



AWS Certified Security Specialty Study Group

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



FAQ

- This will be recorded and sent out in about 24 hours to the email you registered with
- These slides will also be available for download
- You can ask questions at any time and we will answer throughout the presentation or at the end

AWS Certified Security Specialty Study Group

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Today's Session

- Introductions
- Session Events
- Who is this for? (And not for)
- About the exam
- Helpful free resources
- 2 Practice Exam Questions
- Wrapping up

CYBR

skyPurple Cloud
SECURE - OPTIMIZE - AUTOMATE

About Us





AWS Certified Security Specialty Study Group

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist





About Christophe Limpalair

- 📽️ Founder and Trainer at Cybr
- 👨‍💻 8+ years of AWS experience
- I've helped tens of thousands get AWS certified (anyone remember Linux Academy??)
- ⏮️ Background primarily in web dev and AWS cloud
- 🥾 I live in Colorado and love hiking & skiing

Cybr.com/discord

Christophe Limpalair
https://linkedin.com/in/christophelimpalair

@ChristopheLimp
https://twitter.com/christophelimp

CYBR

skyPurple Cloud
SECURE - OPTIMIZE - AUTOMATE

AWS Certified Security Specialty Study Group

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist





aws certified
Security
SPECIALTY

Cybr.com/discord

Christophe Limpalair
https://linkedin.com/in/christophelimpalair

@ChristopheLimp
https://twitter.com/christophelimp

CYBR

skyPurple Cloud
SECURE - OPTIMIZE - AUTOMATE

AWS Certified Security Specialty Study Group

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist





About Roy Long

- 🇬🇧 Founder @ skyPurple Cloud
- 👨‍💻 Over seven years in Cloud
- 30 years in HealthCare & Life Sciences
- Cloud Certified Security Professional (ISC2)
- AWS Solution Architect Professional
- Google Professional Cloud Architect
- Aviatrix Multi-Cloud Networking Professional (ACE)
- A keen surfer in the cold waters of the Atlantic!

Roy Long

https://www.linkedin.com/in/skypurplecloud/

CYBR

skyPurple Cloud
SECURE - OPTIMIZE - AUTOMATE

AWS Certified Security Specialty Study Group

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist





FinOps™ CERTIFIED Engineer

aviatrix ACE PROFESSIONAL

aviatrix ACE SECURITY SPECIALTY

aws certified Solutions Architect PROFESSIONAL

Cloud Architect
GOOGLE CLOUD CERTIFIED · PROFESSIONAL

ISC2 CCSP®

Roy Long

https://www.linkedin.com/in/skypurplecloud/

CYBR

skyPurple Cloud
SECURE - OPTIMIZE - AUTOMATE

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Sessions

- Each session will be 90 minutes long and there will be 4 total sessions
- Session 1: July 11th, 2024; at 9:00AM MT *<- we are here*
    - Intros & about the sessions and exams
    - Couple of practice exam questions
- Session 2: July 24th, 2024; at 9:00AM MT
    - Multiple practice exam questions
- Session 3: August 7th, 2024; at 9:00AM MT
    - Roy takes the exam and shares his experience
    - Practice exam questions
- Session 4: August 28th, 2024; at 9:00AM MT
    - Multiple practice exam questions
    - Review of the exam content

AWS Certified Security Specialty Study Group

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Who is this for?

Who should take this exam?

AWS Certified Security - Specialty is intended for experienced individuals who have five years of IT security experience in designing and implementing security solutions and two or more years of hands-on experience in securing AWS workloads. This certification complements the skills and expertise required for multiple job roles across cloud architecture, database, networking, and DevSecOps.

How will the AWS Certified Security - Specialty help my career?

This certification can build your credibility and position you as a trusted advisor to your stakeholders and customers. As an AWS Certified Security - Specialty certification holder, you can bring best practices and security solutions that meet organizations' and customers' unique needs. Job listings requiring this certification have increased 73% (Oct 2021 - Sept 2022) per Lightcast™ October 2022.

CYBR

skyPurple Cloud
SECURE - OPTIMIZE - AUTOMATE

AWS Certified Security Specialty Study Group

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Who is this for?

What certifications should I earn before taking this exam?

You are not required to earn any specific certifications prior to preparing for this certification. However, candidates commonly earn the AWS Certified Solutions Architect - Associate and/or AWS Certified Solutions Architect - Professional before attempting the AWS Certified Security - Specialty exam.

What AWS Certification(s) should I earn after attaining this certification?

The AWS Certified DevOps Engineer - Professional and the AWS Certified Advanced Networking - Specialty are additional certifications that other cloud professionals have earned to advance further in roles like Networking Engineer or DevSecOps Engineer.

CYBR

skyPurple Cloud
SECURE - OPTIMIZE - AUTOMATE

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



About the Exam

- This exam has 6 domains with different weights:
  - Domain 1: Threat Detection and Incident Response (14% of scored content)
  - Domain 2: Security Logging and Monitoring (18% of scored content)
  - Domain 3: Infrastructure Security (20% of scored content)
  - Domain 4: Identity and Access Management (16% of scored content)
  - Domain 5: Data Protection (18% of scored content)
  - Domain 6: Management and Security Governance (14% of scored content)

Christophe Limpalair
Founder & Trainer
at Cybr

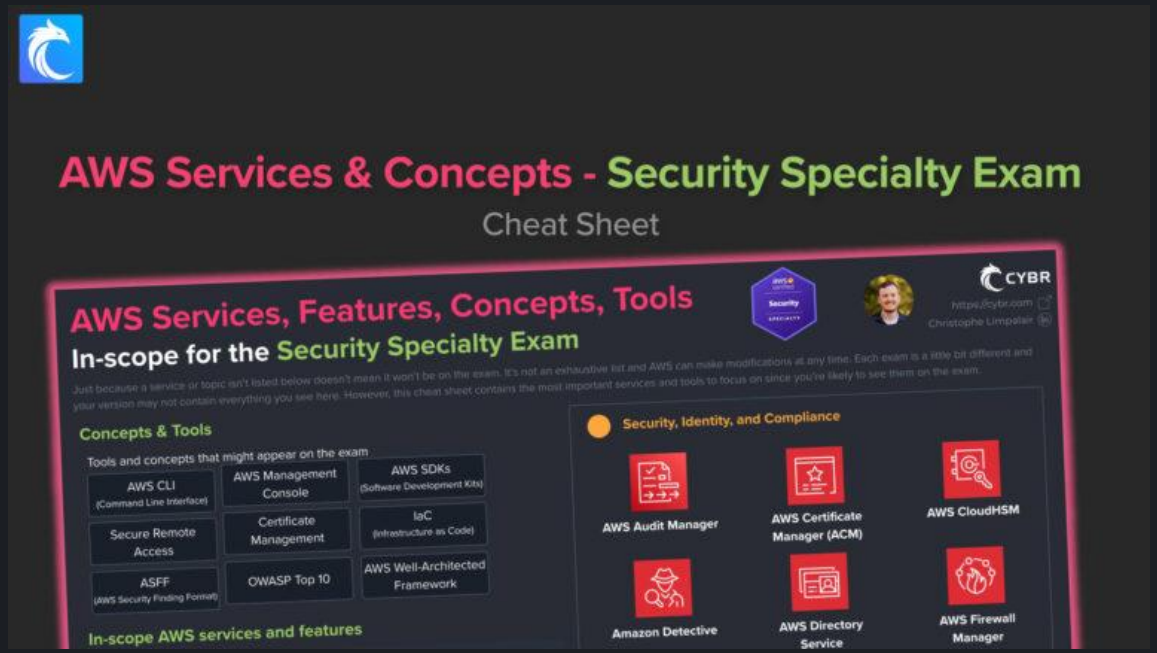


Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Services Covered

Cheat Sheet: https://cybr.com/security-specialty-services-cheatsheet *(not a comprehensive list)*



CYBR

skyPurple Cloud
SECURE - OPTIMIZE - AUTOMATE

Christophe Limpalair
Founder & Trainer
at Cybr

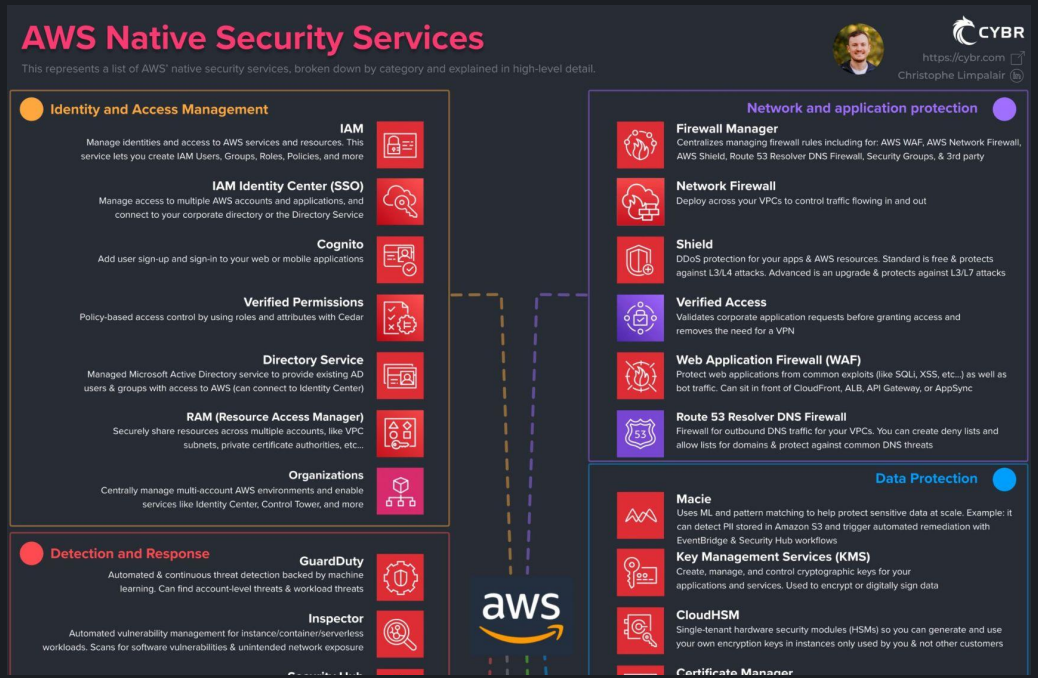


Roy Long
Found, skyPurple Cloud
Cloud Evangelist



AWS-Native Security Services

Cheat Sheet: https://cybr.com/aws-security-services-cheatsheet



CYBR

skyPurple Cloud
SECURE - OPTIMIZE - AUTOMATE

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Helpful Free Resources

- Cybr's free certification prep course (WIP): https://cybr.com/courses/aws-certified-security-specialty-scs-c02-course/
- Cybr's AWS Security Cheat Sheets: https://cybr.com/tag/aws-security-cheat-sheets/
- Cybr's Discord: https://cybr.com/discord
- Official exam guide: https://d1.awsstatic.com/training-and-certification/docs-security-spec/AWS-Certified-Security-Specialty_Exam-Guide.pdf
- Official practice exam questions: https://explore.skillbuilder.aws/learn/course/external/view/elearning/15222/aws-certified-security-specialty-official-practice-question-set-scs-c02-english
- AWS Security Fundamentals course: https://explore.skillbuilder.aws/learn/course/external/view/elearning/48/aws-security-fundamentals-second-edition

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Helpful Free Resources

- Cloud Quest: https://explore.skillbuilder.aws/learn/course/external/view/elearning/7636/cloud-quest
- Security Engineering on AWS: https://aws.amazon.com/training/classroom/security-engineering-on-aws/
- Official AWS exam prep course: https://explore.skillbuilder.aws/learn/course/external/view/elearning/18291/exam-prep-standard-course-aws-certified-security-specialty-scs-c02-english
- Official practice exam questions: https://explore.skillbuilder.aws/learn/course/external/view/elearning/15719/aws-certified-security-specialty-official-practice-exam-scs-c02-english
- Official practice exam question set: https://explore.skillbuilder.aws/learn/course/external/view/elearning/15222/aws-certified-security-specialty-official-practice-question-set-scs-c02-english

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Practice Exam Questions

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Question #1:

You've identified a potential compromise on one of your EC2 instances serving as a Bastion Host, located in its own subnet within a VPC.

Which of these steps is best to restrict access and prevent further compromise while allowing your security team to investigate?

A. Modify the security group rule to block all access except to an internal IP address used by the security team
B. Modify the NACL to block all access except to an internal IP address used by the security team
C. Stop the Bastion Host instance to prevent any more compromise. Take a snapshot of the instance, and then transfer the snapshot to the dedicated digital forensics AWS account
D. Change the IAM roles associated with the Bastion Host instance to restrict access based on the security team's role permissions.

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Answer #1:

B. Modify the NACL to block all access except to an internal IP address used by the security team

Explanation:

In this scenario, you would want to block at the NACL level (subnet level) since you've confirmed that the bastion host is the only resource running in the subnet. Also, security groups are stateful and some connections can remain temporarily alive even after blocking them if they were already established. Since NACLs are stateless, changing rules will immediately block access and are preferred whenever you can block access to entire subnets (which is not always possible).

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Question #2:

After receiving an alert from GuardDuty threat detection regarding a potential threat involving an S3 bucket, you investigate using CloudTrail Lake. While reviewing the logs, you observe suspicious activity related to bucket operations but find no events indicating whether any objects have been accessed or modified. What is the MOST likely reason?

A. No data was likely downloaded or modified by the threat actor
B. CloudTrail trail was not configured to capture data events
C. CloudTrail Lake was not configured to capture data events
D. CloudTrail was properly configured, but did not have the right permissions through its service-linked role to access S3 events
E. Athena was not properly configured when it was initially set up

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



Answer #2:

C. CloudTrail Lake was not configured to capture data events

Explanation:

Lake uses separate data stores than regular CloudTrail trail data, which you set up when configuring Lake. Since the question specifically says that you are investigating using Lake, it would likely mean that the Lake data store was not configured to log data events, which is what you need to log in order to view object-level S3 events, also referred to as data plane operations. By default, only management events are enabled but these will only capture management operations (aka bucket-level operations or control plane operations)

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



🚀 About skyPurple Cloud

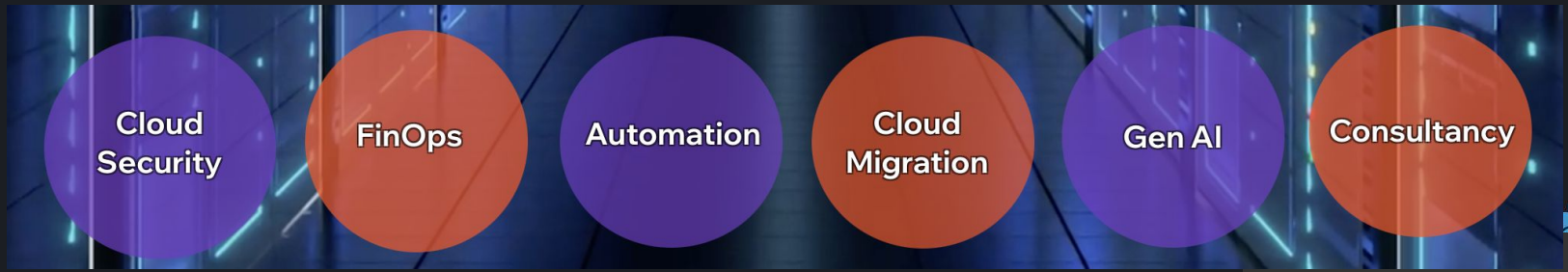
UK-based cloud services company (skyPurple Cloud) with Global customers.

Relatively new start-up - cloud ML, cost optimisation & security services.

Provide strategic cloud security & solution advice to Board & Leadership level.

Multiple AI/ML solution design and deployments completed.

Orca Security Partner, providing licenses & managed services for Orca (CSPM).



AWS Certified Security Specialty Study Group

Christophe Limpalair
Founder & Trainer
at Cybr



Roy Long
Found, skyPurple Cloud
Cloud Evangelist



🔒 About Cybr.com

Learn AWS cloud security hands-on

Access training Courses, 🧪 Hands-On Labs,
and Ebooks on AWS Cloud Security



Thank you for attending!
Any questions?



Christophe Limpalair
https://linkedin.com/in/christophelimpalair

Roy Long
Founder & Cloud Evangelist

LIVE

Upcoming webinars
https://cybr.com/webinars