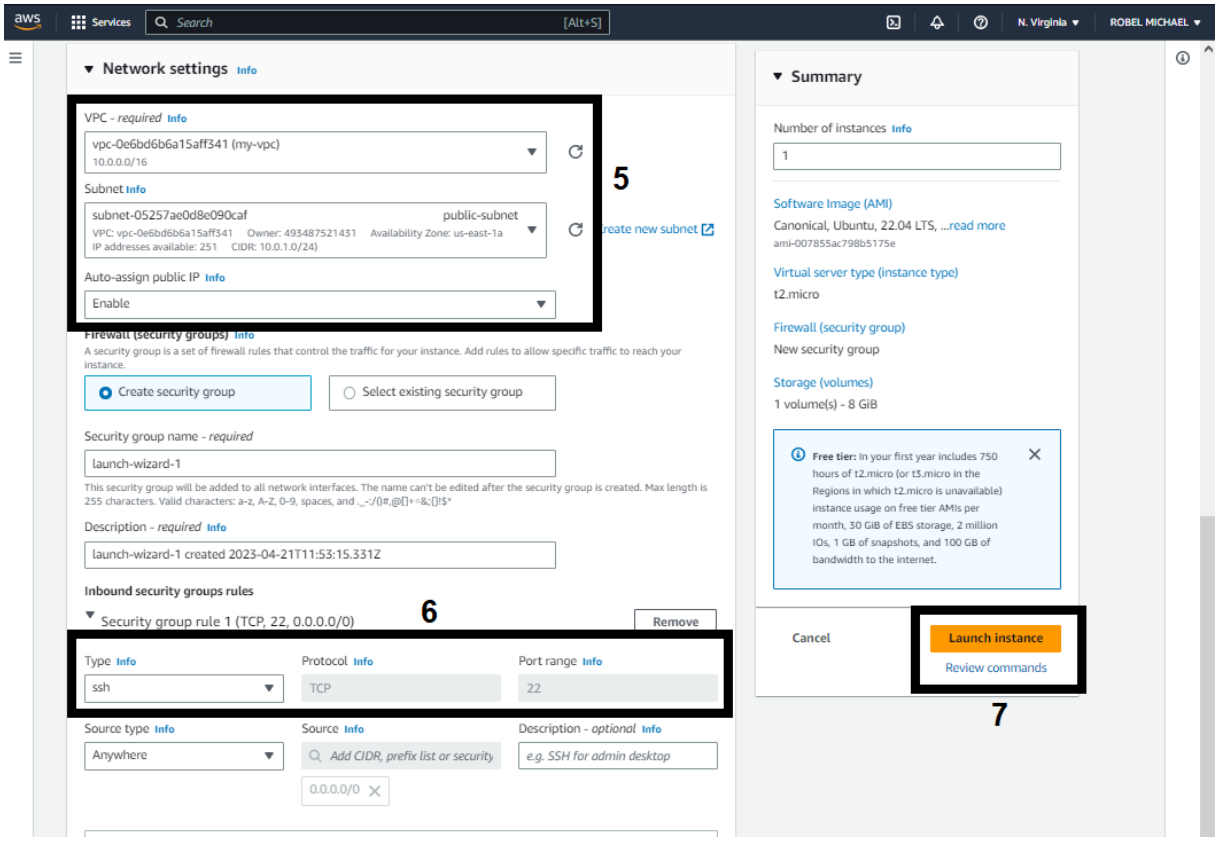


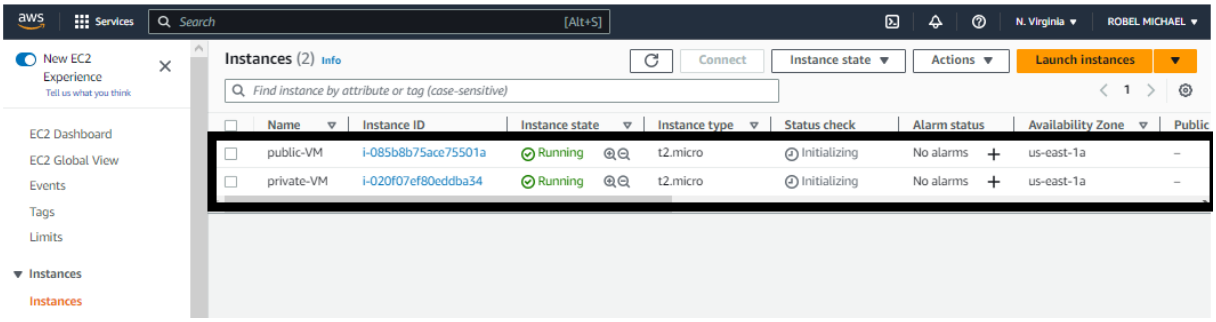


Part 2: AWS - Lab environment EC2 setup



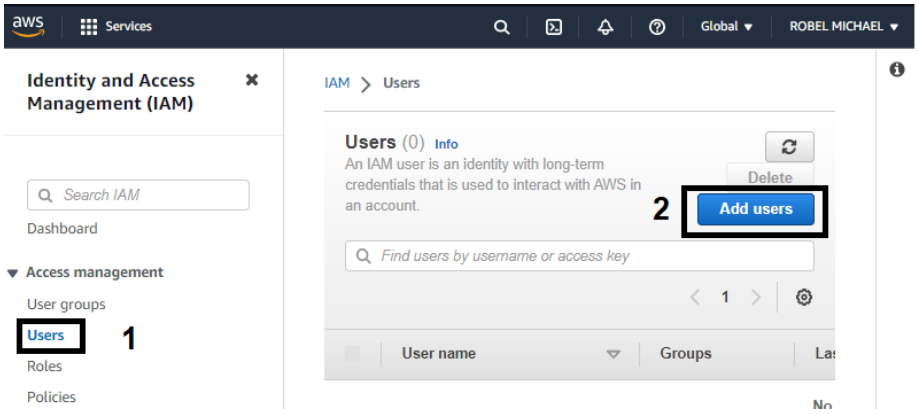


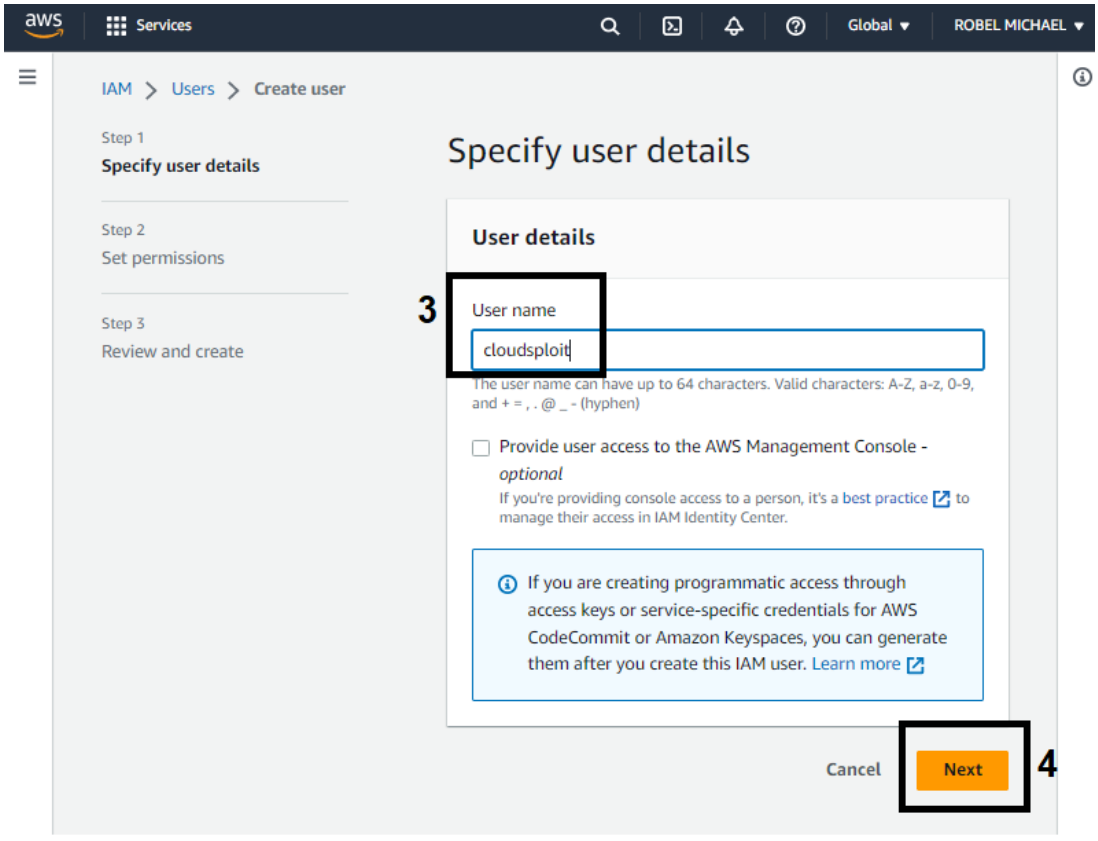

Services
Search
[Alt+S]
N. Virginia
ROBEL MICHAEL
Network settings Info
VPC - required Info
vpc-0e6bd6b6a15aff341 (my-vpc)
10.0.0.0/16
Subnet Info
subnet-05257ae0d8e090caf public-subnet
VPC: vpc-0e6bd6b6a15aff341 Owner: 493487521431 Availability Zone: us-east-1a
IP addresses available: 251 CIDR: 10.0.1.0/24)
Auto-assign public IP Info
Enable
5
Create new subnet
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
launch-wizard-1
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard-1 created 2023-04-21T11:53:15.331Z
Inbound security groups rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
6
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-007855ac798b5175e
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands
7

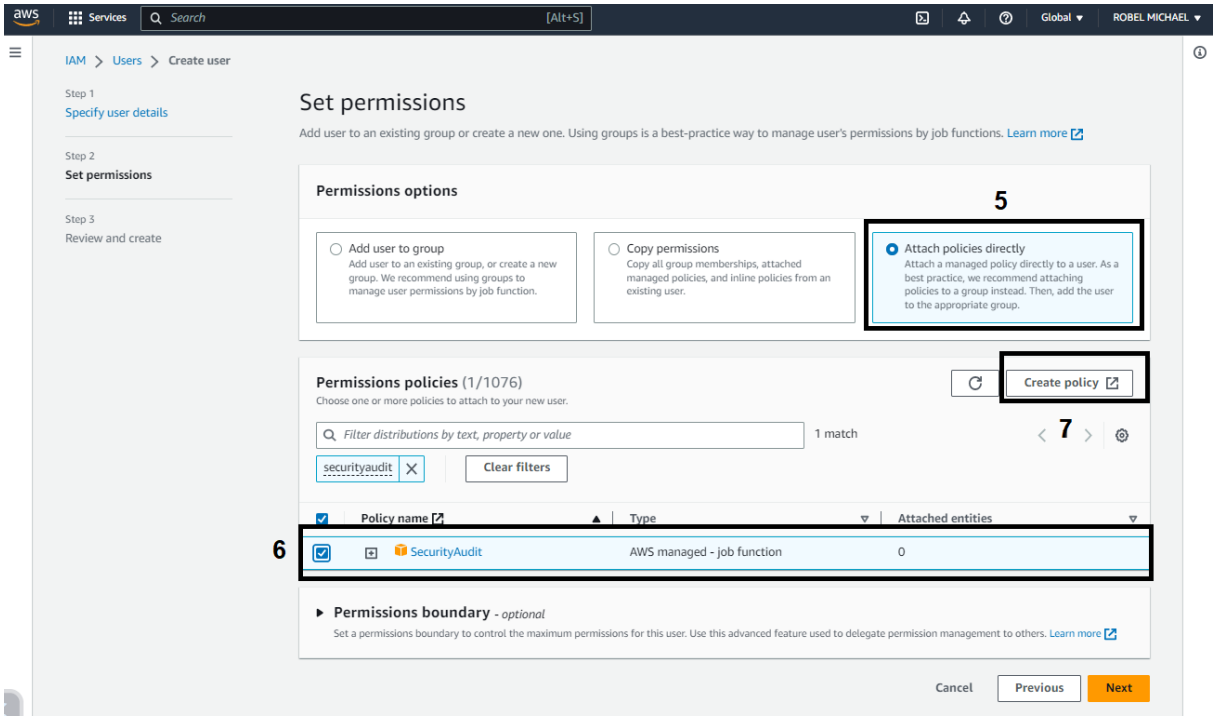

Services
Search
[Alt+S]
N. Virginia
ROBEL MICHAEL
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances
Instances (2) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public
public-VM
i-085b8b75ace75501a
Running
t2.micro
Initializing
No alarms
us-east-1a
private-VM
i-020f07ef80eddba34
Running
t2.micro
Initializing
No alarms
us-east-1a

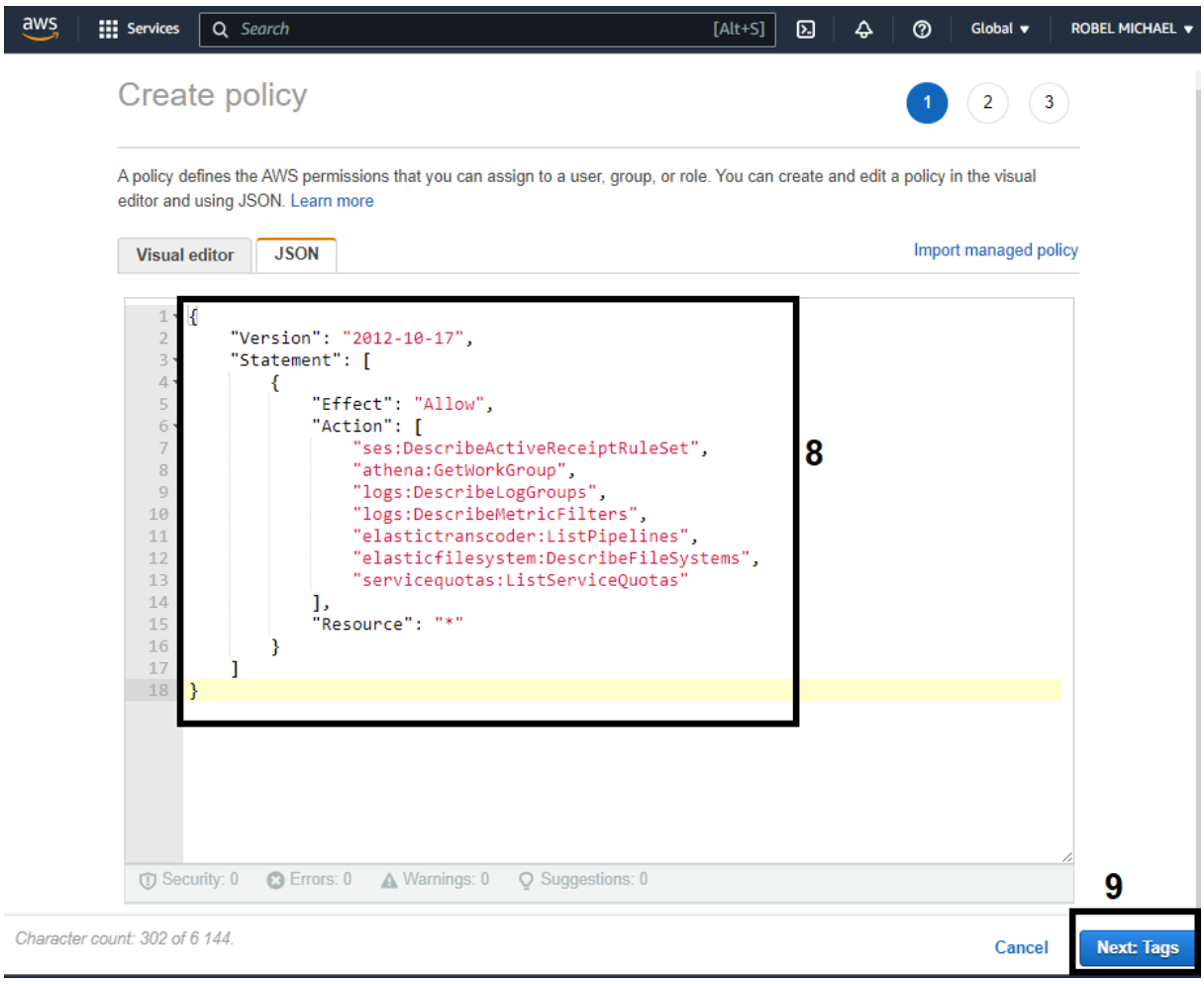
Part 3: CSPMSs setup

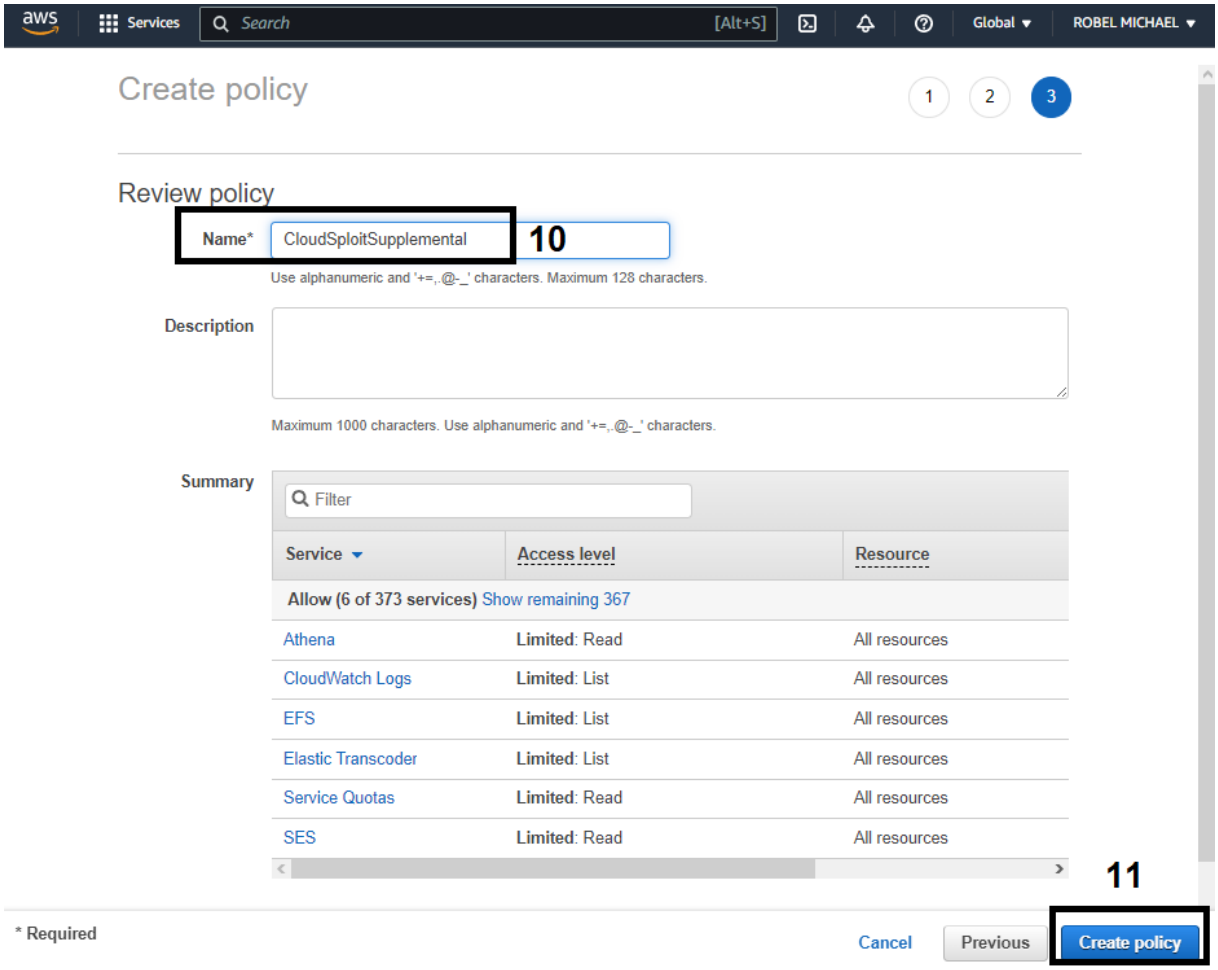
1. CloudSploit setup in AWS

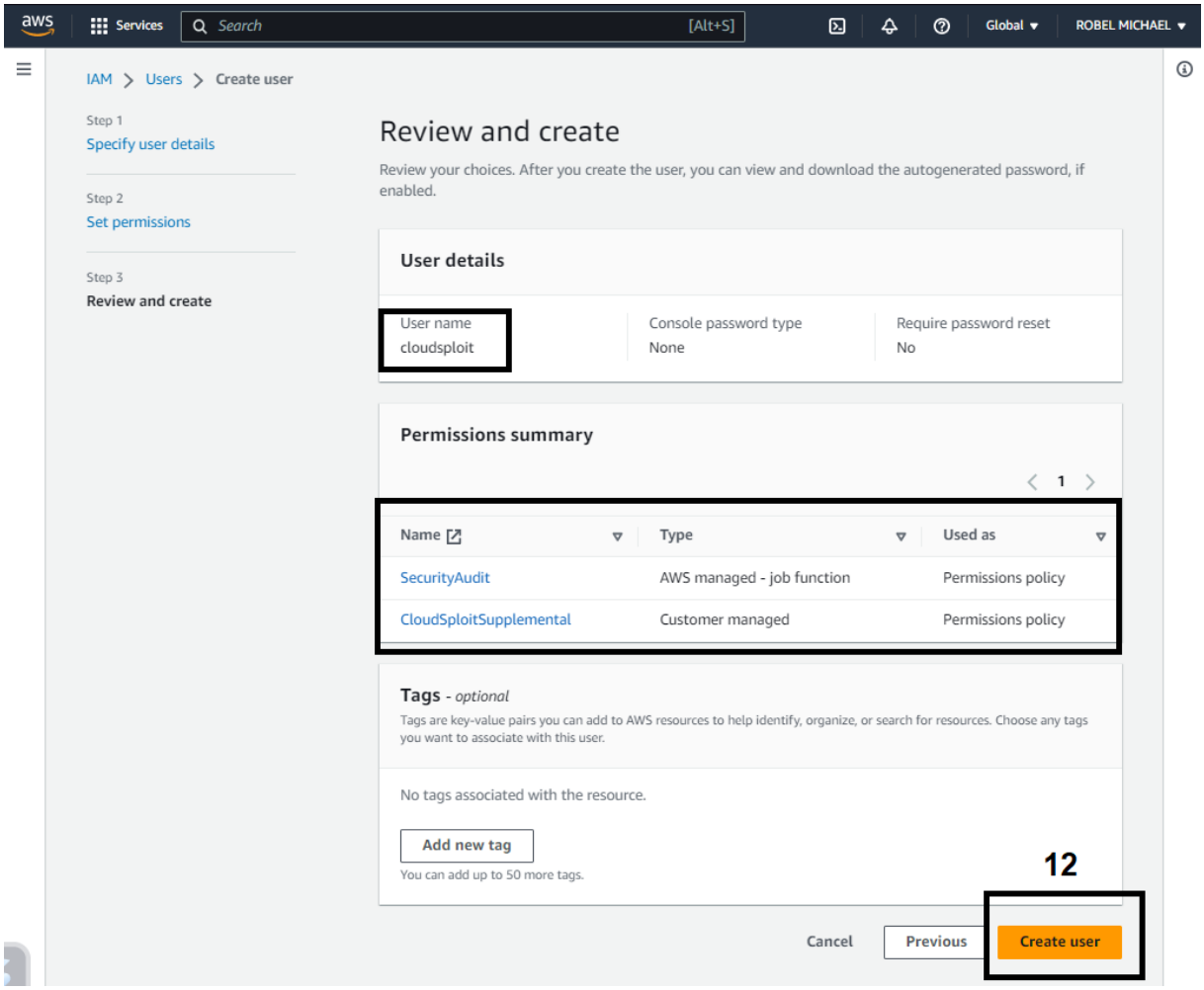




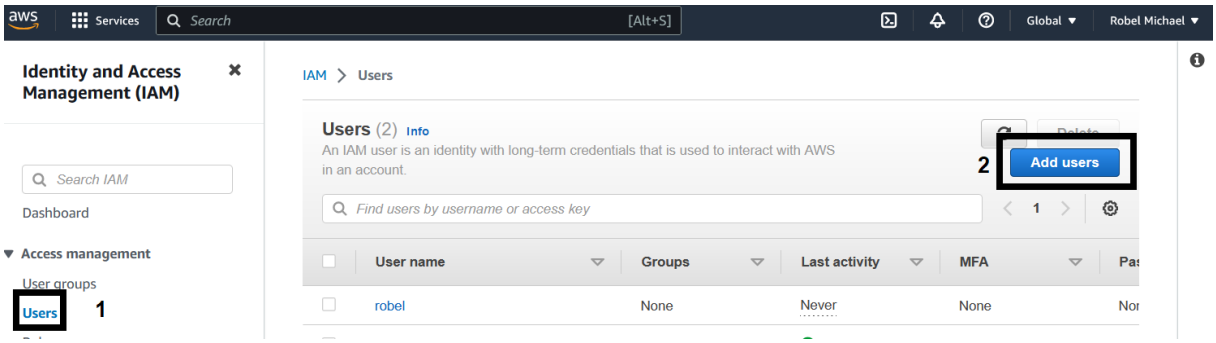

aws
Services
Search
[Alt+S]
Global
ROBEL MICHAEL
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
5
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Permissions policies (1/1076)
Choose one or more policies to attach to your new user.
Create policy
Filter distributions by text, property or value
1 match
7
securityaudit
Clear filters
Policy name
Type
Attached entities
6
SecurityAudit
AWS managed - job function
0
Permissions boundary - optional
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more
Cancel
Previous
Next

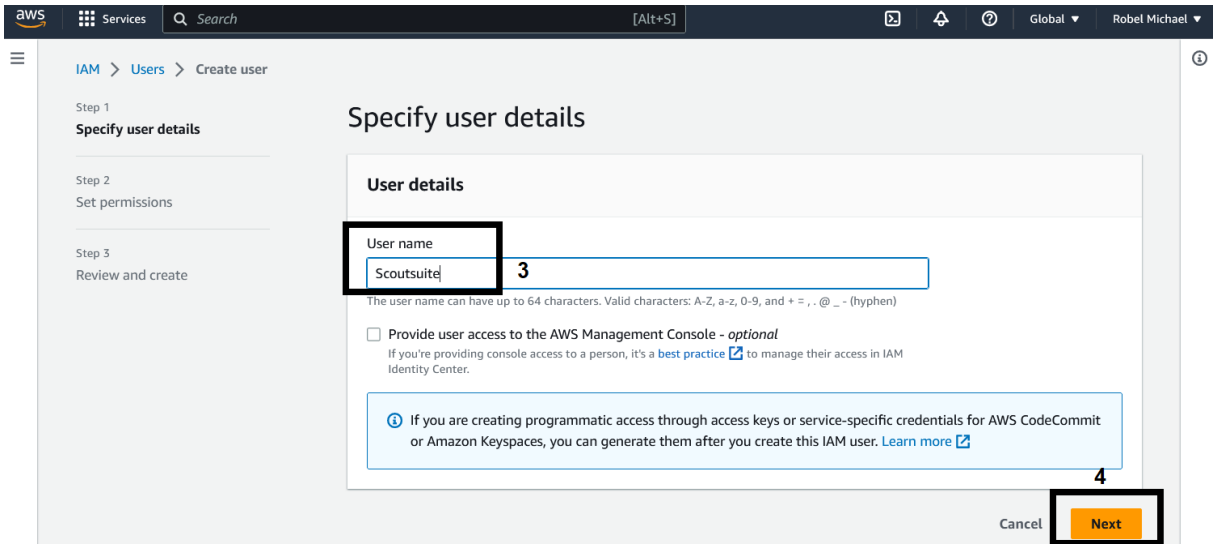

aws
Services
Search
[Alt+S]
Global
ROBEL MICHAEL
Create policy
1
2
3
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more
Visual editor
JSON
Import managed policy
8
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ses:DescribeActiveReceiptRuleSet",
"athena:GetWorkGroup",
"logs:DescribeLogGroups",
"logs:DescribeMetricFilters",
"elastictranscoder:ListPipelines",
"elasticfilesystem:DescribeFileSystems",
"servicequotas:ListServiceQuotas"
],
"Resource": "*"
}
]
}
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
9
Character count: 302 of 6 144.
Cancel
Next: Tags

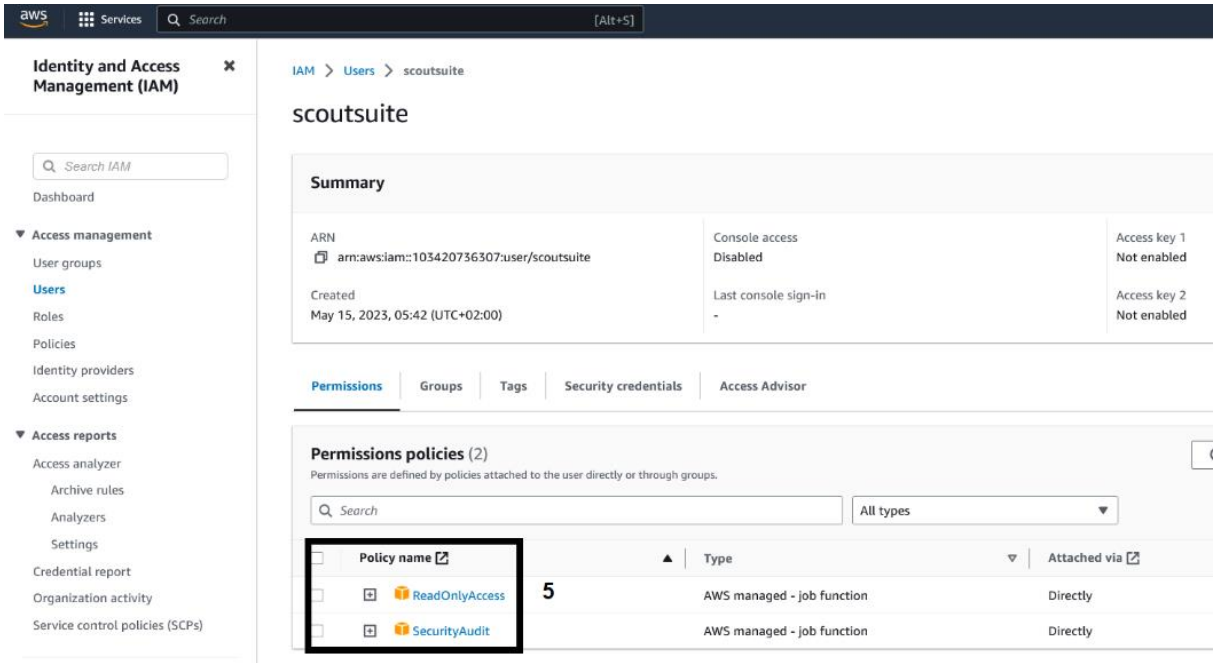

aws
Services
Search
[Alt+S]
Global
ROBEL MICHAEL
Create policy
1
2
3
Review policy
Name*
CloudSploitSupplemental
10
Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.
Description
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Summary
Filter
Service
Access level
Resource
Allow (6 of 373 services) Show remaining 367
Athena
Limited: Read
All resources
CloudWatch Logs
Limited: List
All resources
EFS
Limited: List
All resources
Elastic Transcoder
Limited: List
All resources
Service Quotas
Limited: Read
All resources
SES
Limited: Read
All resources
11
* Required
Cancel
Previous
Create policy


aws
Services
Search
[Alt+S]
Global
ROBEL MICHAEL
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
cloudsploit
Console password type
None
Require password reset
No
Permissions summary
1
Name
Type
Used as
SecurityAudit
AWS managed - job function
Permissions policy
CloudSploitSupplemental
Customer managed
Permissions policy
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
12
Cancel
Previous
Create user

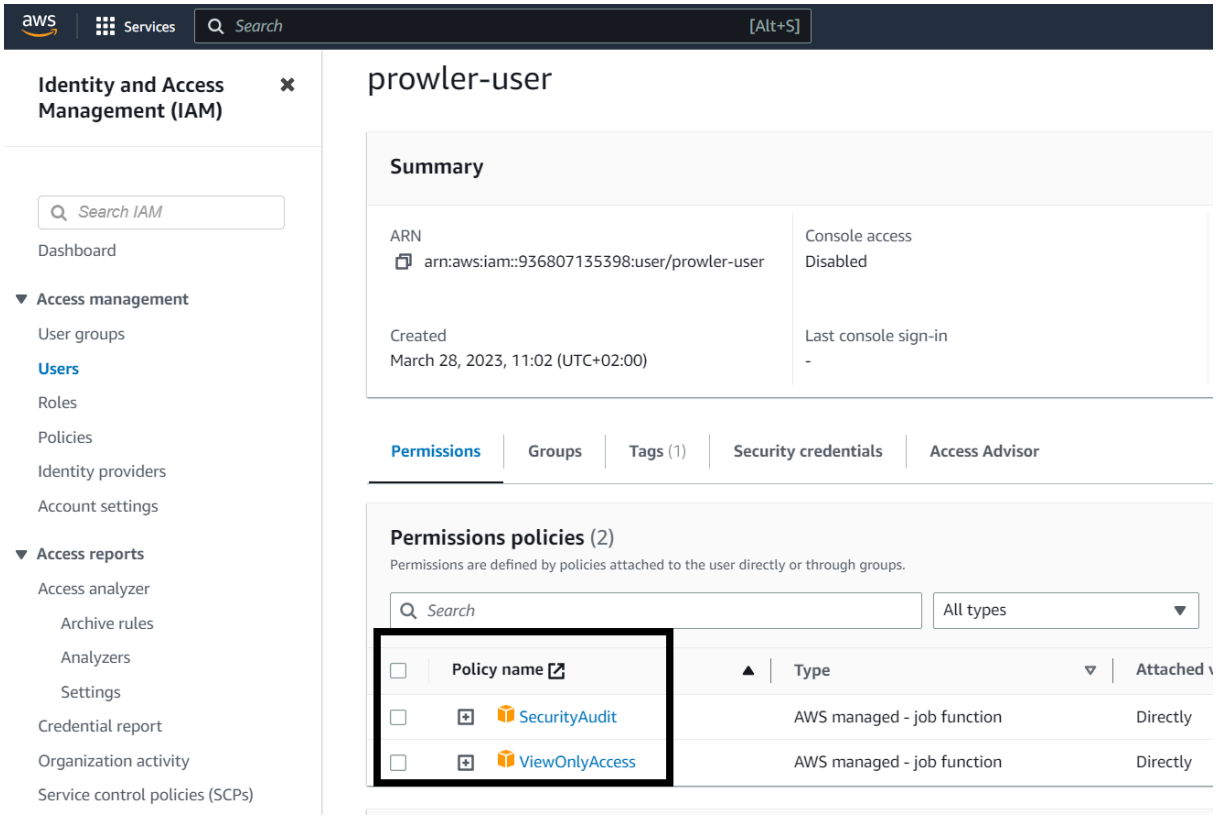
2. Scoutsuite in AWS







3. Prowler


aws
Services
Search
[Alt+S]
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
prowler-user
Summary
ARN
arn:aws:iam::936807135398:user/prowler-user
Console access
Disabled
Created
March 28, 2023, 11:02 (UTC+02:00)
Last console sign-in
-
Permissions
Groups
Tags (1)
Security credentials
Access Advisor
Permissions policies (2)
Permissions are defined by policies attached to the user directly or through groups.
Search
All types
Policy name
Type
Attached
SecurityAudit
AWS managed - job function
Directly
ViewOnlyAccess
AWS managed - job function
Directly