
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC218

Introducing Amazon GuardDuty RDS Protection

Amit Megiddo

Principal Product Manager, GuardDuty

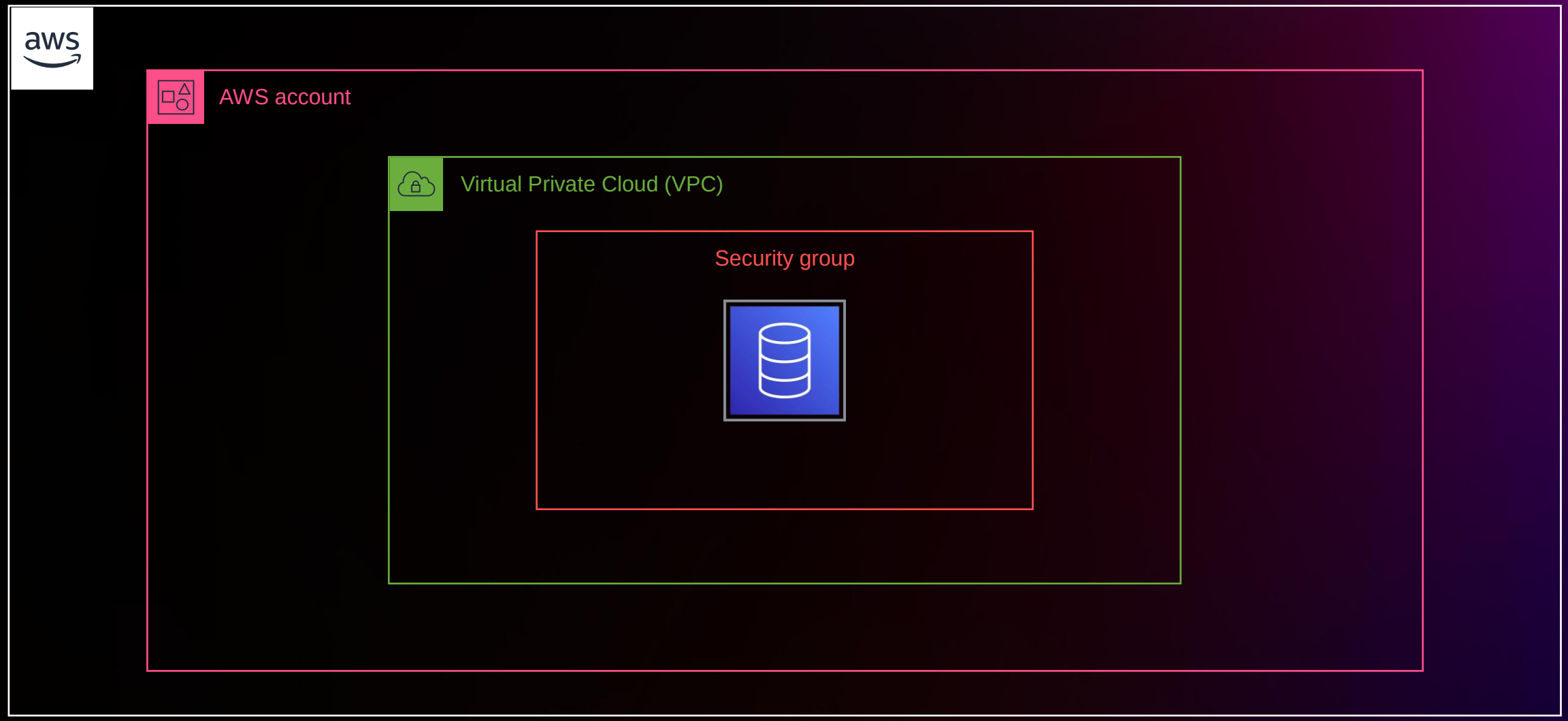
Jeremiah Wilton

Senior Principal Technologist, AWS Databases

aws

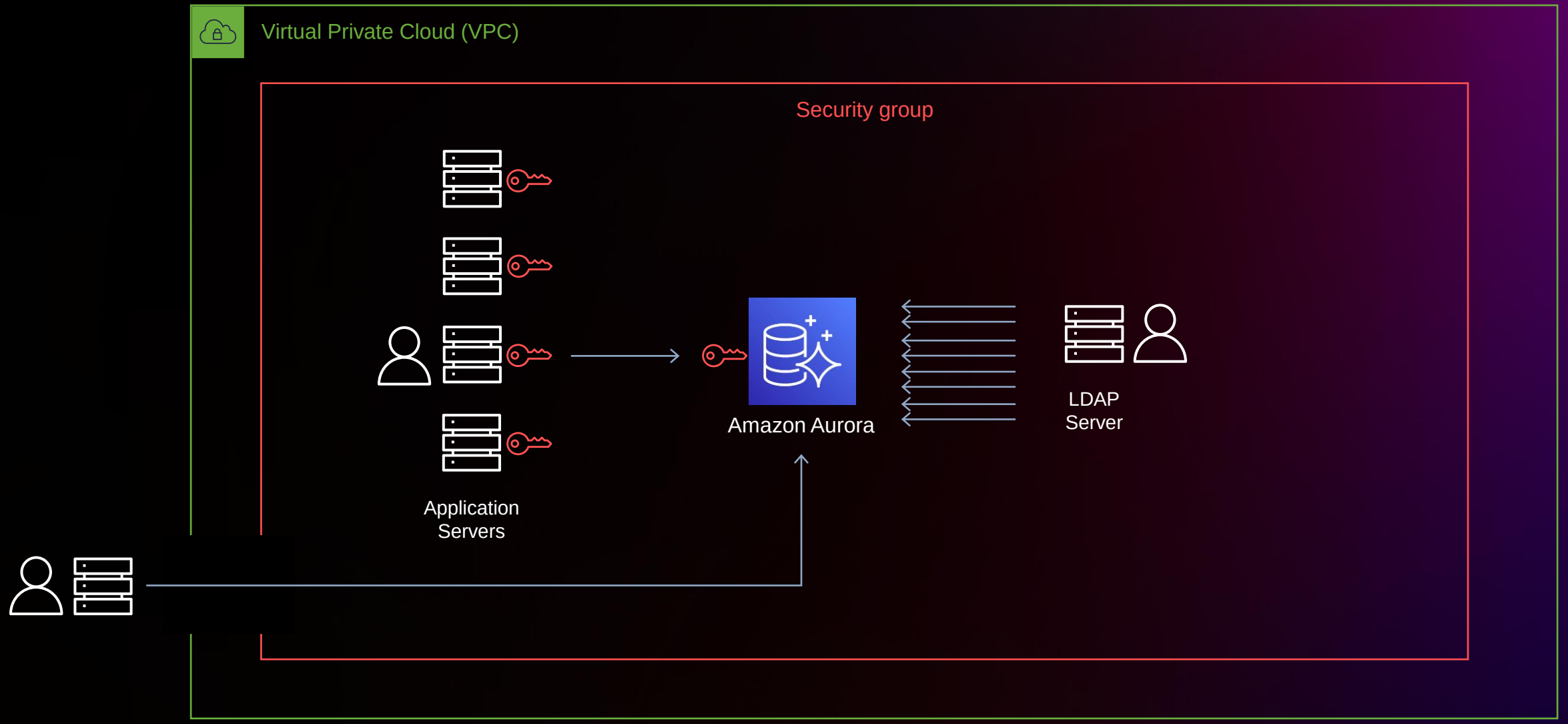
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

For databases, security is the highest priority



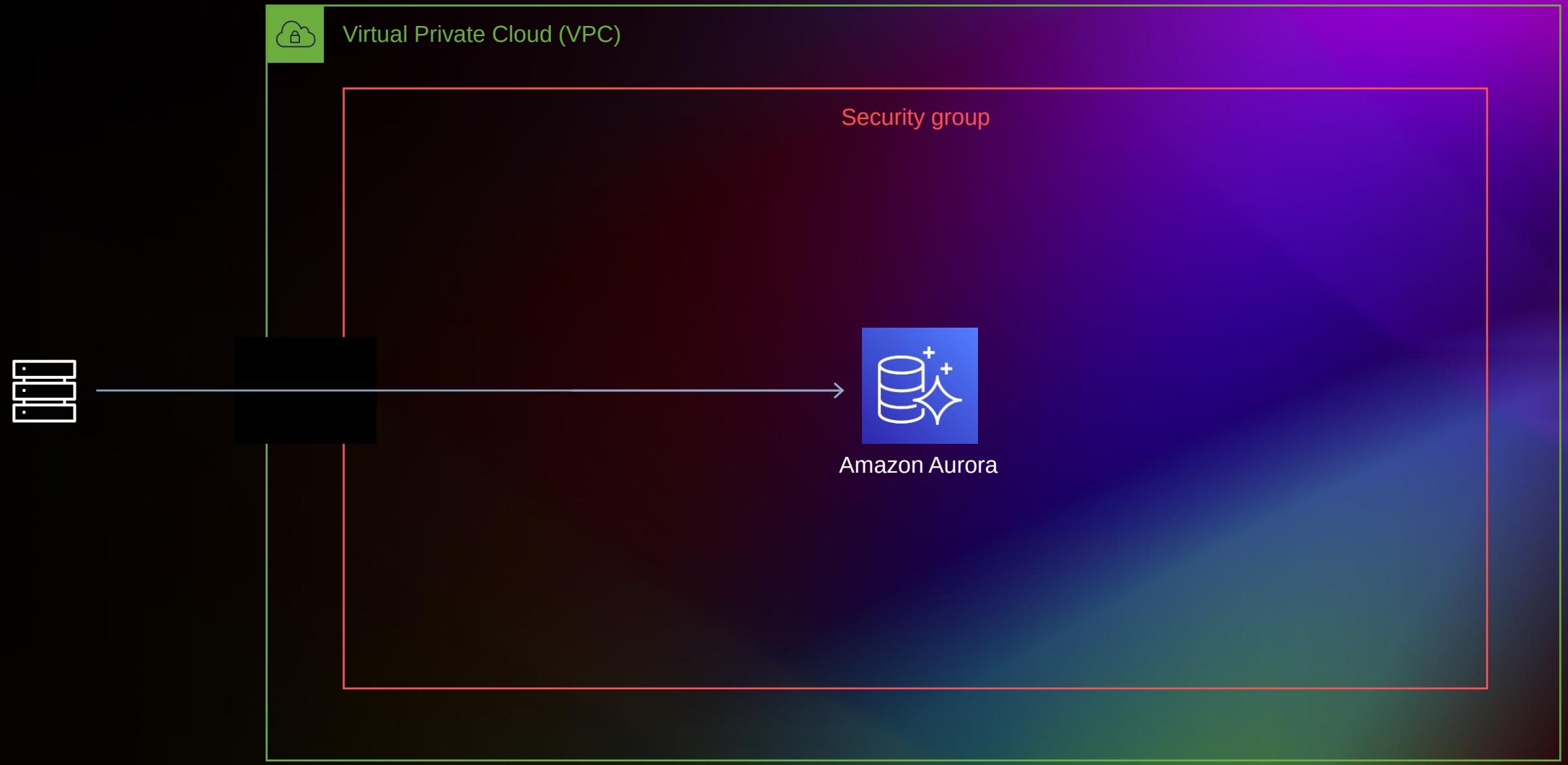
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Databases call for security specialization



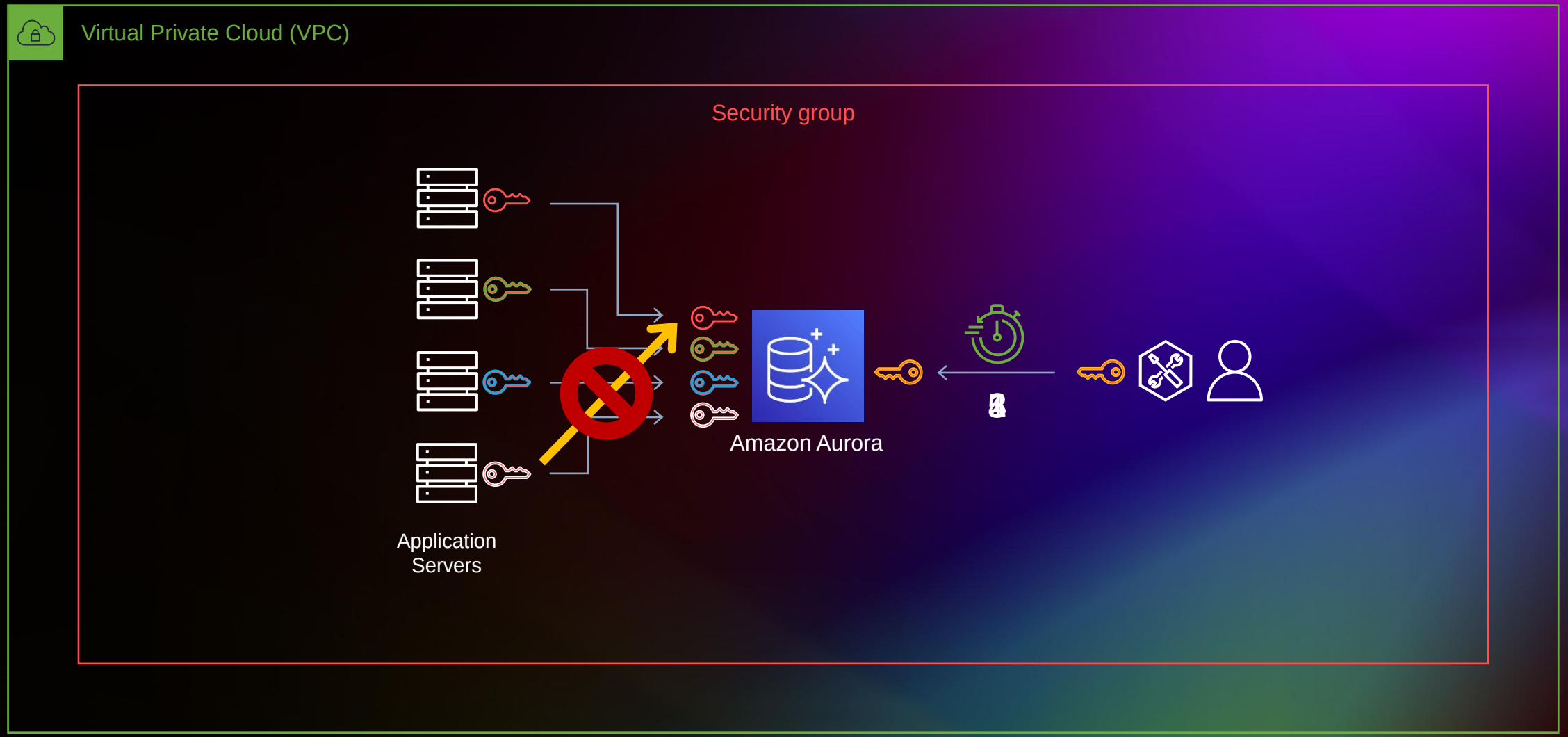
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What can you do to protect an AWS database?



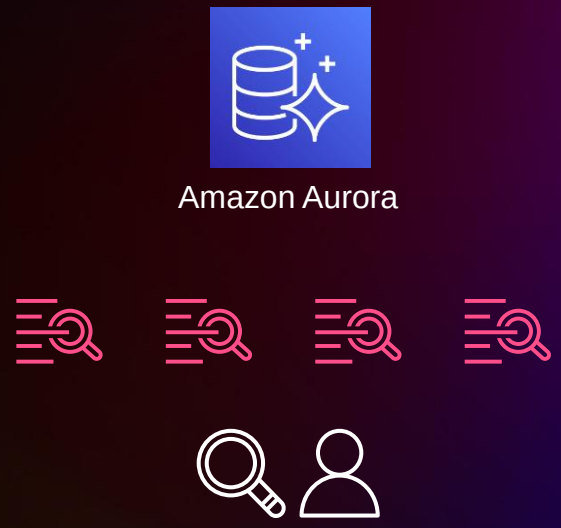
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What else can you do to protect an AWS database?



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

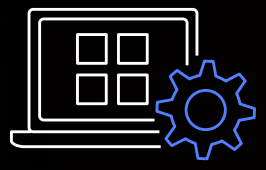
What else can you do to protect an AWS database?



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon GuardDuty

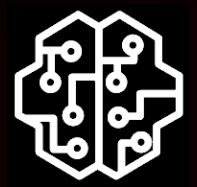
Protect your AWS accounts, workloads, and data with intelligent threat detection and continuous monitoring



Single-click organization-wide activation



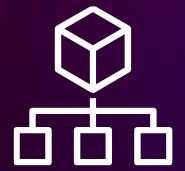
Continuous monitoring of AWS accounts and resources



ML to detect evasive attack techniques



Threat intelligence from AWS and leading third-parties



Enterprise-wide consolidation & management

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon GuardDuty: How does it work?



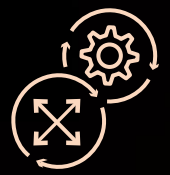
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Relational Database Service (Amazon RDS)

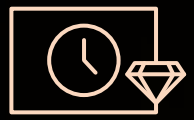
Set up, operate, and scale a relational database in the cloud with just a few clicks



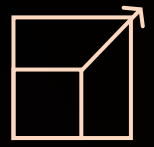
12+ years of operational expertise, security best practices, and innovation



Remove inefficient administrative tasks with managed databases



High availability and durability with Amazon RDS Multi-AZ



Build and scale with the database of your choice



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

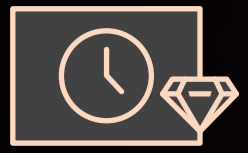
Amazon Aurora

Designed for unparalleled high performance and availability at global scale with full MySQL and PostgreSQL compatibility at 1/10th the cost of commercial databases



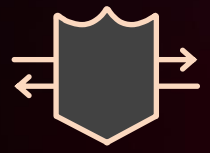
Performance & scalability

- *5x throughput of standard MySQL and 3x of standard PostgreSQL*
- *Scale out up to 15 read replicas*
- *Decoupled storage and compute enabling cost optimization*
- *Fast database cloning*
- *Distributed, dynamically scaling storage subsystem*



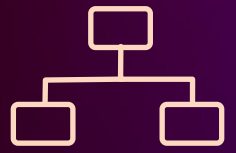
Availability & durability

- *6 copies of data across 3 AZs (customers pays for 1)*
- *Automatic, continuous, incremental backups with point-in-time recovery (PITR)*
- *Fault-tolerant, self-healing, auto-scaling storage*
- *Global Database for disaster recovery*



Highly secure

- *Network isolation*
- *Encryption at rest/in transit*
- *Supports multiple secure authentication mechanisms and audit controls*



Fully managed

- *Automates time-consuming management of administration tasks like hardware provisioning, database setup, patching, and backups*
- *Serverless configuration options*

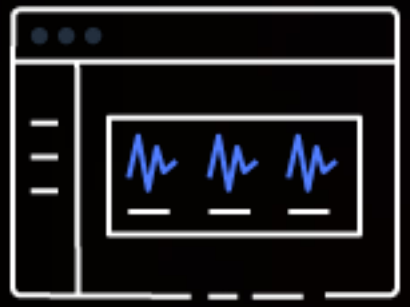
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Toward a more automated database







Amazon RDS
Performance Insights

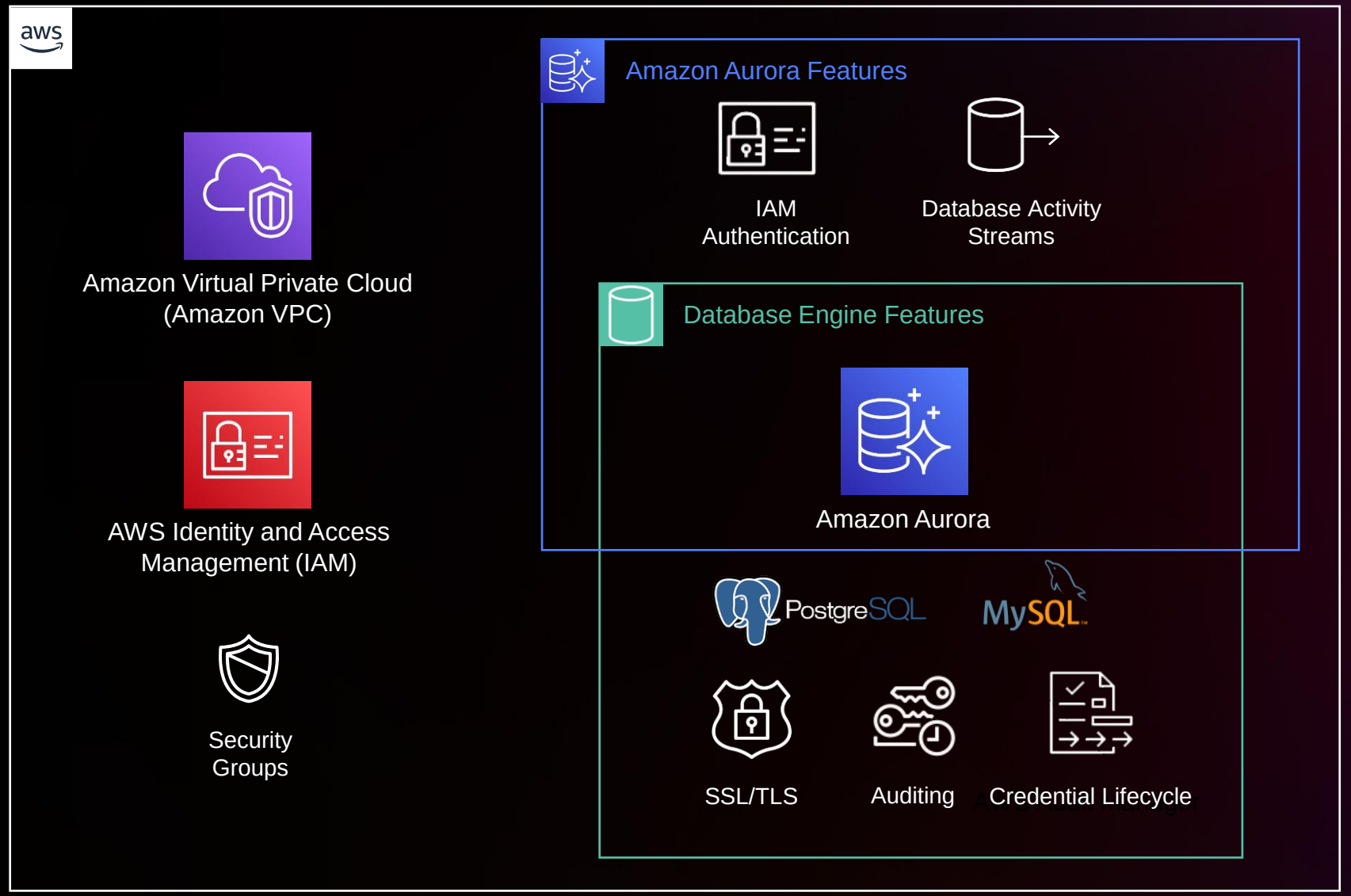


DevOps Guru for RDS

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

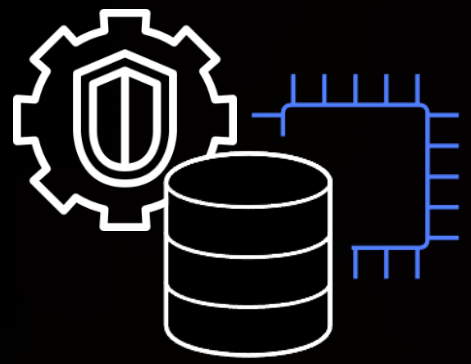
Aurora security features





aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing Amazon GuardDuty RDS Protection



Protect your data stored in Amazon RDS databases (starting with Amazon Aurora) by identifying suspicious login attempts to mitigate threats before they escalate

Continuously monitor all Aurora databases across your organization with a single click

Machine learning helps reduce noise and avoid alert fatigue

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

An Expansion of GuardDuty

Data Sources

- VPC flow logs
- DNS logs
- Amazon Aurora Login events
- CloudTrail events
- S3 data plane events
- EKS audit logs

Security Analytics

Machine Learning

Threat Intelligence

Continuous learning

Incorporating new machine learning techniques that model RDS login activity to accurately detect suspicious logins to RDS databases

Security Findings

Actionable

Accurate

Contextual

Security findings are enriched with contextual data, so you can quickly answer questions such as, what database was accessed? Where was it accessed from? Has this user previously accessed the database?

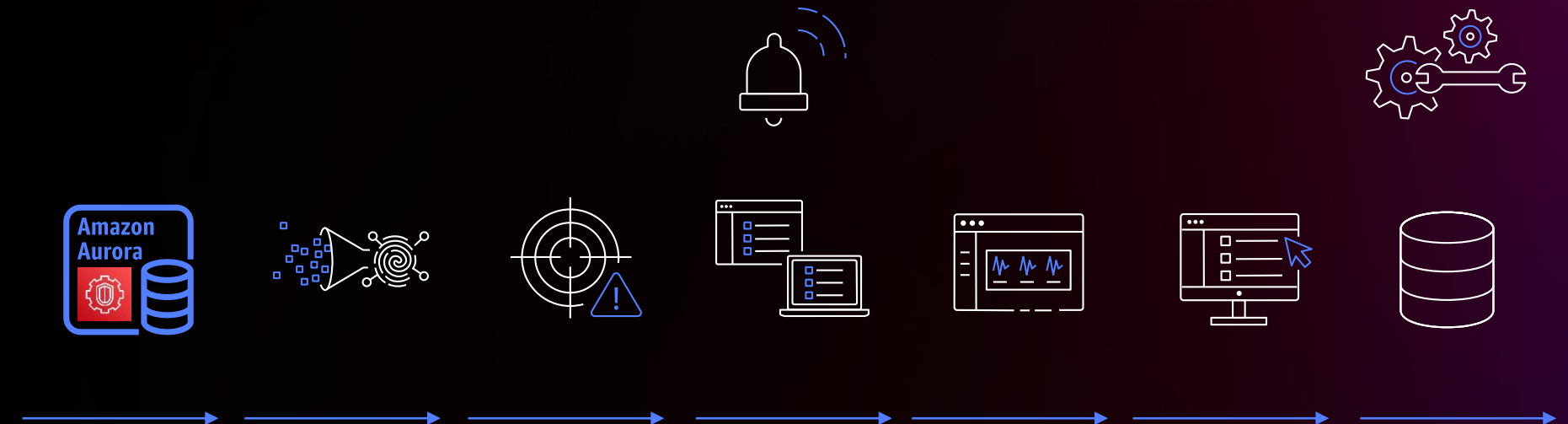
Integration

- Amazon Detective
- AWS Security Hub
- Amazon EventBridge
- AWS Partner Network

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon GuardDuty RDS Protection: How does it work?



Aurora + GuardDuty RDS Protection

Metrics ingestion

Detect suspicious activity

GuardDuty

Amazon GuardDuty RDS Protection

Explain + understand

Remediate

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon GuardDuty RDS Protection: Anomaly detection deep dive





Detects suspicious activity

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon GuardDuty RDS Protection: Anomaly detection deep dive

```
2022-11-12 20:23:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=17gf9qmuSrqNk9lwJbj59A==)(PORT=43092) 0
2022-11-12 20:24:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=iqwe+vH+QvWaPhfFSuOEyw==)(PORT=43122) 0
2022-11-12 20:25:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=P7hL98RcSKy9yYpdxu2EPA==)(PORT=43132) 0
2022-11-12 20:26:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=qiTInLFVRJScftfATN3aTQ==)(PORT=43162) 0
2022-11-12 20:27:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=PsIQU1xEQIKwARZ6cN4d3A==)(PORT=43176) 0
2022-11-12 20:28:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=0jM1ujVYQI+GHjghJyg1aA==)(PORT=43188) 0
2022-11-12 20:29:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=xBSMY67DQHKw7+KpqohQng==)(PORT=43202) 0
2022-11-12 20:30:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=Afw1FnnHT26/lJr6uuBqrQ==)(PORT=43212) 0
2022-11-12 20:31:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=S71Pw6H4QU+gGfkYnAPyxA==)(PORT=43232) 0
2022-11-12 20:32:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=BkNoMTouS6SSkwg0U1Mucg==)(PORT=43244) 0
2022-11-12 20:33:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=QwGWIv1ESleOUU8i40CBHg==)(PORT=43260) 0
2022-11-12 20:34:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=8pY+2FnpQ66UQLNDdwAY5Q==)(PORT=43270) 0
2022-11-12 20:35:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=X1pbOkc0QRuImfda6rJk8w==)(PORT=43282) 0
2022-11-12 20:36:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=PtHMIDi5S5W2yTtsaJ7kiw==)(PORT=43300) 0
2022-11-12 20:37:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=StNmg+NNQ8u2z4Nm8ifeSA==)(PORT=43312) 0
2022-11-12 20:38:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=2BtvfsZuRt6UTOMzwW0JIQ==)(PORT=43324) 0
2022-11-12 20:39:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=f6SPJbz3TEuX5lR/2HRi0w==)(PORT=43340) 0
2022-11-12 20:40:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=bVOVh0WwQWiuwPWuQYWY2g==)(PORT=43350) 0
2022-11-12 20:40:19 * (connection=(applicationName=psql)(clientHost =159.28.1.1)(USER=system)(database=postgres)(ssl=none)(connID=bVOVh0WwQWiuwPWuQYWY2g==)(PORT=43355) 1017
2022-11-12 20:41:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=1eqytReKQ++srXW1ycx67g==)(PORT=43368) 0
2022-11-12 20:42:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=b5JilvsQREagGiVwMBggHA==)(PORT=43380) 0
2022-11-12 20:43:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=NUI7I07mRUyjZDYvOz5w6Q==)(PORT=43396) 0
2022-11-12 20:44:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=urqmj5BRT7+8Z8D3WuGdwg==)(PORT=43408) 0
2022-11-12 20:45:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=hxosrlalQPOpsWYyj14hgw==)(PORT=43418) 0
2022-11-12 20:46:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=U1SUcHXUTgeYxWT5DG0Rpg==)(PORT=43438) 0
2022-11-12 20:47:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=PH2rzJ7GQHedVIZdrUIcOA==)(PORT=43452) 0
2022-11-12 20:48:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=KWHUPJ9WTRyVtmyzA0ZGTQ==)(PORT=43464) 0
2022-11-12 20:49:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=TYldR9n1SguUY/KvPNAzIA==)(PORT=43478) 0
2022-11-12 20:50:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=BMQunSFmSvGyLfua08JJVw==)(PORT=43490) 0
2022-11-12 20:51:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=ixEkQK9HRwqJab1yaIF0vg==)(PORT=43508) 0
2022-11-12 20:52:00 * (connection=(applicationName=PostgreSQL JDBC Driver)(clientHost=192.168.10.31)(user=glappusr01a)(database=gldbna01)(ssl=TLSv1.2)(connID=eBYgWafARyupz4P+pgShaA==)(PORT=43520) 0
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

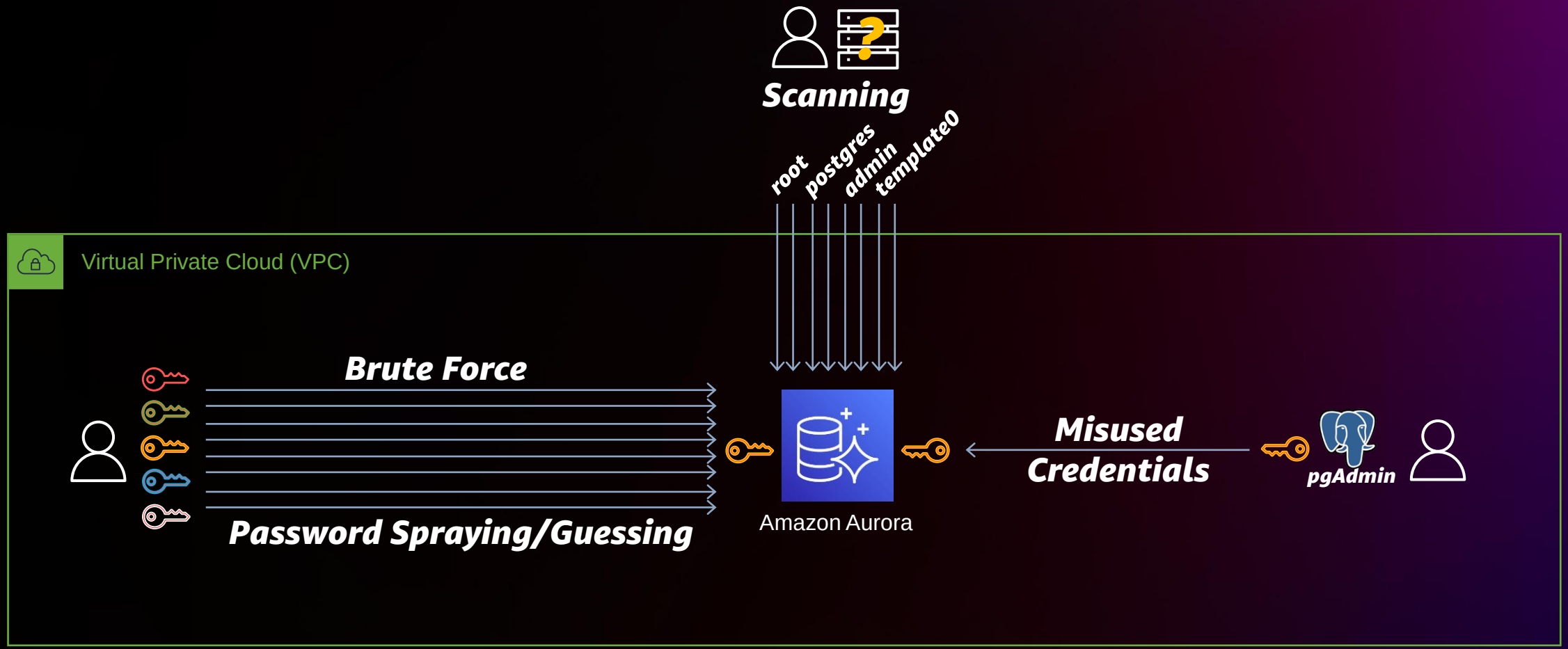
Amazon GuardDuty RDS Protection: Anomaly detection deep dive

Date	Time	Program	Client IP Addr	User	DB	Encryption	Status
2022-11-12	20:23:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:24:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:25:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:26:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:27:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:28:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:29:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:30:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:31:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:32:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:33:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:34:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:35:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:36:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:37:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:38:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:39:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:40:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:40:19	psql	159.28.1.1	postgres	postgres	none	28P01
2022-11-12	20:41:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:42:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:43:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:44:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:45:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:46:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:47:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:48:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:49:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:50:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:51:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0
2022-11-12	20:52:00	PostgreSQL JDBC Driver	192.168.10.31	glappusr01a	gldbna01	TLSv1.2	0

aws

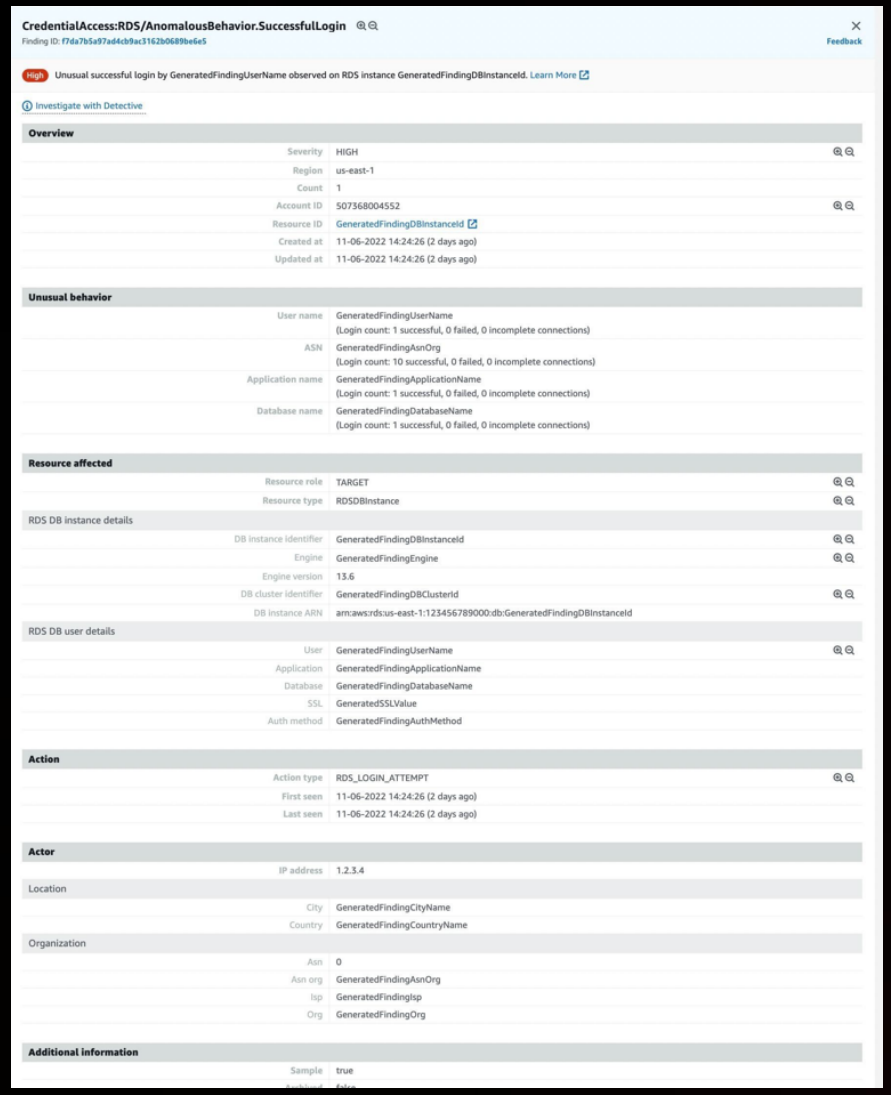
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What GuardDuty RDS Protection can detect



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Context to quickly investigate and respond



Finding name indicates whether the anomalous behavior was a successful or failed login

Unusual behavior section allows you to quickly see what suspicious behavior triggered the alert, including user, database, and application names, and the ASN the database was accessed from

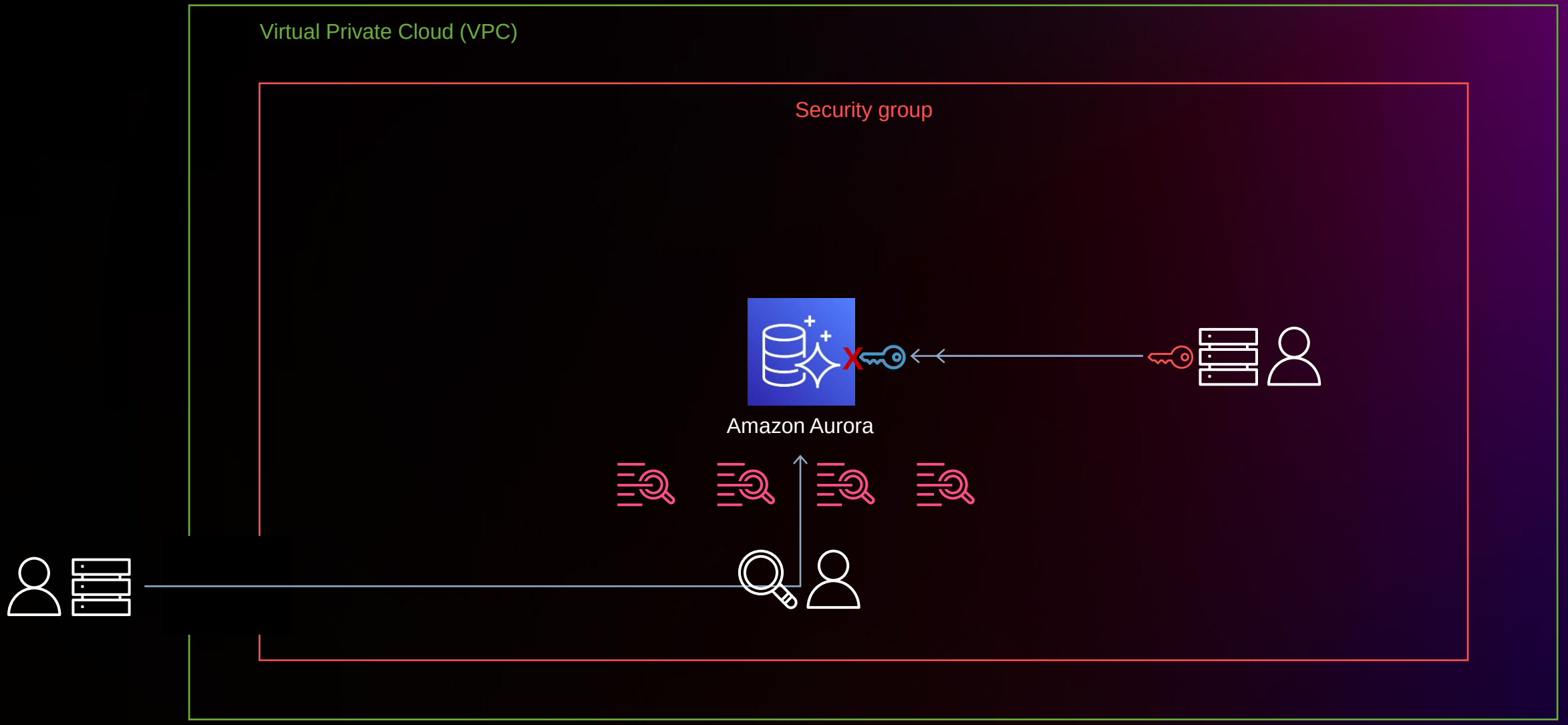
Resource section provides details on the database, and the user that accessed it

Actor section provides details on the IP address that the database was accessed from, including country, and ASN

aws

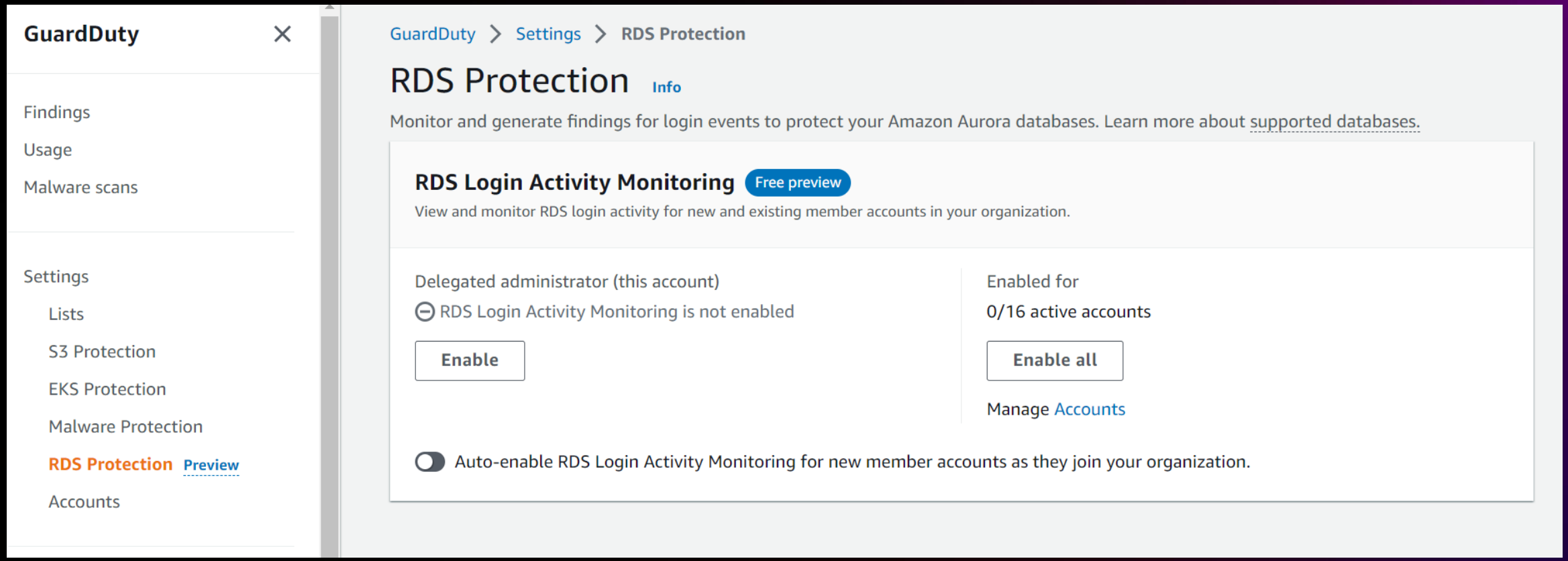
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

When GuardDuty RDS Protection detects a threat you can quickly take action

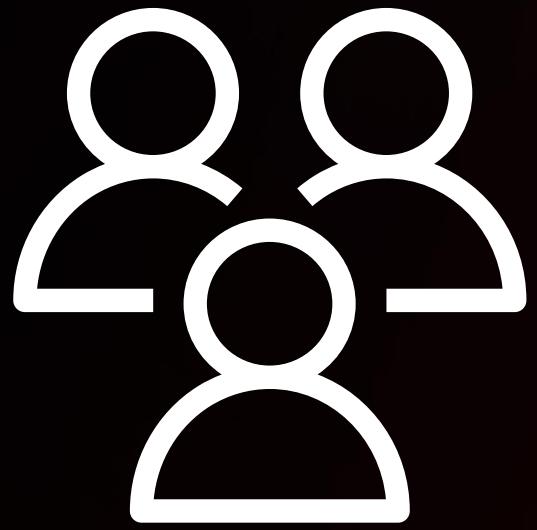


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting started



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Available resources



Amazon GuardDuty:

https://aws.amazon.com/guardduty/

Amazon Aurora Security:

https://aws.amazon.com/rds/aurora/features/#Highly_Secure





GuardDuty RDS Protection User Documentation:

https://docs.aws.amazon.com/guardduty/latest/ug/rds-protection.html

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



***Please complete the session survey in the* mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.