

亚马逊云科技云原生等保方案指南

目录

1 文档介绍	4
2 方案整体介绍	5
2.1 方案架构图	5
2.2 方案用到的服务	5
3 搭建基础环境	7
3.1 创建 VPC	7
3.2 创建 EC2 实例（含安全组）	8
3.3 创建 RDS 数据库	12
3.3.1 创建数据库子网组 <i>subnet group</i>	12
3.3.2 创建 RDS 实例	14
3.3.3 配置 RDS 安全组	18
3.4 创建 ALB 应用负载均衡	20
3.4.1 创建安全组	20
3.4.2 创建目标群组	22
3.4.3 创建 ALB	24
3.5 部署 WEB 服务	27
3.5.1 部署服务	27
3.5.2 验证网站效果	28
3.5.2 配置域名访问	28
3.5 创建 S3 存储桶	29
3.5.1 创建私有存储桶	29
3.5.2 通过 VPC 私网访问存储桶	31
3.5.3 存储桶设置权限	32
4 身份访问控制 IAM	34
4.1 创建系统管理员	34
4.1.1 创建用户组	34
4.1.2 创建用户	35
4.1.3 开启 MFA	38
4.1.4 验证登录时的 MFA 效果	47
4.2 创建安全管理员	48
4.2.1 创建用户	48
4.2.2 验证效果	50
4.3 创建审计员	51
4.3.1 创建用户	51
4.3.2 验证效果	52
5 开通云审计 CLOUDTRAIL	55
5.1 创建跟踪	55
5.2 审计跟踪结果	57

6 四层网络访问控制	58
6.1 虚拟私有网络 VPC	58
6.2 四层网络访问控制 SG 和 NACL	58
6.3 网络 IDS GUARDDUTY	59
6.3.1 启用 GuardDuty	59
6.3.2 GuardDuty PoC	60
1 场景说明	60
2 执行步骤	60
3 查看结果	61
4 参考资料	62
6.4 GUARDDUTY 与 NACL 和 WAF 联动来实现 IPS (可选)	62
7 七层网络访问控制	63
7.1 创建 WEB ACL	63
7.2 WEB ACL 关联到 ALB	65
7.3 日志保存在 S3 中	66
7.4 验证效果	67
7.4.1 正常 URL	67
7.4.2 SQL 注入	67
8 安全运维	69
8.1 SESSION MANAGER 方式	69
8.1.1 配置 Systems Managers	69
8.1.2 安装 SSM Agent	71
8.1.3 Session Manager 配置	71
8.1.4 增加 EC2 profile 的权限	74
8.1.5 创建到 Systems Manager 的接入端点	75
8.1.5 使用 Session Manager 运维 EC2 服务器	78
8.1.6 查看 CloudWatch Logs 中的运维日志	79
8.2 堡垒机方式	81
9 主机安全	82
9.1 主机监控与告警	82
9.2 安恒主机安全 EDR	83
9.3 亚马逊云科技主机安全服务	83
9.3.1 CVE 漏洞检测 Inspector	83
9.3.2 恶意软件检测 GuardDuty Malware Detection	83
9.3.3 补丁管理 Patch Manager	84
9.4 OS 加固	84
10 数据安全	85
10.1 敏感数据加密	85
10.2 RDS 密钥轮转 (可选)	85
10.2.1 创建密钥	85
10.2.2 使用密钥	87
10.3 网站 HTTPS	88
10.3.1 申请证书	88

10.3.2 配置 HTTPS 访问.....	90
10.3.3 验证 HTTPS 访问.....	92
10.4 网页防篡改.....	93
11 数据库审计	94
11.1 开启审计日志配置	94
11.1.1 RDS MySQL	94
11.1.2 RDS PostgreSQL	97
11.1.3 DynamoDB.....	97
11.2 日志发送到 CLOUDWATCH LOGS.....	98
11.3 验证效果.....	99
11.3.1 造数据库日志.....	99
11.3.2 在 CloudWatch Logs 中查看日志.....	100
12 云安全中心	101
12.1 统一管理安全事件	101
12.1.1 开通 Config 服务.....	101
12.1.2 开通 Security Hub 服务.....	103
12.2 GUARDDUTY 集成 SECURITY HUB.....	105
12.3 管理控制台的其他访问控制	105
13 日志集中审计	106
13.1 安装 CLOUDWATCH AGENT	107
13.2 配置 CLOUDWATCH AGENT	108
13.2.1 通过 Wizard 配置	108
13.2.2 使用 parameter store 配置.....	112
13.3 验证集中日志效果	114
14 备份	116
14.1 创建备份计划.....	116
14.2 创建备份角色	117
14.2 分配备份资源.....	118
14.3 设置备份到异地 REGION.....	119
14.4 查看备份结果	120

1 文档介绍

基于云原生等保解决方案，为客户提供 step by step 的部署实施手册，并提供测评机构检查点对应的演示内容。

本文档可以加快客户的等保技术方案实施及整改过程。

本文档主要是技术演示目的，客户在对自己生产环境变更的时候还需要按自己的方式进行，建议先在测试环境验证，然后再对生产环境变更。

本文档在各个章节都有对应的官方帮助文档的链接，对于有些特定场景的情况请参考描述更完善的官方帮助文档。

2 方案整体介绍

2.1 方案架构图

本方案是先构建一个单账号单 Region 的三层架构云环境，然后再此基础上构建安全能力。



2.2 方案用到的服务

如下服务是安全能力建设相关的服务，没包括基础云资源（如 EC2、ALB、RDS、S3 等）。

Standard (75分左右)	功能说明	定价 (宁夏)	成本预估 (万CNY/年 , 按月付)
VPC/INACL\安全组	网络隔离	free	0
IAM(MFA)	权限访问控制	free	0
CloudTrail	云资源操作日志	¥0.65 per 100,000 data events recorded	0.5
CloudWatch	设备和资源监控及告警	2 per metric per month for the first 10,000 metrics	0.5
Certificate Manager	SSL证书服务	free	0
Secret Manager	RDS密钥轮转	¥0.344 per 10,000 API calls	0.1
Security Hub	安全管理中心	¥0.0067 per check per month for the first 100,000 checks	0.2
GuardDuty	云威胁检查	不同日志定价不同、阶梯定价	2
KMS	加密服务	¥0.20 per 10,000 requests	0.1
WAF	7层安全防护	¥ 32.65 per month per ACL , ¥ 3.92 per 1 million requests	2
CloudWatch log/S3	日志集中审计	6.228 per GB ingested	1
RDS log	数据库日志审计	统计到CloudWatch Log中	0
Backup	跨区域备份	RDS快照，每月每 GB ¥ 0.580	2
Bastion Host	安恒合作定制版	PDM报价	—
EDR	安恒合作定制版	PDM报价	—

注 : 以100vcpu、10M流量的规模预估 ; 实际成本与业务量强相关 , 以实际账单为准。

3 搭建基础环境

本章节是可选部分，主要是为了后续安全能力建设步骤的演示使用；客户根据自己的真实生产环境做后续步骤的安全建设即可。

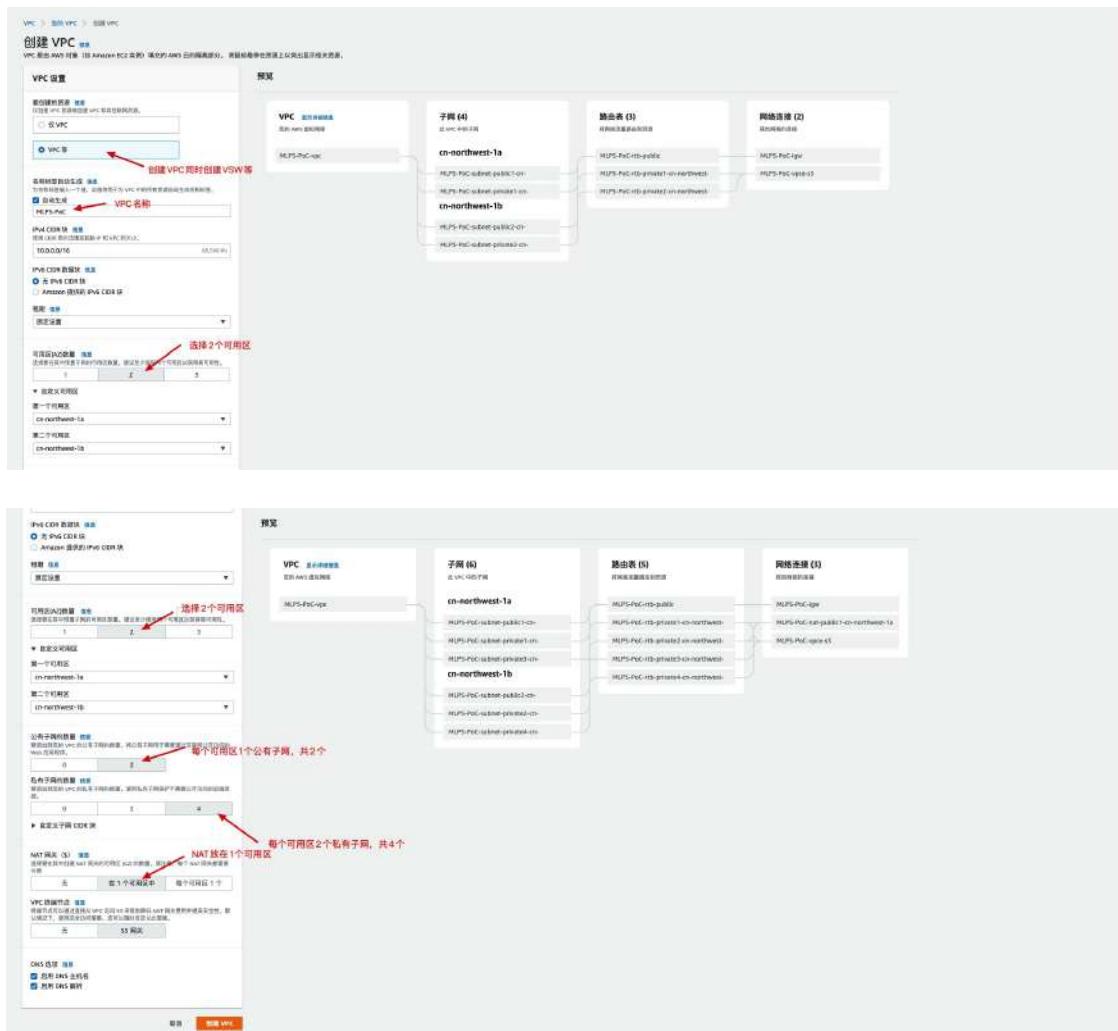
在中国区 Beijing Region 创建生产环境，然后在 Ningxia Region 做异地备份。

参考官方帮助文档：

创建 VPC 及 EC2:<https://docs.amazonaws.cn/vpc/latest/userguide/vpc-getting-started.html>

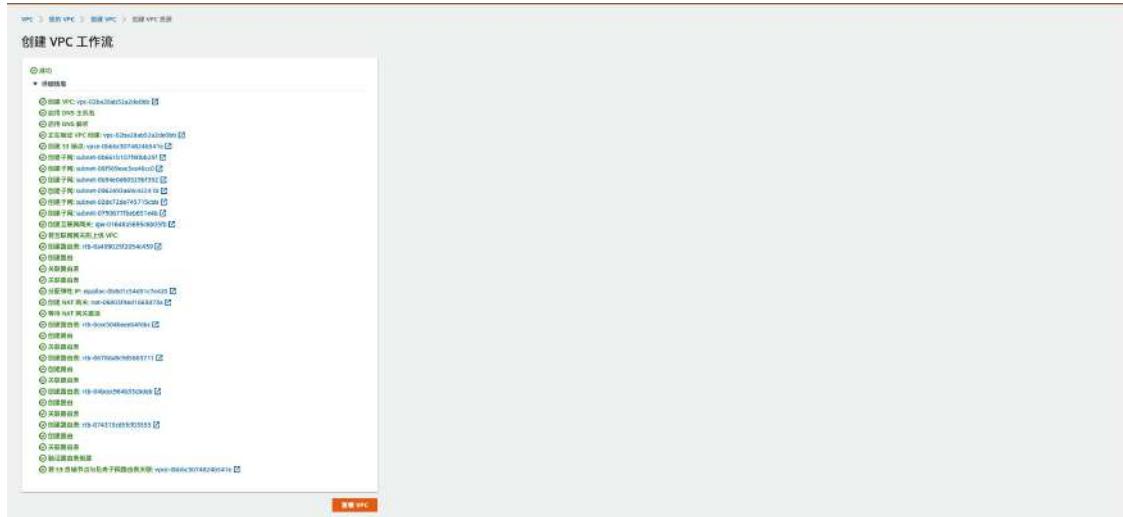
3.1 创建 VPC

1. 通过控制台 Console 导航到 VPC 页，开始创建 VPC，包括 4 个子网，1 个 NAT。按实际需要，选择对应的参数：



2. 选完参数后，点击“创建 VPC”按钮，开始创建。

如下每个步骤都执行完成，即表示 VPC 和子网等创建完成：



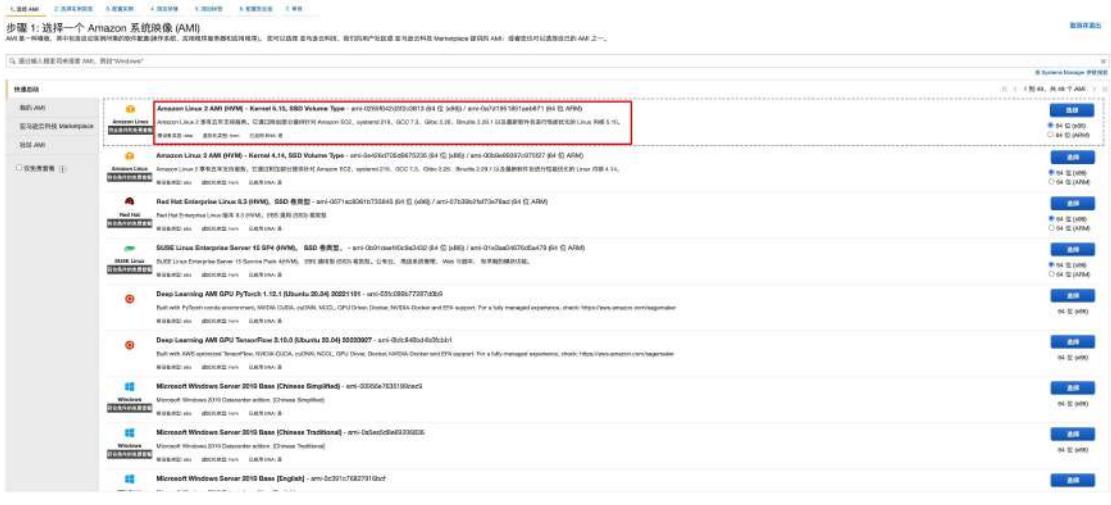
在该 VPC 中，在两个可用区中，一共创建了 6 个子网：

- 2 个 public subnet, 用于部署 ALB 和堡垒机等；
 - 2 个 private subnet 子网用来部署 EC2 及应用, MLPS-PoC-subnet-private1-cn-northwest-1a 和 MLPS-PoC-subnet-private2-cn-northwest-1b；
 - 2 个 private subnet 子网用来部署 RDS, MLPS-PoC-subnet-private3-cn-northwest-1a 和 MLPS-PoC-subnet-private4-cn-northwest-1b。

3.2 创建 EC2 实例（含安全组）

通过控制台 Console 导航到 EC2 页，开始新创建 EC2 实例；创建 2 个 EC2 实例，如下步骤演示的是在 MLPS-PoC-subnet-private1-cn-northwest-1a 子网创建实例，然后再自行按同样方法在子网 MLPS-PoC-subnet-private2-cn-northwest-1b 创建一台 EC2。

1. 选择 Amazon Linux 2 的 x84 镜像



2.按实际需求选择实例规格：

步骤 2: 选择一个实例类型
Amazon EC2 是亚马逊云服务，适合不适合使用该服务没有类型的限制，购买的是可以按照应用需求选择和配置。它包括 CPU、内存、存储和网络带宽不同的规格，可以根据用途为您的应用程序选择适当的规格。有关购买的建议以及如何选择特定的计算套餐的信息，请参阅“了解更多”。

实例	类型	vCPU	内存 (GiB)	实例存储 (GiB)	实例存储带宽 (GiB/s)	网络带宽 (Mbps)	GPU
t2	12.nano	1	0.9	0.007 GiB	-	1 Gbps	
t2	12.nano	1	1	0.007 GiB	-	1 Gbps	
t2	12.small	2	4	0.007 GiB	-	1 Gbps	
t2	12.medium	2	8	0.007 GiB	-	1 Gbps	
t2	12.large	4	16	0.007 GiB	-	1 Gbps	
t2	12.xlarge	8	32	0.007 GiB	-	1 Gbps	
t2	12.2xlarge	2	63	0.007 GiB	-	1 Gbps	
t2	12.4xlarge	2	1	0.007 GiB	-	1 Gbps	
t2	12.6xlarge	2	2	0.007 GiB	-	1 Gbps	
t2	12.8xlarge	2	4	0.007 GiB	-	1 Gbps	
t2	12.10xlarge	2	8	0.007 GiB	-	1 Gbps	
t2	12.12xlarge	4	16	0.007 GiB	-	1 Gbps	
t2	12.16xlarge	8	32	0.007 GiB	-	1 Gbps	
m4	ingress	7	3.0	0.007 GiB	-	1 Gbps	
m4	48.nano	2	1	0.007 GiB	-	1 Gbps	
m4	16.nano	2	2	0.007 GiB	-	1 Gbps	
m4	48.medium	2	4	0.007 GiB	-	1 Gbps	
m4	16.medium	2	8	0.007 GiB	-	1 Gbps	
m4	48.large	4	16	0.007 GiB	-	1 Gbps	
m4	16.large	4	32	0.007 GiB	-	1 Gbps	
m4	48.xlarge	8	64	0.007 GiB	-	1 Gbps	
m4	16.xlarge	8	128	0.007 GiB	-	1 Gbps	

3.子网选择 MLPS-PoC-subnet-private1-cn-northwest-1a

步骤3: 配置实例详细信息

配置实例详细信息，选择使用一个 VPC 上的多个子网，通过 IPv4 地址和其子网、向实例分配的可用子网等参数。

基础设置	<input type="text" value="1"/>
网络安全	<input type="checkbox"/> 启用 IPv4 天线 网卡 ① <input checked="" type="radio"/> /opt/CloudWatchLogs/Logstash/Logstash-1.log C 使用 VPC 子网 ② <input checked="" type="radio"/> 从所有子网中选择 (1) 个子网 自动分配 IP ③ <input checked="" type="radio"/> 从所有子网中选择 (1) DNS 属性 ④ <input checked="" type="radio"/> 使用子网的 DNS 名称 DNS Headers ⑤ <input checked="" type="radio"/> Create a private IPv4 (A record) DNS 选项 ◎ 为该子网创建 IPv4 (A) 和 IPv6 (AAAA) DNS 选项 ◎ 在子网中使用 IPv6 (AAAA) DNS 选项
带宽设置	<input type="checkbox"/> 将实例添加到带宽队列 带宽队列 ⑥ <input checked="" type="radio"/> 标准队列
弹性伸缩	<input type="checkbox"/> 弹性伸缩 弹性伸缩保护 ⑦ <input type="checkbox"/> 弹性伸缩为弹性伸缩之父启用 弹性伸缩停止 ⑧ <input type="checkbox"/> 弹性伸缩停止 弹性伸缩停止 ⑨ <input type="checkbox"/> 弹性伸缩停止 策略 ⑩ <input type="checkbox"/> 使用 CloudWatch 弹性伸缩 将对弹性伸缩进行限制 弹性伸缩在满足所有限制后停止运行 弹性伸缩停止 ⑪ <input type="checkbox"/> 弹性伸缩停止 策略 ⑫ <input type="checkbox"/> 弹性伸缩停止 将对弹性伸缩进行限制 弹性伸缩在满足所有限制后停止运行
文件系统	<input type="checkbox"/> 无 不使用自动挂载

网络接口 ⑬ 新建文件系统

取消 上一步 完成并启动 下一步：启动配置

4.按需填写系统盘的大小和规格：

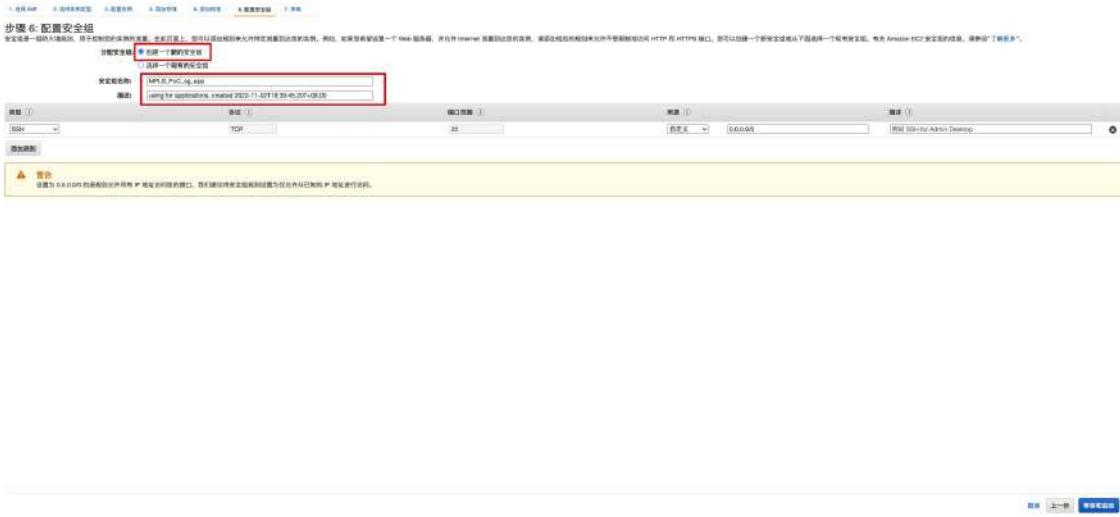
步骤4: 添加存储

选择实例所需的存储类型。您可以将其映射到新购买的存储或已有的存储。存储可以是具有固定容量的Amazon EBS 存储或带有 Amazon EBS 中存储的快照。

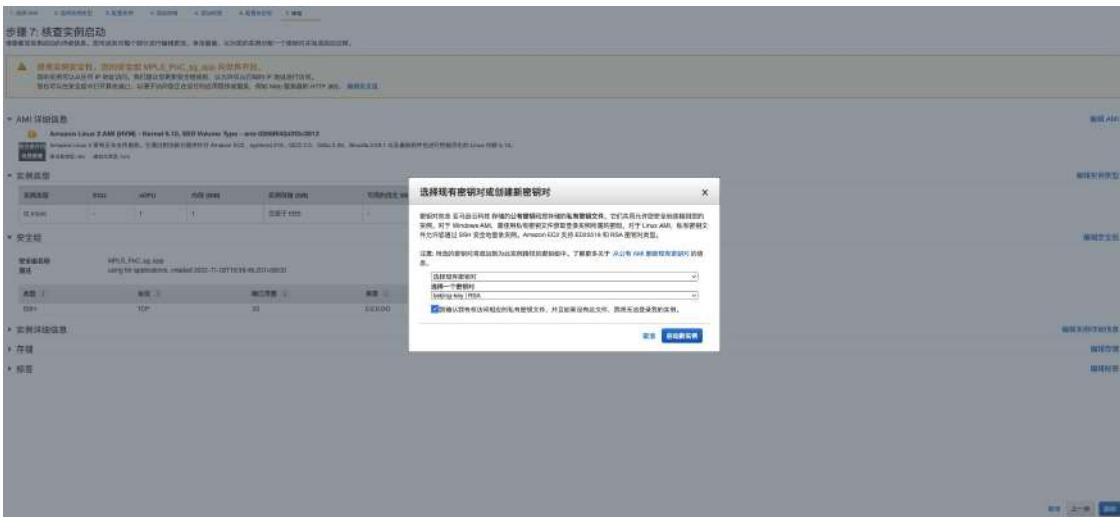
卷类型 ⑭	仅卷 ⑮ <input type="radio"/> 临时 ⑯ <input type="radio"/> 快照 ⑰ <input type="radio"/> EBS ⑱ <input checked="" type="radio"/> 混合 ⑲	大小 (GB) ⑳ <input type="text" value="80"/>	卷类型 ㉑ <input type="radio"/> 临时 ㉒ <input checked="" type="radio"/> EBS ㉓ <input type="text" value="80 GB"/> ㉔ 不适用 ㉕ 未设置 ㉖	IPDS ㉗	带宽 (Mbps) ㉘ <input type="text" value="30000"/> 不适用 ㉙	连接限制 ㉚	挂载 ㉛
有关如何为多卷安装的更多信息，请参阅 Amazon Linux 安装指南。有关免费权限要使用哪种使用限制的信息，请参阅“了解更多”。							
<p>Shared file system ㉜</p> <p>You currently don't have any file systems on this instance. Before "Add file system" button becomes visible on this screen.</p> <p>Add file system ㉝</p>							

取消 上一步 完成并启动 下一步：启动配置

5.创建一个新的安全组，规则用默认只放行 22 端口访问；在网络安全章节部分，会再设置安全组的规则

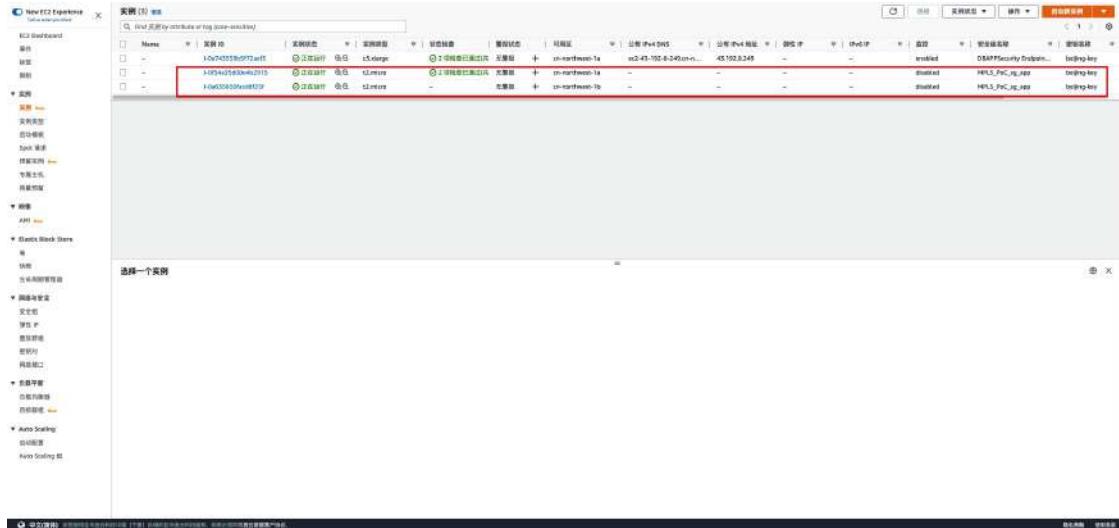


6.选择一个密钥对，用来通过 ssh 登陆 EC2 用；如果没有之前创建好的密钥对，选择新建一个。



7.同样方法在子网 MLPS-PoC-subnet-private2-cn-northwest-1b 再创建一台 EC2；

新创建好的 2 台 EC2：

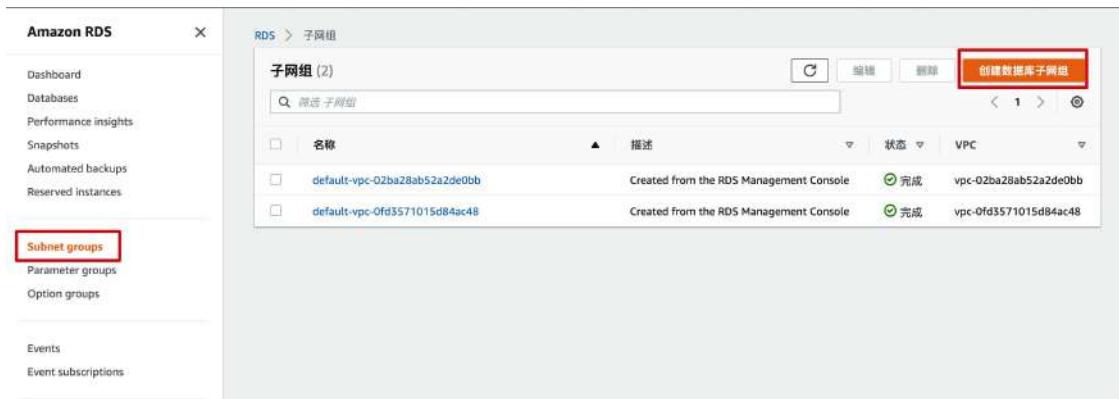


3.3 创建 RDS 数据库

3.3.1 创建数据库子网组 subnet group

数据库 subnet group 时用来制定 RDS 实例所在的 subnet，可以提前创建好、也可以在创建 RDS 的时候自动创建。本示例中我们提前创建好，便于规划网络架构。

1. 在 RDS 控制台导航到 subnet groups 列表页，然后创建数据库子网组



2. 起个名字，然后选择之前创建好的 VPC

Amazon RDS

RDS > 子网组 > 创建数据库子网组

创建数据库子网组

要创建新的子网组，请指定其名称和描述，并选择一个现有 VPC，然后，您将能够添加与该 VPC 相关的子网。

子网组详细信息

名称
您在创建子网组后将无法修改名称。
db-subnet-group-mlps

描述
create RDS subnet group

VPC
选择一个当您要为数据库子网组使用的子网相对应的 VPC 标识符。您在创建子网组后将无法选择其他 VPC 标识符。
MLPS-PoC-vpc (vpc-02ba28ab52a2de0bb)

3. 选择 subnet 时，先点击添加与此 VPC 关联的所有子网，然后保留 private3 和 4 子网；private3 和 4 子网对应的子网 ID 可以在 VPC 控制台的 subnets 列表页查到。
- 如下图是查 private3 和 4 子网对应的子网 ID：

VPC dashboard

Filter by VPC: Select a VPC

Virtual private cloud

Your VPCs

Subnets

Name	子网 ID	状态	VPC	IPv4 CIDR
MLPS-PoC-subnet-private3-cn-northwest-1a	subnet-02de72de745715cbb	Available	vpc-02ba28ab52a2de0bb ML...	10.0.16.0/20
MLPS-PoC-subnet-public1-cn-northwest-1b	subnet-06f569eac3ce46cc0	Available	vpc-02ba28ab52a2de0bb ML...	10.0.16.0/20
-	subnet-02ff2b5d99d731d19	Available	vpc-0fd5571015d84ac48	172.31.0.0/16
-	subnet-04fa12ba381f2047e	Available	vpc-0fd3571015d84ac48	172.31.1.0/16
MLPS-PoC-subnet-private1-cn-northwest-1a	subnet-0b94e0d60529bf392	Available	vpc-02ba28ab52a2de0bb ML...	10.0.128.0/20
MLPS-PoC-subnet-public1-cn-northwest-1a	subnet-0b661b10780bb25f	Available	vpc-02ba28ab52a2de0bb ML...	10.0.0.0/16
MLPS-PoC-subnet-private4-cn-northwest-1b	subnet-0790677fbeb851e4b	Available	vpc-02ba28ab52a2de0bb ML...	10.0.176.0/20
MLPS-PoC-subnet-private2-cn-northwest-1b	subnet-0962493a69c42241b	Available	vpc-02ba28ab52a2de0bb ML...	10.0.144.0/20
-	subnet-095acab61630f3874	Available	vpc-0fd3571015d84ac48	172.31.3.0/16

选择一个子网

4. 然后按查到的子网 ID 来选择子网：

Amazon RDS

Dashboard

Databases

Performance insights

Snapshots

Automated backups

Reserved instances

Subnet groups

Parameter groups

Option groups

Events

Event subscriptions

添加子网

将子网添加到此子网组。您可以在下面一次添加一个子网，或者添加与此 VPC 相关的所有子网。编辑该组后，您可以对其进行添加/编辑。至少需要 2 个子网。

添加与此 VPC 相关的所有子网

可用区
cn-northwest-1a

子网
subnet-02de72de745715cbb (10.0.160.0/20)

此子网组中的子网 (2)

可用区	子网 ID	CIDR 块	操作
cn-northwest-1a	subnet-02de72de745715cbb	10.0.160.0/20	删除
cn-northwest-1b	subnet-0790677fbeb851e4b	10.0.176.0/20	删除

创建

5. 然后创建子网组，在 subnet group 列表页，可以看到我们新创建好的 subnet group

The screenshot shows the 'Subnet groups' section of the Amazon RDS console. It lists three subnet groups: 'db-subnet-group-mlps', 'default-vpc-02ba28ab52a2de0bb', and 'default-vpc-0fd3571015d84ac48'. The first group is highlighted with a red box.

3.3.2 创建 RDS 实例

在本章节中，我们创建一个多 AZ 的 MySQL 数据库。

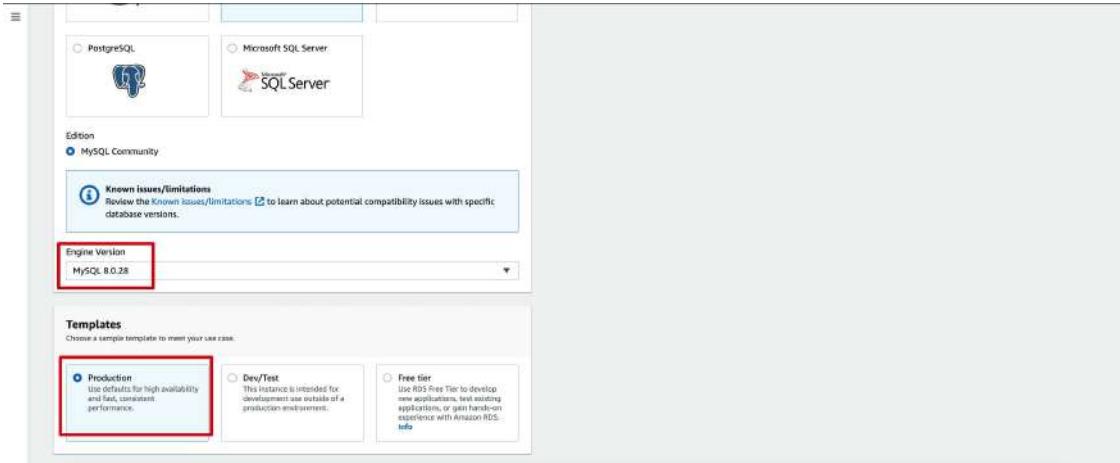
- 首先在管理控制台中导航到 RDS 页，然后在 Databases 实例列表页里点击“Create database”

The screenshot shows the 'Databases' section of the Amazon RDS console. It lists two databases: 'database-1' and 'database-99'. The 'Create database' button is highlighted with a red box.

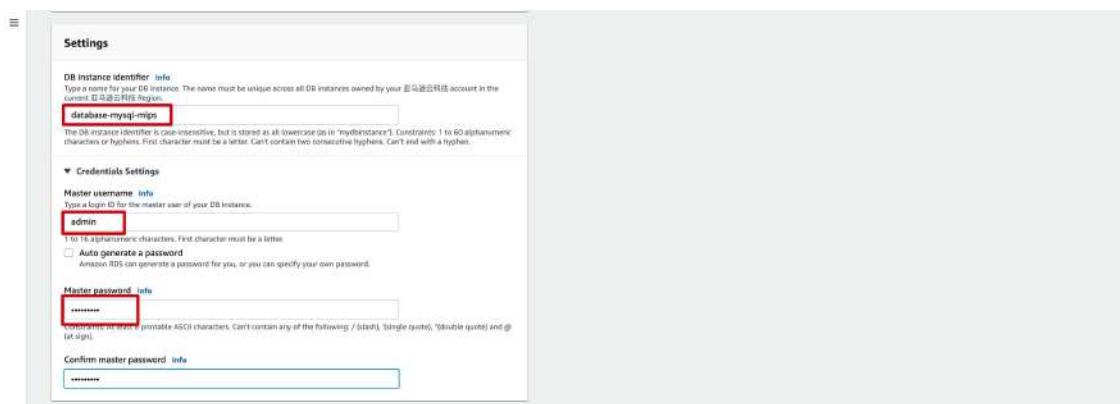
- 然后选择“Standard create”和“MySQL”数据库引擎，

The screenshot shows the 'Create database' wizard. In the 'Choose a database creation method' step, 'Standard create' is selected. In the 'Engine options' step, 'MySQL' is selected under 'Engine type'.

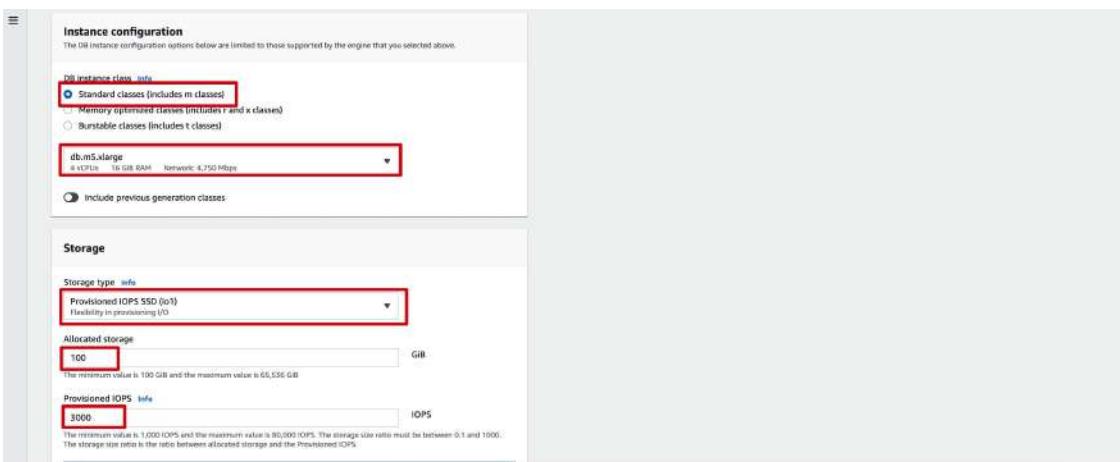
3. MySQL 版本按自己需要来选择,



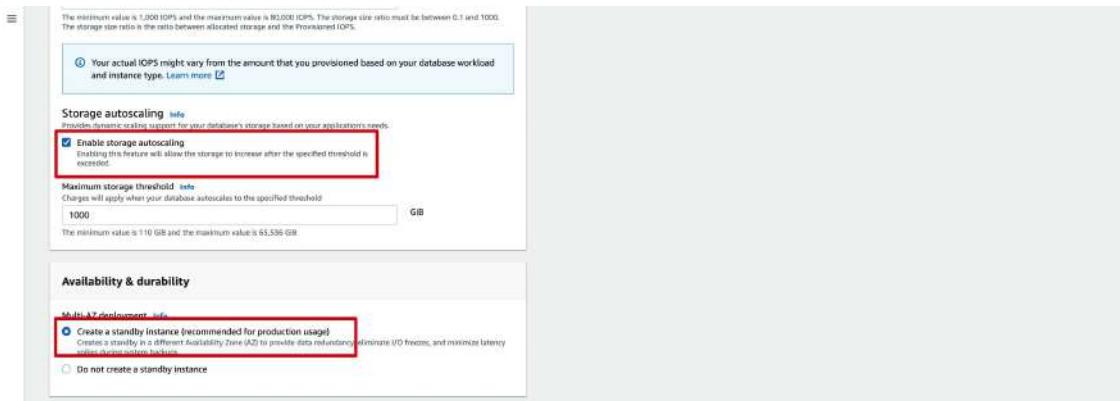
4. 填写数据库名称、数据库主账号的账号名和密码,



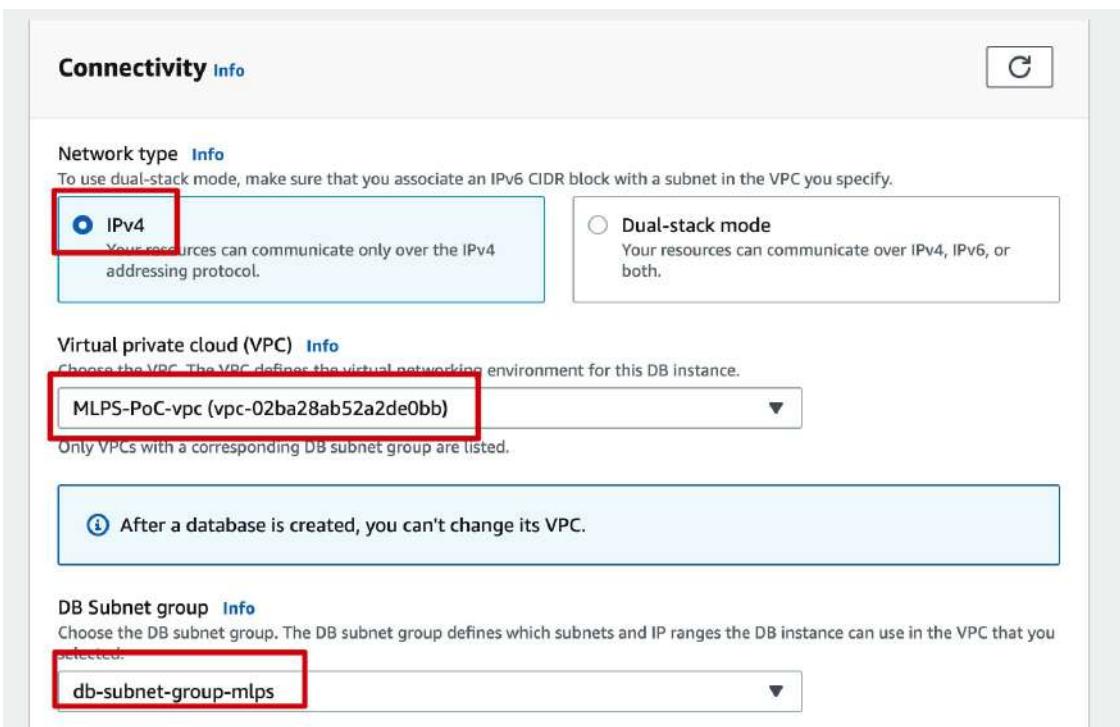
5. 选择数据库运行实例的规格, 按自己实际需要填写



6. 选择多 AZ 的形式, 这个等保中有要求, 多 AZ 可以提高数据库的可用性



- 选择之前创建好的 VPC 和 subnet group；数据库设置为不可公网访问，创建新的数据库实例的安全组，安全组规则默认是只开 3306 端口



Public access [Info](#)

Yes
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

No
RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall) [Info](#)
Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

Choose existing
Choose existing VPC security groups

Create new
Create new VPC security group

New VPC security group name

▶ Additional configuration

8. 基于 password 的认证,

Database port [Info](#)
TCP/IPv4 port that the database will use for application connections.
3306

Database authentication

Database authentication options [Info](#)

Password authentication
Authenticates using database passwords.

Password and IAM database authentication
Authenticates using the database password and user credentials through Amazon IAM users and roles.

Password and Kerberos authentication
Chooses a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

Monitoring

Performance Insights [Info](#)

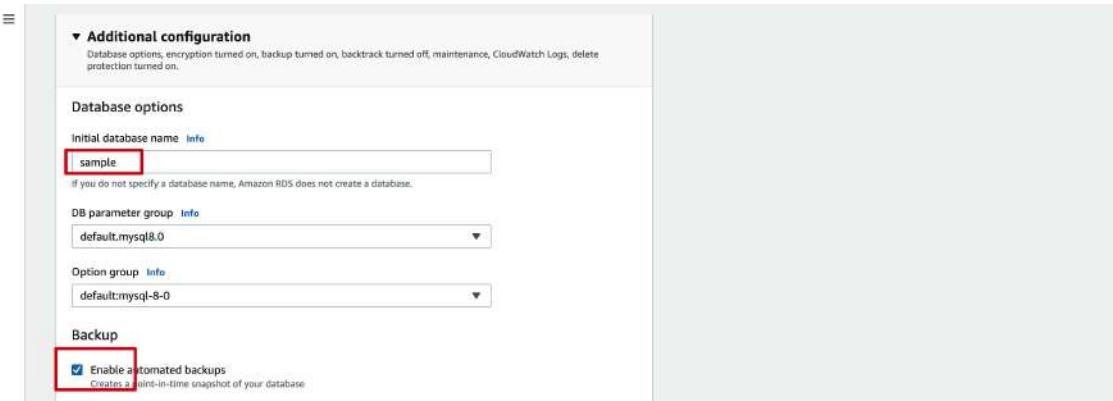
Enabling Performance Insights will automatically enable the MySQL Community performance schema.
Learn more [\[?\]](#)

Turn on Performance Insights [Info](#)

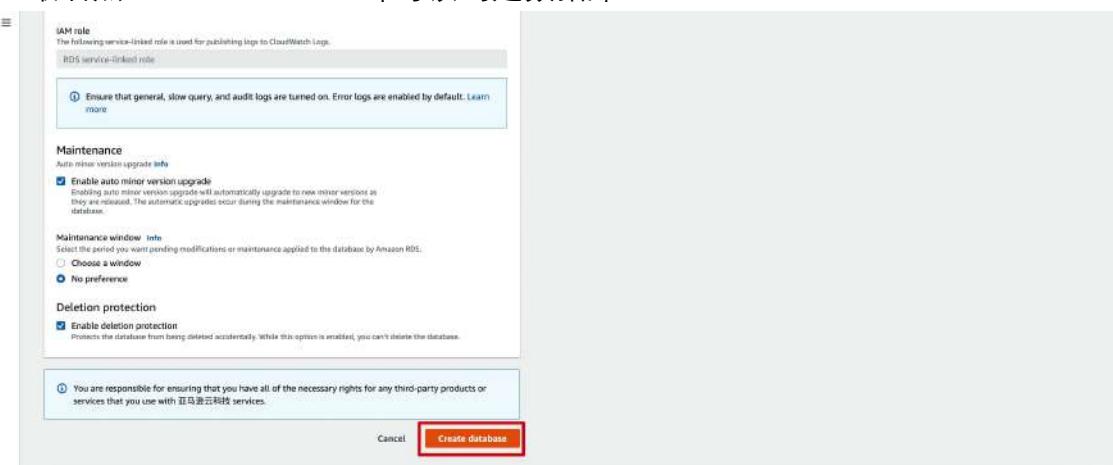
Retention period [Info](#)

9. 在 alternatively 配置中, 初始数据库名称填“sample”, 这个名称在后边部署 web 服务时会用到; 确认下 backup 是启用的, 参数默认即可。

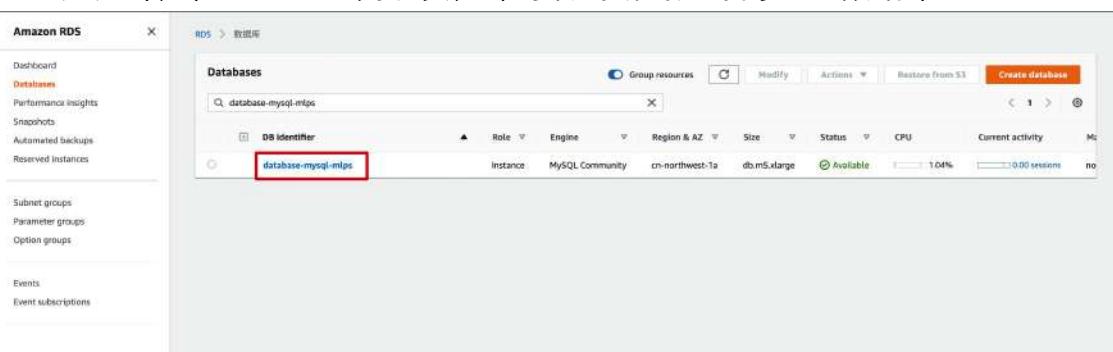
backup 是等保的必选项。此处的 backup 是本 region 的 backup, 后续章节中我们会介绍跨 Region 的 backup, 跨 Region 的 backup 是等保三级的必选项, 等保二级可选。



10. 最后点“Create database”即可以创建数据库



11. 过几分钟，在 database 列表页，即可看到新创建好的 RDS 数据库。



3.3.3 配置 RDS 安全组

给 RDS 的安全组增加入站规则，允许部署在 EC2 上的 app 能访问 RDS。

1. 在 EC2 控制台的安全组列表页，找到我们在创建 RDS 时创建的安全组

The screenshot shows the AWS RDS Security Groups console. On the left, there's a sidebar with navigation links for various AWS services like Lambda, VPC, and Auto Scaling. The main area displays a table of security groups with columns for Name, Security Group ID, Security Group Name, VPC ID, Description, Owner, Inbound Rules Count, and Outbound Rules Count. One specific security group, 'sg-027de42168b1b906c - MPLS_PoC_sg_database', is selected and highlighted with a red box. Below the table, there's a detailed view of this selected security group, showing its name, ID, description ('Created by RDS management console'), and VPC ID ('vpc-02ba28ab52a2de0bb').

2. 编辑入站规则

This screenshot shows the AWS EC2 Security Groups console. The left sidebar includes links for EC2, VPC, Lambda, and Auto Scaling. The main content area shows the 'Inbound Rules' tab for the security group 'sg-027de42168b1b906c - MPLS_PoC_sg_database'. It lists one rule: 'sg-008f135d5b1ff24d...' which allows MySQL/Aurora traffic from port 3306 to 52.82.200.6/32. A red box highlights this rule. Another red box highlights the 'Edit Inbound Rule' button at the top right of the rule list.

3. 添加一条新规则，源选择部署 app 的安全组，然后保存即可。这样部署在该安全组内的 EC2 上的 app 都可以访问这个 RDS 了。

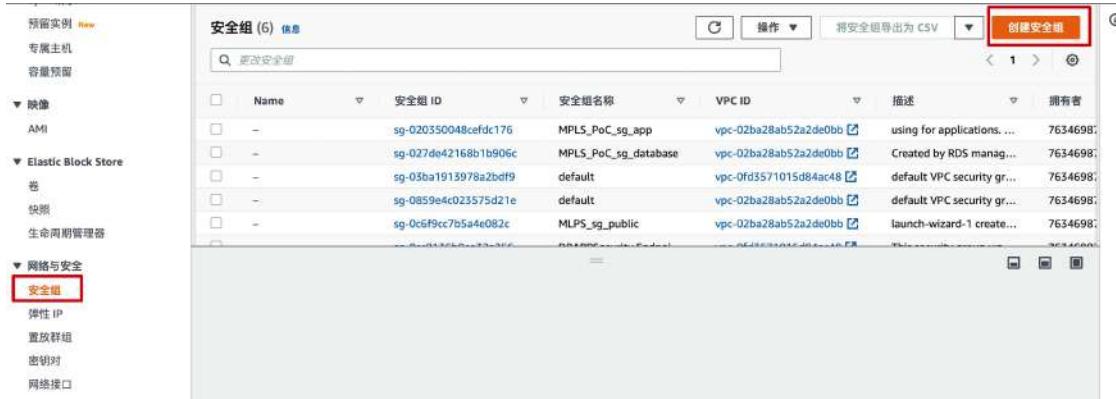
This screenshot shows the 'Edit Inbound Rule' dialog box. It has tabs for 'Inbound Rule' and 'Description'. Under 'Inbound Rule', it shows a table with columns for Name, Security Group Rule ID, IP Version, Type, Protocol, Port Range, and Source. A new rule is being added, with the 'Name' field empty and the 'Source' dropdown set to 'sg-008f135d5b1ff24d...' (the app deployment security group). The 'Type' dropdown is set to 'MySQL/Aurora'. The 'Protocol' is 'TCP', 'Port Range' is '3306', and 'Source' is '52.82.200.6/32'. The 'Description' field contains the placeholder 'MPLS_PoC_sg_app | sg-020350048cefdc176'. At the bottom, there are 'Cancel', 'Preview更改', and 'Save Rule' buttons. A red box highlights the 'Source' dropdown.

3.4 创建 ALB 应用负载均衡

3.4.1 创建安全组

给待创建的 ALB 提前创建一个安全组，然后在 app 的安全组入向规则中增加新创建的安全组（即让 alb 能转流量到 app 的 EC2）。

1. 在 EC2 控制台的安全组列表页，新建安全组



The screenshot shows the AWS EC2 Security Groups list page. On the left, there's a sidebar with options like Preemptible Instances, Dedicated Hosts, Capacity Reservations, Images, Elastic Block Store, Volumes, Snapshots, and Network & Security. Under Network & Security, 'Security Groups' is selected and highlighted with a red box. The main area displays a table of existing security groups with columns for Name, Security Group ID, Security Group Name, VPC ID, Description, and Owner. One row is selected, showing 'sg-0c5f9cc7b5a4e082c' with 'MLPS_sg_public' as its name.

2. 起个名字，选择之前创建的 vpc



The screenshot shows the 'Create Security Group' wizard. It's on the 'Basic Information' step. The 'Name' field is filled with 'MLPS_sg_public_web'. The 'Description' field has 'for alb' typed into it. The 'VPC' dropdown menu is open, showing 'vpc-02ba28ab52a2de0bb' as the selected option. There are tabs for 'Information' and 'Advanced' at the bottom of each section.

3. 入站规则，协议 TCP，端口 8088（这个是为了演示用的端口，实际使用的时候一般是 https 的 443 和 http 的 80；因为 443 和 80 需要走备案流程才能打开，所以选了 8088），任意源 IP；

出站规则，默认，全部放行。

4. 然后创建即可。安全组列表页即可看到刚创建的安全组

Name	安全组 ID	安全组名称	VPC ID	描述	拥有者
sg-0132aa70a917cd174	MPLS_sg_public_web	vpc-02ba28ab52a2de0bb	for alb	7634698	
sg-020350048cefdc176	MPLS_PoC_sg_app	vpc-02ba28ab52a2de0bb	using for applications. ...	7634698	
sg-027de42168b1b906c	MPLS_PoC_sg_database	vpc-02ba28ab52a2de0bb	Created by RDS manag...	7634698	
sg-03ba1913978a2bdf9	default	vpc-0fd3571015d84ac48	default VPC security gr...	7634698	
sg-0859e4c023575d21e	default	vpc-02ba28ab52a2de0bb	default VPC security gr...	7634698	

5. 在安全组列表中找到部署 app 应用的安全组，MPLS_PoC_sg_app，在该安全组中增加入方向规则，放行刚创建的 alb 的安全组

Name	安全组 ID	安全组名称	VPC ID	描述	拥有者
sg-0132aa70a917cd174	MPLS_sg_public_web	vpc-02ba28ab52a2de0bb	for alb	7634698	
sg-020350048cefdc176	MPLS_PoC_sg_app	vpc-02ba28ab52a2de0bb	using for applications. ...	7634698	
sg-027de42168b1b906c	MPLS_PoC_sg_database	vpc-02ba28ab52a2de0bb	Created by RDS manag...	7634698	
sg-03ba1913978a2bdf9	default	vpc-0fd3571015d84ac48	default VPC security gr...	7634698	
sg-0859e4c023575d21e	default	vpc-02ba28ab52a2de0bb	default VPC security gr...	7634698	

编辑入站规则

入站规则

安全组规则 ID	类型	协议	端口范围	信息	源信息	描述 - 可选
sgr-05fad1b409353f9d6	SSH	TCP	22	自定义		<input type="text"/> 删除
sgr-04c4216e0a09d02f0	HTTP	TCP	80	自定义		<input type="text"/> 删除
-	HTTP	TCP	80	自定义	<input type="text"/> Q	<input type="button"/> 取消 <input type="button"/> 预览更改 <input type="button"/> 保存规则

3.4.2 创建目标群组

为下一步创建 alb 时提前准备目标群组，即 app 的 EC2 组合

- 在 EC2 控制台的目标群组列表中，创建新的目标组

Elastic Block Store

卷

快照

生命周期管理器

网络与安全

安全组

弹性 IP

置放群组

密钥对

网络接口

负载平衡

负载均衡器

目标群组 New

- 目标类型选择实例

第 1 步
指定组详细信息

您的负载均衡器会将请求路由到一个目标组并对目标执行运行状况检查。

第 2 步
注册目标

基本配置

创建目标组后，无法更改本部分中的设置。

选择目标类型

实例

- 支持将负载均衡到特定 VPC 中的实例。
- 有助于使用 Amazon EC2 Auto Scaling 来管理和扩展您的 EC2 容量。

IP 地址

- 支持将负载均衡到 VPC 和本地资源。
- 促使路由到同一实例上的多个 IP 地址和网卡接口。
- 借助基于微服务的架构提供灵活性，简化应用程序间通信。
- 支持 IPv6 目标，支持连接到 IPv6 通信和 IPv4 到 IPv6 NAT。

- 选择之前创建的 VPC，端口选择 80

目标组名称
webappgroup

最多允许使用 32 个字母数字字符(包括连字符)，但名称不能以连字符开头或结尾。

协议 端口
HTTP : 80

VPC
选择包含要添加到此目标组的实例的 VPC。
MLPS-PoC-vpc
vpc-02ba28ab52a2de0bb
IPv4: 10.0.0.0/16

协议版本
 HTTP1
使用 HTTP/1.1 发送请求到目标。在请求协议为 HTTP/1.1 或 HTTP/2 时受支持。
 HTTP2
使用 HTTP/2 发送请求到目标。在请求协议为 HTTP/2 或 gRPC 时受支持。但特定于 gRPC 的功能不可用。
 gRPC
使用 gRPC 发送请求到目标。在请求协议为 gRPC 时受支持。

4. 运行状况检查用默认配置

运行状况检查
关联的负载均衡器按照下面的设置定期发送请求至已注册目标，以测试其状态。

运行状况检查协议
HTTP

运行状况检查路径
使用"/"的默认路径对 root 执行 ping 操作；如果您愿意，也可以指定自定义路径。
/

最多允许 1024 个字符。

▶ 高级运行状况检查设置

5. 选择两个待部署 app 的 EC2

第 1 步
指定组详细信息

这是创建目标组的可选步骤。但是，为确保负载均衡器将流量路由到此目标组，您必须注册目标。

第 2 步
注册目标

可用的实例 (2/3)

实例 ID	名称	状态	安全组	区	子网 ID
<input checked="" type="checkbox"/> i-0a635650facd8f25f	app_mysqlclient	<input checked="" type="radio"/> running	MPLS_PoC_sg_app	cn-northwest-1b	subnet-0962493a69c42241b
<input type="checkbox"/> i-05bf6b5ec81c349a3	jump_public_subnet	<input checked="" type="radio"/> running	MLPS_sg_public	cn-northwest-1a	subnet-0b661b107f80bb25f
<input checked="" type="checkbox"/> i-046a37dcda3ff24eb		<input checked="" type="radio"/> running	MPLS_PoC_sg_app	cn-northwest-1a	subnet-0b94e0d60529bf392

2 个已选择

所选实例的端口
用于将流量路由到所选实例的端口。

6. 然后点“包含如下待处理事项”，再点“创建目标组”

The screenshot shows the 'Create Target Group' wizard. Step 2 is titled '包含如下待处理事项' (Include the following pending items). Below it, there's a note: '下面的 2 个选项待注册。请在跳转后添加或注册更多目标。' (The following 2 items are pending registration. Please add or register more targets after the jump.). The main area is titled '查看目标' (View Targets) and shows a table with 2 rows:

删除	运行状况	实例 ID	名称	端口	状态	安全组	区	子网 ID
X	挂起	i-046a37dcda5ff24eb		80	running	MPLS_PoC_sg_app	cn-northwest-1a	subnet-0b94e0d60529bf392
X	挂起	i-0a635650facdf8f25f	app_mysqlclient	80	running	MPLS_PoC_sg_app	cn-northwest-1b	subnet-0962493a69c42241b

At the bottom, there are buttons: '2 挂起' (2 pending), '上一步' (Previous Step), and a red-bordered '创建目标组' (Create Target Group) button.

7. 然后点击创建目标组；回到目标组列表，即可看到刚创建的目标组（还未关联负载均衡的状态）

The screenshot shows the EC2 Target Groups list. On the left, there's a navigation sidebar with sections like AMI, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. Under Load Balancing, '目标群组' (Target Groups) is highlighted with a red box. The main panel shows a table with one row:

名称	ARN	端口	协议	目标类型	负载均衡器
webappgroup	arn:aws-cn:elasticloadbalan...	80	HTTP	实例	① 没有关联

Below the table, there's a message: '已选择 0 目标组' (0 target groups selected) and '选择以上的目标组' (Select the target groups above).

3.4.3 创建 ALB

1. 在 EC2 控制台的负载均衡器列表页，创建负载均衡器

The screenshot shows the EC2 Load Balancers list. On the left, there's a navigation sidebar with sections like Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. Under Load Balancing, '负载均衡器' (Load Balancers) is highlighted with a red box. The main panel shows a table with one row:

名称	DNS 名称	状态	VPC ID	可用区	类型
没有负载均衡器					

Below the table, there's a message: '您在 cn-northwest-1 中没有任何负载均衡器' (You have no load balancers in the cn-northwest-1 region) and a red-bordered '创建负载均衡器' (Create Load Balancer) button.

2. 选择创建应用负载均衡器



3. 选择面向互联网、IPv4 的类型（如果有 IPv6 的需求，可以选择双栈类型），

基本配置

负载均衡器名称
名称在您的亚马逊云科技账户中必须是唯一的，并且在创建负载均衡器后不能更改。

最多允许使用 32 个字母数字字符(包括连字符)，但名称不能以连字符开头或结尾。

模式 [信息](#)
创建负载均衡器后无法更改模式。
 面向互联网 [查看](#)
面向互联网的负载均衡器会通过互联网将来自客户端的请求路由到目标。需要一个公共子网。 [了解更多信息](#)
 内部 [查看](#)
内部负载均衡器会使用私有 IP 地址将来自客户端的请求路由到目标。

IP 地址类型 [信息](#)
选择子网使用的 IP 地址类型。
 IPv4 [查看](#)
推荐用于内部负载均衡器。
 双堆栈 [查看](#)
包括 IPv4 和 IPv6 地址。

4. 下拉选择我们之前创建的 VPC, 和两个 public subnet

Network mapping 信息
负载均衡器会根据您的 IP 地址设置，将流量路由到选定子网中的目标。

VPC 信息
为您的目标选择 Virtual Private Cloud (VPC)，仅有具有互联网网关的 VPC 才可供选择。创建负载均衡器后，无法更改选定的 VPC。要确认您的目标的 VPC，请查看您的目标组 [\[1\]](#)。

MLPS-PoC-vpc vpc-02ba28ab52a2de0bb IPv4: 10.0.0.0/16	[2]
--	---------------------

映射 信息
每个区域至少选择两个可用区和一个子网。负载均衡器仅将流量路由到这些可用区中的目标。负载均衡器或 VPC 不支持的可用区域不可供选择。

cn-northwest-1a

子网
subnet-0b661b107f80bb25f **MLPS-PoC-subnet-public1-cn-northwest-1a**

IPv4 设置
由 亚马逊云科技 分配

cn-northwest-1b

子网
subnet-06f569eac3ce46cc0 **MLPS-PoC-subnet-public2-cn-northwest-1b**

IPv4 设置
由 亚马逊云科技 分配

5. 选择给 alb 创建的安全组

安全组 信息
安全组是一组防火墙规则，用于控制至负载均衡器的流量。

安全组
最多选择 5 个安全组

<input type="checkbox"/> Q	MLPS_sg_public_web VPC: vpc-02ba28ab52a2de0bb	sg-0132aa70a917cd174	[3]
	MPLS_PoC_sg_app VPC: vpc-02ba28ab52a2de0bb	sg-020350048cefcd176	
	MPLS_PoC_sg_database VPC: vpc-02ba28ab52a2de0bb	sg-027de42168b1b906c	
	default VPC: vpc-02ba28ab52a2de0bb	sg-0859e4c023575d21e	
	MLPS_sg_public VPC: vpc-02ba28ab52a2de0bb	sg-0c6f9cc7b5a4e082c	[4]

6. 端口写 8088， 目标组选择上一节创建的



7. 回到负载均衡列表页，可以看到刚创建好的 ALB，已经处于 active 状态



3.5 部署 Web 服务

3.5.1 部署服务

参考如下链接，在两台 EC2 上部署 web 服务，数据写到 RDS，通过 ALB 做负载均衡。

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateWebServer.html

这个 web 服务示例，需要注意如下两点：

1. 在两台服务器上，分别执行 `sudo echo "hello world" >/var/www/html/index.html`，这样 ALB 的健康检查就会成功（即 `httpd` 返回 200），否则健康检查提示失败（`httpd` 返回的是 403）。
2. 在 RDS 数据库中，确保创建 RDS 时创建的初始数据库名时 sample，否则需要提前创建一个名为 sample 的 database，因为 `SamplePage.php` 页面会连接名为 sample 的数据库，如果链接不上会返回 500 错误。

然后在跳板机（或能访问这两台 app 的 EC2）上 curl 每台 EC2 上部署的 web 服务，能通即代表成功。（前面两个是 ALB 健康检查用的；后两个是对外提供的 WEB 功能）

curl <http://10.0.141.79:8088/>

curl <http://10.0.147.215:8088/>

curl <http://10.0.141.79:8088/SamplePage.php>

curl <http://10.0.147.215:8088/SamplePage.php>

3.5.2 验证网站效果

然后在浏览器上，通过 ALB 的公网地址来访问网站：

[\[compute.amazonaws.com:8088/SamplePage.php\]\(http://ec2-55-122-41-31.us-west-2.compute.amazonaws.com:8088/SamplePage.php\)](http://ec2-55-122-41-31.us-west-</p></div><div data-bbox=)

页面会返回输入学习姓名和地址的页面；输入姓名和地址后，会下下面显示出来：

The screenshot shows a web browser window with the following content:

Address bar: alb-mlps-388779185.cn-northwest-1.elb.amazonaws.com:8088/SamplePage.php

Page title: Sample page

Form fields:

NAME	ADDRESS
<input type="text"/>	<input type="text"/>

Table data:

ID	NAME	ADDRESS
1	zhang san1	beijing1

Add Data button: Add Data

附另一个参考资料：创建一个 wordpress 的 WEBSITE 的 workshop：

<https://general-webapp.workshop.aws/lab1.html>

3.5.2 配置域名访问

如果有自己的域名可以直接使用，还没有域名可以在亚马逊云科技 国际站的 Route53 上申请（中国站不支持域名注册申请）。

本示例中，在其它域名服务上处已经有一个已经注册好的域名，awsliyangln.com

1. 在该域名服务商系统上，增加一个解析记录，web.awsliyangln.com，CNAME 记录解析到 ALB 的地址

2. 然后通过域名访问网站, <http://web.awsliyangln.com:8088/SamplePage.php>

ID	NAME	ADDRESS
1	zhang san1	beijing1
2	li si1	tianjin1

3.5 创建 S3 存储桶

本章节演示的存储桶是为了保持集中审计日志的，所以设置的是私有桶及对应的权限。如果您的存储桶是保持生产环境的文件或其他场景等，请根据实际需求来设计访问权限。

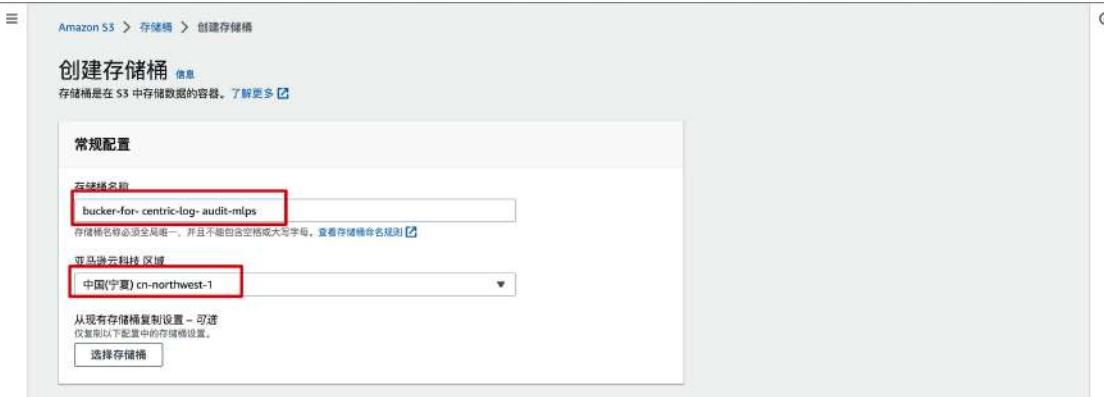
3.5.1 创建私有存储桶

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/creating-bucket.html>

1. 通过管理控制台导航到 S3 控制台，然后开始创建新的存储桶。

名称	亚马逊云科技 区域	访问	创建日期
没有存储桶			

2. 填写存储桶名字和位置；存储桶名称全局唯一。



3. 选择 ACL 已禁用（现在推荐使用 policy 来控制访问权限），设置阻止所有公开访问



4. 其他配置根据实际需求配置；如果没有特别需求，按默认配置即可；



5. 点击“创建存储桶”



6. 在存储桶的列表页，可以看到我们新创建好的 bucket

名称	亚马逊云科技 区域	访问	创建日期
bucker-for-centric-log-audit-mips	中国(宁夏) cn-northwest-1	存储桶和对象不是公开的	2022年11月25日 pm1:33:49 CST

3.5.2 通过 VPC 私网访问存储桶

参考资料：

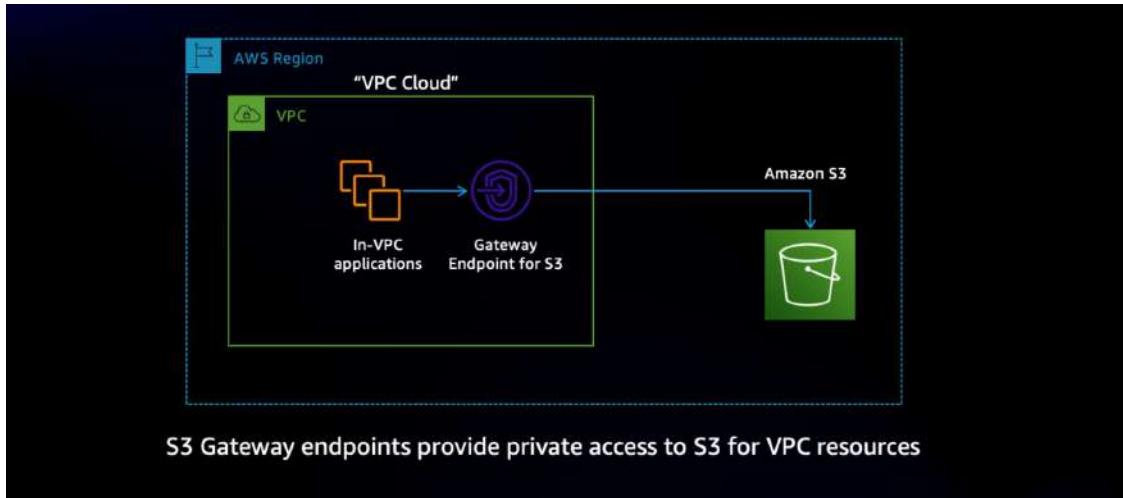
对应的 workshop：

<https://catalog.us-east-1.prod.workshops.aws/workshops/3a8d4ddf-66c5-4d26-ae6f-6292a517f46c/en-US>

使用 VPC Endpoint 从 VPC 或 IDC 内访问 S3，官方博客：

<https://aws.amazon.com/cn/blogs/china/use-vpc-endpoint-access-from-vpc-or-idc-s3/>

1. VPC 里的应用通过私网（非公网）访问 S3 时，架构图如下：



2. 创建 VPC 里的 Gateway Endpoint for S3。因为我们在创建 VPC 步骤的时候已经选择了创建 Gateway Endpoint for S3，所以在 VPC 的 endpoint 列表页能看到已经创建好的 Gateway Endpoint for S3，如下图。如果在创建 VPC 的时候选择不创建，那么在此步骤中需要参考如上 workshop 的链接说明来创建。

Name	VPC 接端节点 ID	VPC ID	服务名称
<input checked="" type="checkbox"/> MLPS-PoC-vpce-s3	vpce-0bbc3074824b541e	vpc-02ba28ab52a2de0bb MLPS-PoC-v...	com.amazonaws.cn-northwest-1.s3

3. 测试验证，在 VPC 内的一台 EC2 上配置 AWS CLI 命令，然后执行上传文件到 S3 并查看：

```
[ec2-user@ip-10-0-147-215 ~]$ aws s3 cp testfile.xyz s3://bucker-for-centric-log-audit-mlps
upload: ./testfile.xyz to s3://bucker-for-centric-log-audit-mlps/testfile.xyz
[ec2-user@ip-10-0-147-215 ~]$ aws s3 ls s3://bucker-for-centric-log-audit-mlps
2022-11-25 07:41:15 1073741824 testfile.xyz
```

3.5.3 存储桶设置权限

新创建的 bucket，默认的 policy 权限是空的，即没有针对 user 或 service 的任何限制。

对于 CloudWatch Logs 和 CloudTrail 投递过来的集中日志审计，提供写入权限。具体内容在对应日志审计章节介绍。

对于审计员的 IAM user，设置只读权限。

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html#example-bucket-policies-use-case-2>

4 身份访问控制 IAM

在等保中，在统一控制台集中管理的权限管理、云服务器运维里的权限管理等方面，有明确要求。

本章节创建的账号，除为了说明做必要的安全加固之外，在后续账号的权限管理中还会使用到。

创建 IAM user 相关的参考文档：

创建 user groups：

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_create.html

给 user groups 增加 policy：

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_manage_attach-policy.html

创建 user：

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html

启用 MFA 双因子认证：

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html#enable-virt-mfa-for-iam-user

4.1 创建系统管理员

创建系统管理员即云环境运维人员，并分配不同的权限。

4.1.1 创建用户组

1. 在管理控制台导航到 IAM 控制台的用户组列表页，创建用户组



2. 用户组名称 usergp_sysops；先不添加用户，等创建好用户之后再添加；



3. 添加权限策略；用 administrator 搜索，然后选择 administratorAccess；点击创建组



4. 然后回到用户组列表页，可以看到我们新创建的用户组



4.1.2 创建用户

1. 在 IAM 控制台的用户列表页，创建用户

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' at the top. Under '访问管理' (Access Management), '用户' (User) is selected and highlighted with a red box. The main area is titled '用户 (1) 信息' (User (1) Information) and contains a table with one row for 'user'. The table columns include '用户名' (Username), '组' (Group), '上次活动' (Last Activity), 'MFA' (Multi-Factor Authentication), '密码期限' (Password Last Used), and '活动状态' (Activity Status). The 'Add User' button at the top right is also highlighted with a red box.

- 创建用户的时候，一次可以创建多个，此处我们创建 2 个运维账号；这两个运维账号，在后续 Session Manager 做运维管控的时候，可以分配不同的权限。

The screenshot shows the 'Add User' wizard, Step 1: Set User Details. It has five steps numbered 1 to 5. Step 1 is active. The 'User Name' field contains 'user_sysops1' and 'user_sysops2'. There is a link to 'Add other users'. Below it, under 'Select AWS Cloud Access Type', it says '选择这些用户主要访问 AWS 云科技 的方式。如果选择仅编程访问，则不会阻止用户使用假定角色访问控制台。最后一个步骤提供了访问密钥和自动生成的密码。' (Select the primary access type for these users to AWS Cloud. If you choose Programmatic Access, it will not prevent users from using assumed roles to access the console. The last step provides access keys and automatically generated passwords.) The 'Programmatic Access - API, CLI, SDK' checkbox is checked. Under 'Control Panel Password', 'Automatically generated password' is selected. A note says '用户必须在下次登录时创建新密码' (The user must create a new password the next time they log in) and '用户自动获得 IAMUserChangePassword 策略以允许其更改自己的密码' (The user automatically receives the IAMUserChangePassword policy to allow them to change their own password). The 'Next Step: Permissions' button is highlighted with a red box.

- 添加到系统运维组里；



4. 标签和审核步骤默认通过，然后创建

用户名	用户类型	访问类型
user_sysops1 和 user_sysops2	亚马逊云科技	管理控制台访问 - 使用密码

控制台密码类型	需要重置密码	权限边界
自动生成	是	未设置权限边界

权限摘要

上面显示的用户将添加到以下组中。

类型	名称
组	usergp_sysops
托管策略	IAMUserChangePassword

5. 然后保存用户的密钥文件，用于分发给对应的用户；这里的密钥是初始密钥，首次登录的时候需要重置。
6. 回到用户列表页，可以看到刚创建好的两个用户

用户名	组	上次活动	MFA	密码期限	活动密钥有效期
user1	无	5 天前	无	89 天前	5 天前
user_sysops1	usergp_sysops	从不	无	从不	-
user_sysops2	usergp_sysops	从不	无	从不	-

4.1.3 开启 MFA

亚马逊云科技的 MFA 支持多种方式，包括 FIDO security keys、Virtual authenticator apps、TOTP hardware tokens，具体参考 [https://aws.amazon.com/iam/features/mfa/。](https://aws.amazon.com/iam/features/mfa/)

本示例用 Virtual authenticator apps 方式，需要提前在手机上安装 [Google Authenticator](#)。

1. 给 user_sysops1 用户开启 MFA；先通过 IAM 控制台的 user 列表页，打开 user_sysops1 的详情



The screenshot shows the AWS IAM User List page. On the left, there's a navigation sidebar with options like Identity and Access Management (IAM), Control Panel, and various management sections. Under '访问管理' (Access Management), '用户' (Users) is selected and highlighted with a red box. The main area displays a table of users with columns for Username, Group, Last Activity, MFA, Password Last Used, and Account Creation Date. The user 'user_sysops1' is highlighted with a red box in the 'Username' column.

2. 然后切换到安全证书 tab 页



The screenshot shows the AWS IAM User Details page for 'user_sysops1'. The left sidebar has the same navigation as the previous screen. The main area is titled '摘要' (Summary). It shows the User ARN (arn:aws:iam::763469678564:user/user_sysops1), Path (/), and Creation Time (2022-12-01 10:04 UTC+0800). Below this, there are tabs for '权限' (Permissions), '组 (1)' (Groups), '标签' (Tags), and '安全证书' (Security Certificates). The '安全证书' tab is selected and highlighted with a red box. It lists the attached policies: 'IAMUserChangePassword' and '亚马逊云科技 托管策略' (AWS Managed Policies).

3. 点击管理 MFA

Identity and Access Management (IAM)

用户 > user_sysops1

摘要

用户 ARN: arn:aws-cndaam::763489878584:user/user_sysops1

路径: /

创建时间: 2022-12-01 10:04 UTC+0800

权限: 权限 (1) 标签 安全证书

登录凭证

摘要: 控制台登录链接: https://763489878584.siginin.amazonaws.cn/console

控制台密码: 已启用 (从未登录) | 管理

已分配 MFA 设备: 未分配 | 管理

签名证书: 无

访问密钥

使用访问密钥从 亚马逊云科技 CLI、PowerShell 工具、亚马逊云科技 开发工具包以编程方式调用 亚马逊云科技，或者直接进行 亚马逊云科技 API 调用。您一次最多可拥有两个访问密钥（活跃或非活跃）。

删除用户

搜索 IAM



3. 出现如下页面，然后打开手机 app 程序 Google Authenticator，扫描如下二维码。

管理 MFA 设备



如果您的虚拟 MFA 应用程序支持扫描 QR 代码，可使用智能电话的摄像头扫描以下图片。



▶ 显示手动配置密钥

配置应用程序后，在下框中输入连贯的认证代码并单击“激活虚拟 MFA”。

认证代码 1

认证代码 2

取消

激活虚拟 MFA

5. 扫描二维码后，会出现一个 6 位数的数字，添加到上图的认证代码 1 中；然后等一会儿，待手机 app 上的 6 位数的数字换成新的后，把新的 6 位数的数字填到“认证代码 2”中，然后点“激活虚拟 MFA”按钮，即可完成。

手机扫二维码界面：

17:58



...



设置首个帐号

使用双重身份验证设置（Google 或第三方服务）中显示的二维码或设置密钥。如果您遇到问题，请转到
g.co/2sv



扫描二维码



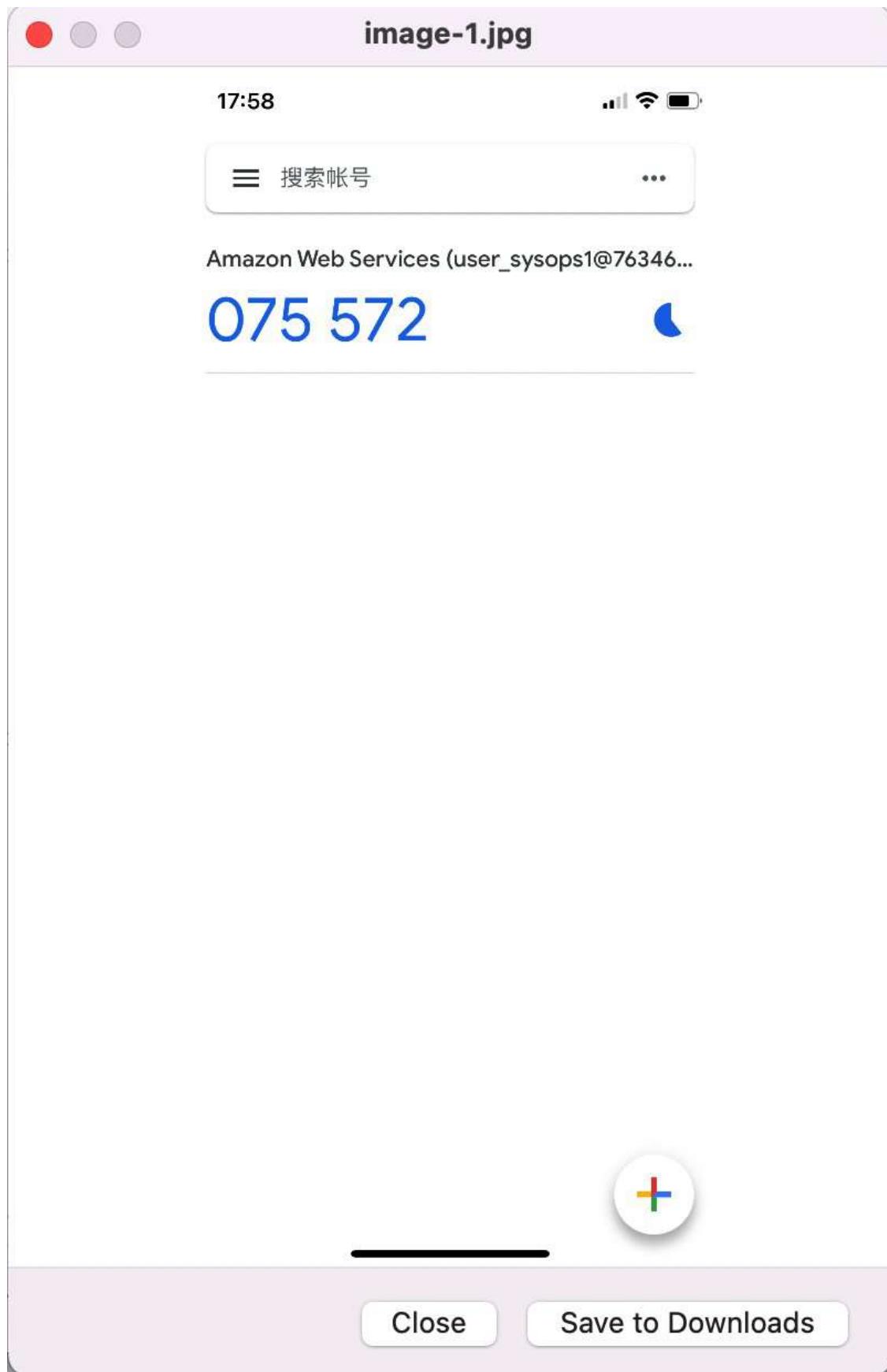
输入设置密钥

要导入现有帐号吗？

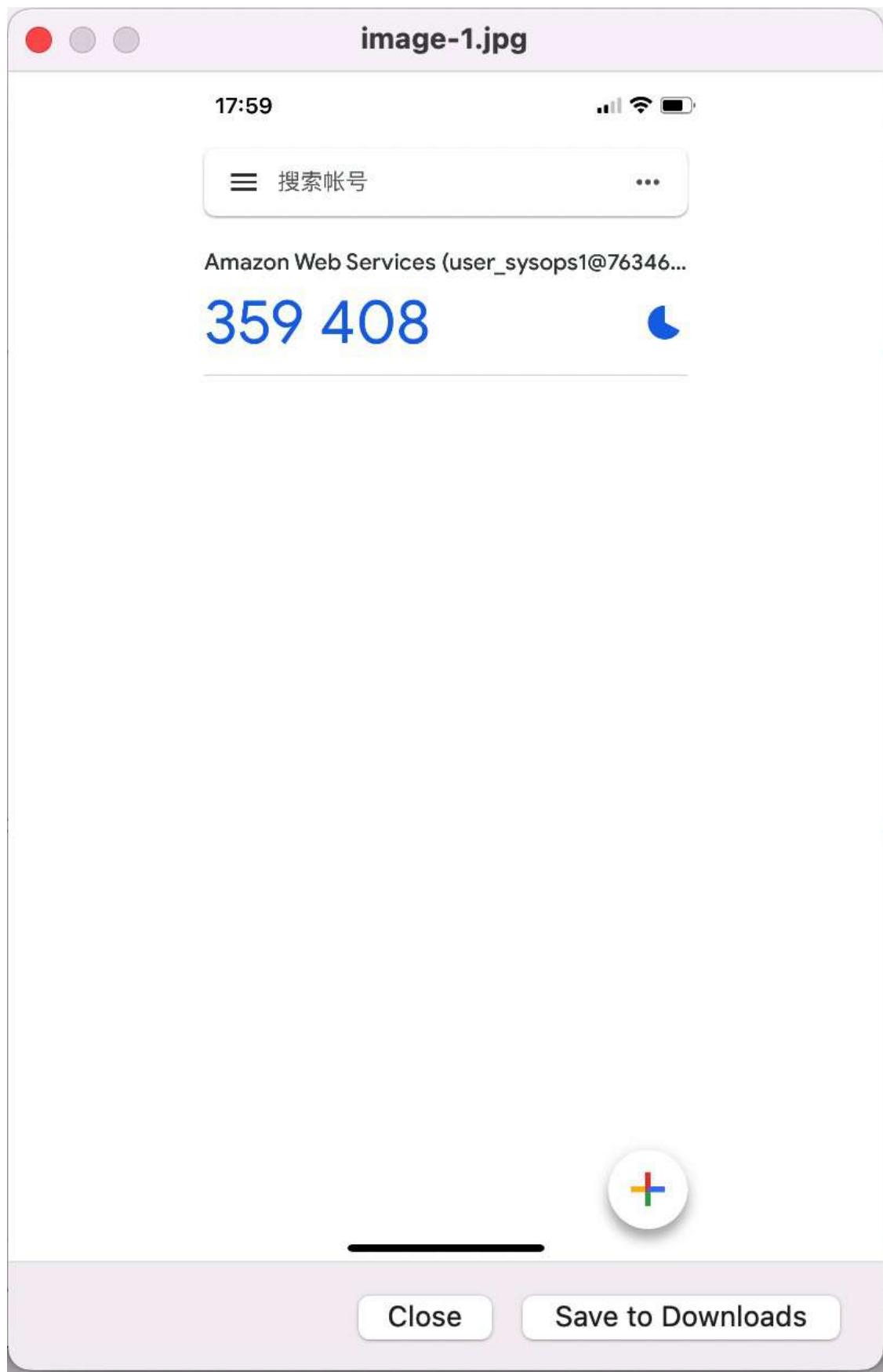
Close

Save to Downloads

手机第一个 6 位数界面：



手机第二个 6 位数界面：



6. 如上两个 6 位数按如下格式填写：



7. 激活成功。

Identity and Access Management (IAM)

用户 > user_sysops1

摘要

用户 ARN: arn:aws-cn:iam::763469678584:user/user_sysops1
路径: /
创建时间: 2022-12-01 10:04 UTC+0800

权限 **组 (1)** **标签** **安全证书**

登录凭证

摘要: • 控制台登录链接: https://763469678584.signin.amazonaws.cn/console
• 登录时需要 MFA。 [了解更多](#)

控制台密码: 已启用 (从未登录) | 管理

已分配 MFA 设备: arn:aws-cn:iam::763469678584:mfa/user_sysops1 (Virtual TOTP) | 管理

签名证书: 无

访问密钥

8. 用同样的方式，开启 user_sysops2 用户的 MFA。

4.1.4 验证登录时的 MFA 效果

1. 找到 IAM user 登录的地址；或者直接在 console 登录页，选择通过 IAM user 登录、输入 account uid 也可以。

Identity and Access Management (IAM)

用户 > user_sysops1

摘要

用户 ARN: arn:aws-cn:iam::763469678584:user/user_sysops1
路径: /
创建时间: 2022-12-01 10:04 UTC+0800

权限 **组 (1)** **标签** **安全证书**

登录凭证

摘要: • 控制台登录链接: https://763469678584.signin.amazonaws.cn/console
• 登录时需要 MFA。 [了解更多](#)

控制台密码: 已启用 (从未登录) | 管理

已分配 MFA 设备: arn:aws-cn:iam::763469678584:mfa/user_sysops1 (Virtual TOTP) | 管理

签名证书: 无

访问密钥

2. 输入用户名和密码

Sign in as IAM user

Account ID (12 digits) or account alias: 763469678584

IAM user name: user_sysops1

Password [Forgot password?](#):

Remember this account

Sign in

New to Amazon Web Services? [Create a new Amazon Web Services account](#)

Amazon GuardDuty
智能的威胁检测和持续的安全监控

[了解更多](#)

3. 然后登录，提示输入 MFA code，说明之前启用的 MFA 成功；

Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code:

885485

Submit

Cancel

English ▾

Terms of Use Privacy Policy

帮助 中文

京 ICP 备 00000000 号-1

4. 如果是首次用 IAM user 登录，需要重制秘密。然后正常进入控制台

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with links for 'AWS Lambda', 'AWS Lambda Regions', 'AWS Lambda Metrics', 'AWS Lambda Metrics Region', 'Services' (with a dropdown arrow), and 'Support'. On the right side of the top bar, there's a user profile section with a red box around the email address 'user_sysops1 @ 7634-6987-85...'. Below the top bar, the main title 'Amazon Web Services Management Console' is centered. To the left, there's a sidebar with sections for 'Amazon Web Services services', 'Find Services' (with a search bar containing 'Example: Relational Database Service, database, RDS'), 'Recently visited services' (empty), and 'All services'. In the center, there are three cards: 'Launch a virtual machine' (with EC2), 'Build a web app' (with Elastic Beanstalk), and 'Connect an IoT device' (with Amazon IoT). To the right, there are two 'Helpful tips' cards: 'Manage your costs' (with a budget icon) and 'Free Tier tips' (with a cloud icon). A large text box on the right side contains a note about the availability of the Amazon Web Services China (Ningxia) Region.

The Amazon Web Services China (Ningxia) Region, operated by Ningxia Western Cloud Data Technology Co., Ltd., is now available. By using Amazon Web Services services from the Amazon Web Services China (Ningxia) Region, you agree to the Western Cloud Data Customer Agreement.

4.2 创建安全管理员

分配安全事件管理服务的权限，包括 Security Hub 和 GuradDuty 的全部权限，其他权限可以按需再分配。

创建过程和上节创建运维人员的过程是一样的，只是权限分配不一样。

本节只记录几个关键步骤的截图。

4.2.1 创建用户

1. 填写用户组名称

Identity and Access Management (IAM)

创建用户组

为组命名

用户组名: usergo_sec

将用户添加到组 - 可选 (3) 信息

用户名	组	上次活动	创建时间
usergo_sec	usergo_sec		2022-12-03 10:08 (UTC+08:00)
usergo_sec	usergo_sec		2022-12-03 10:08 (UTC+08:00)
usergo_sec	usergo_sec		2022-12-03 10:08 (UTC+08:00)

2. 添加 securityhub 和 guardduty 的 fullaccess 权限

Identity and Access Management (IAM)

摘要

用户组名: usergo_sec

创建时间: December 03, 2022, 10:08 (UTC+08:00)

ARN: arn:aws:iam::763469878584:group/usergo_sec

权限策略 (2) 信息

策略名称	类型	描述
AmazonGuardDutyFullAccess	亚马逊云科技 托管	Provides full access to use Amazon GuardDuty.
AWSecurityHubFullAccess	亚马逊云科技 托管	Provides full access to use AWS Security Hub.

3. 创建用户

添加用户

设置用户详细信息

您可以一次添加多个具有相同访问类型和权限的用户。了解更多

用户名*: user_sec1

选择 亚马逊云科技 访问类型

选择这些用户主要访问 亚马逊云科技 的方式。如果选择仅编程访问，则不会阻止用户使用假定角色访问控制台，最后一个步骤提供了访问密钥和自动生成的密码。了解更多

选择 亚马逊云科技 凭证类型:

- 访问密钥 - 编程访问
为 亚马逊云科技 API、CLI、SDK 和其他开发工具启用 访问密钥 ID 和 私有访问密钥。
- 密码 - 亚马逊云科技 管理控制台访问
启用密码，使得用户可以登录到 亚马逊云科技 管理控制台。
- 自动生成的密码
自动生成并显示。

* 必填

取消 下一步: 权限

4. 用户添加到组

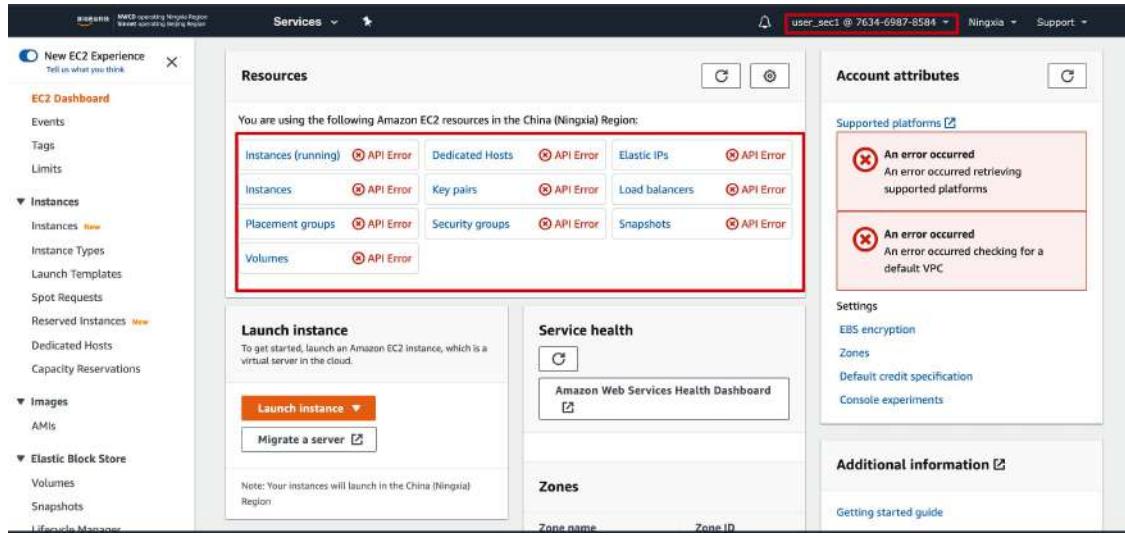


4.2.2 验证效果

- 用 user_sec1 账号登录控制台，可以进入 security hub 控制台

Failed checks	Resource
4	arm:aws-cn:elasticloadbalancing:cn-northwest-1:763469878584:loadbalancer/app/alb-mtls/b4ef864d226a25c6
3	AWS::Account:763469878584
3	arm:aws-cn:ec2:cn-northwest-1:763469878584:instance/i-046a37dcda3ff24eb
3	arm:aws-cn:ec2:cn-northwest-1:763469878584:instance/i-058def963946534c1
3	arm:aws-cn:ec2:cn-northwest-1:763469878584:instance/i-05bf6b5ec81c549a3

- 切换到 EC2 控制台，不能查看任何信息，提示 API Error，是因为调用 EC2 API 的时候没有权限。



4.3 创建审计员

分配查看 S3 中保存审计日志的只读权限。后续可以在优化一下，可以精细化到具体 bucket 的权限分配。

在集中日志审计方案中，如果是采用精简模式（即把日志集中到 CloudWatch Logs 中），那么需要给审计员开通 CloudWatch Logs 的查看权限，具体参考第 13 章。

创建过程和上节创建运维人员的过程是一样的，只是权限分配不一样。

本节只记录几个关键步骤的截图。

4.3.1 创建用户

添加用户组名称



添加权限，选择 S3 只读权限

The screenshot shows the AWS Identity and Access Management (IAM) Groups page. On the left, there's a sidebar with navigation options like '访问管理' (Access Management), '用户组' (Groups), '角色' (Roles), '策略' (Policies), and '账户设置' (Account Settings). The main area displays a list of policies under the heading '附加权限策略 - 可选 (已选 1/423)'. A search bar at the top allows filtering by policy name, with 'S3' currently selected. The list includes several policies, with 'AmazonS3ReadOnlyAccess' being the one highlighted by a red box.

创建用户

This screenshot shows the 'Create New User' wizard, Step 2: Set User Details. It asks for the user's name, which is 'user_auditor1', and provides a link to add other users. Below it, it asks for access type, choosing 'AWS Management Console' and 'Programmatic Access'. It also asks for a password, selecting 'Automatically generated'.

添加到组

This screenshot shows the 'Add User' wizard, Step 3: Set Permissions. It has three tabs: 'Attach existing policies directly', 'From existing user copy permissions', and 'Create new policy'. The first tab is selected, showing a list of groups. The 'user_auditor' group is selected and highlighted with a red box.

4.3.2 验证效果

- 用 user_auditor1 登录到 S3 控制台，可以查看 bucket 及其里面的文件

Amazon S3

Buckets

- Access Points
- Object Lambda Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Amazon Organizations settings

Amazon S3 > Buckets

Account snapshot

Last updated: Dec 2, 2022 by Storage Lens. Metrics are generated every 24 hours. Learn more

Total storage	Object count	Average object size	You can enable advanced metrics in the 'default-account-dashboard' configuration.
1.0 GB	52	19.7 MB	

Buckets (4) Info

Buckets are containers for data stored in S3. Learn more

Name	Amazon Web Services Region	Access	Creation date
bucker-for-centric-log-audit-mlps	China (Ningxia) cn-northwest-1	Bucket and objects not public	November 25, 2022, 13:33:49 (UTC+08:00)

Create bucket

Amazon S3

Buckets

- Access Points
- Object Lambda Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Amazon Organizations settings

Amazon S3 > Buckets > bucker-for-centric-log-audit-mlps

bucker-for-centric-log-audit-mlps Info

Objects

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
testfile.xyz	xyz	November 25, 2022, 15:41:15 (UTC+08:00)	1.0 GB	Standard

2. 试试创建删除文件，提示失败

Delete objects: status

The information below will no longer be available after you navigate away from this page.

Summary

Source	Successfully deleted	Failed to delete
s3://bucker-for-centric-log-audit-mlps	0 objects	1 object, 1.0 GB

Failed to delete

Failed to delete (1 object, 1.0 GB)

Name	Folder	Type	Last modified	Size	Error
testfile.xyz	-	xyz	November 25, 2022, 15:41:15 (UTC+08:00)	1.0 GB	Access denied

3. 切换到 EC2 控制台，没有权限查看具体信息

The screenshot shows the AWS EC2 Dashboard for the Ningxia Region. On the left, a sidebar lists navigation options like Events, Tags, Limits, Instances, Images, and Elastic Block Store. The main area is divided into sections: 'Resources' (listing Instances [running], Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, and Volumes, all with API Error status), 'Launch instance' (with 'Launch instance' and 'Migrate a server' buttons), and 'Service health' (linking to the Amazon Web Services Health Dashboard). On the right, 'Account attributes' include sections for Supported platforms (showing errors for retrieving supported platforms and checking for a default VPC), Settings (EBS encryption, Default credit specification, Console experiments), and Additional information (Getting started guide).

4. 切换的 Security Hub 控制台，没有权限打开

The screenshot shows the AWS Security Hub Home page for the cn-northwest-1 region. The URL in the browser bar is `cn-northwest-1.console.amazonaws.cn/securityhub/home?region=cn-northwest-1/`. A red box highlights the URL bar. A prominent red error message at the top states: 'Insufficient permissions. Your account does not have necessary permissions required to perform this action.' There is a 'Learn more' link at the bottom right of the message.

5 开通云审计 CloudTrail

CloudTrail 是对云资源相关操作的记录，对云环境的管理和审计至关重要。也是等保中集中日志审计的重要组成部分。

CloudTrail 在控制台支持一键开通。对于日志集中审计，需要把 CloudTrail 日志同步到 CloudWatch Logs（集中日志审计的精简模式）中或 S3 bucket（集中日志审计的普通模式）中，保存 180 天。

开启 CloudTrail 参考如下链接：

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-tutorial.html>

使用 IAM user user_sysops1 登陆、开通创建 trail。

第一个管理事件的 trail 是免费的，第二个及之后是按量付费的。

You can deliver one copy of your ongoing management events to your Amazon S3 bucket for free by creating trails.

<https://aws.amazon.com/cloudtrail/pricing/>

5.1 创建跟踪

1. 通过管理控制台，导航到 CloudTrail 控制台，开始创建跟踪。在跟踪的列表页来创建跟踪，这里的入口是标准化的创建流程；CloudTrail 首页里创建跟踪的流程是简化版，没办法选择 S3 bucket 等。



2. 填写 CloudTrail 名称，保存在我们之前创建好的 bucket 中



3. 启用加密存储，新建一个 kms；如果需要把 trail 日志同步到 CloudWatch Logs 查看，在 CloudWatch Logs 的“已启用”前打勾。



4. 日志事件选择默认即可，只开启管理事件；有个有需要也可以把数据事件和 insight 事件打开，这样对应的费用也会有所增加。





5. 点击确认，即可完成创建。

名称	主区域	多区域跟踪	Insights	S3 存储桶	日志文件前缀	CloudWatch Logs 日志组	状态
CloudTrail_mtls	中国 (宁夏)	是	已启用	bucker-for-centric-log-audit-mtls			日志

5.2 审计跟踪结果

1. 用审计员账号登录 S3 控制台，就可以看到上节创建好的跟踪日志。

名称	类型	上次修改时间	大小	存储类
CloudTrail-Digest/	文件夹	-	-	-
CloudTrail/	文件夹	-	-	-

6 四层网络访问控制

6.1 虚拟私有网络 VPC

等保三级需要双可用区的高可用，具体参考 3.1 章节。

6.2 四层网络访问控制 SG 和 NACL

四层网络的访问控制可以通过安全组 SG 和网络层访问控制 NACL。

安全组充当 EC2 实例的虚拟防火墙，用于控制传入和传出流量。入站规则控制传入到实例的流量，出站规则控制从实例传出的流量。

网络访问控制列表 (ACL) 在子网级别允许或拒绝特定的入站或出站流量。您可以使用 VPC 的默认网络 ACL，也可以为 VPC 创建自定义网络 ACL，使其规则与您安全组的规则相似，以便为您的 VPC 添加额外安全层。

安全组的帮助文档：

https://docs.aws.amazon.com/zh_cn/vpc/latest/userguide/vpc-security-groups.html

NACL 的帮助文档：

https://docs.aws.amazon.com/zh_cn/vpc/latest/userguide/vpc-network-acls.html

SG 和 NACL 配置的最佳实践：

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

NACL 配置指导：

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-examples>

NACL 可实现针对端口级别的控制，log4j 的示例：

Customers may be able to use [Network Access Control List rules](#) (NACLs) to block some of the known log4j-related outbound ports to help limit further compromise of successfully exploited systems. We recommend customers consider blocking ports 1389, 1388, 1234, 12344, 9999, 8085, 1343 outbound.

6.3 网络 IDS GuardDuty

GuardDuty 是亚马逊云科技提供的偏向网络和云环境的威胁检测服务。可以对应到等保的网络边界安全的入侵检测 IDS 功能。

6.3.1 启用 GuardDuty

- 在亚马逊云科技管理控制台导航到 GuardDuty 产品，然后开启服务，有 1 个月的免费使用期



2. 启用服务



- 然后即可，不需要再做什么配置了。GuardDuty 是全托管服务，如果发现异常，会在“结果”列表页有展示，并自动同步到 SecurityHub 服务中。



6.3.2 GuardDuty PoC

如果为了验证 GuardDuty 的产品能力，或者给测评机构提供一些截图记录，可以通过官方提供的 PoC 方法来进行演示。

1 场景说明

参考如下亚马逊云科技官方提供的 GuradDuty 能力测试方法，创建 Linux 和 Windows EC2 各一台，然后在一台其他 EC2 上执行如下命令，即可看到 GuardDuty 检测的 findings 及详细信息。

2 执行步骤

```
# 1 - simulate internal recon and attempted lateral movement
sudo nmap -sT $BASIC_LINUX_TARGET

# 2 - ssh brute force with list of keys found on web
for j in `seq 1 20`; do sudo ./crowbar/crowbar.py -b sshkey -s $BASIC_LINUX_TARGET/32 -U users -k ./compromised_keys; done

# 3 - rdp brute force with known user and list of passwords found on web
echo 'Sending 250 password attempts at the windows server...'
hydra -f -L /home/ec2-user/users -P ./passwords/password_list.txt
rdp://$BASIC_WINDOWS_TARGET

# 4 - CryptoCurrency Activity
curl -s http://pool.minergate.com/dkjdkjdlssajdkljalsskajdkssajkllalkdisalkjdsalkjdlkasj >
/dev/null &
curl -s http://xmr.pool.minergate.com/dhdhjkhdjkhdkhajkhdjskahhjkjhkahdsjkkakjasdhkjahdjk >
/dev/null &
```

5 - DNS Exfiltration

```
dig -f ./domains/queries.txt > /dev/null &
```

6 - Backdoor:EC2/C&CActivity.B!DNS

```
dig GuardDutyC2ActivityB.com any
```

3 查看结果

通过亚马逊云科技 Console 导航到 GuardDuty 页，点击“Findings”，

The screenshot shows the AWS GuardDuty console with the 'Findings' tab selected. A single finding is highlighted in red: 'Backdoor:EC2/C&CActivity.B!DNS'. The table lists various findings with columns for 'Finding type', 'Resource', 'Last seen', and 'Count'. The highlighted finding has a count of 1 and was last seen 21 hours ago.

Finding type	Resource	Last seen	Count
UnauthenticatedAccess EC2/SSH/Unauthorized	Instance: i-077529d975a549911f	1 hour ago	7
UnauthenticatedAccess EC2/PortForward	Instance: i-2302837f35a25a81a	3 hours ago	2
Backdoor:EC2/C&CActivity.B!DNS	Instance: i-077529d975a549911f	3 hours ago	1
CryptoCurrency EC2/IotScan/Unauthorized	Instance: i-077529d975a549911f	4 hours ago	4
Records EC2/PortScan	Instance: i-030829f1f0a801a	4 hours ago	3
Execution EC2/MaliciousFile	EC2Cluster: security/runner/lambda/CloudWatchLogsLambda	21 hours ago	1
Execution EC2/MaliciousFile	Instance: i-030829f1f0a801a	21 hours ago	1
UnauthenticatedAccess EC2/PortForward	Instance: i-077529d975a549911f	21 hours ago	1
UnauthenticatedAccess EC2/PortForward	Instance: i-2302837f35a25a81a	21 hours ago	1
Backdoor:EC2/C&CActivity.B!DNS	Instance: i-077529d975a549911f	21 hours ago	1
CryptoCurrency EC2/IotScan/Unauthorized	Instance: i-030829f1f0a801a	21 hours ago	4
CryptoCurrency EC2/IotScan/Unauthorized	Instance: i-030829f1f0a801a	21 hours ago	2
UnauthenticatedAccess EC2/SSH/Unauthorized	Instance: i-077529d975a549911f	21 hours ago	1
UnauthenticatedAccess EC2/SSH/Unauthorized	Instance: i-277529d975a549911f	21 hours ago	8

点击其中一个 Finding，可以查看详细信息：

The screenshot shows the detailed view of the highlighted finding. The top navigation bar shows 'Backdoor:EC2/C&CActivity.B!DNS' and 'Overview'. The main content area includes sections for 'Overview', 'Malware scan', 'Resource affected', and 'Instance details'. The 'Overview' section provides a summary of the finding, including the resource ID, region, account, creation time, and update time. The 'Malware scan' section shows the scan ID, status, start time, end time, and security status. The 'Resource affected' section identifies the target and instance. The 'Instance details' section provides specific details about the instance, including its ID, type, state, and network information.

Backdoor:EC2/C&CActivity.B!DNS 未分类
AWS实例 i-077529d975a549911f 正在查询一个域名关联于一个 known Command & Control 服务器。

概述

Severity	低级
Region	us-east-1
Cloud	E
Account ID	622393626930544811f
Resource ID	i-077529d975a549911f
Created at	2022-11-02 23:05:46 UTC (4 hours ago)
Updated at	2022-11-02 23:15:01 UTC (2 hours ago)

恶意软件扫描

Scan ID	b625f788a11d84467f1230004fa
完成状态	COMPLETED
启动时间	2022-11-02 23:13:00 UTC
结束时间	2022-11-02 23:13:25 UTC
安全性状态	LOW

受影响的资源

受影响的类型	TARGET
受影响的 ID	i-077529d975a549911f
受影响的类型	实例
受影响的 ID	i-077529d975a549911f

实例详细信息

实例 ID	i-077529d975a549911f
实例类型	t2.micro
实例状态	运行中
网络连接	eni-077529d975a549911f
IP 地址	49.67.72.209.61.197
系统描述	Amazon Linux 3 Kernel 5.10.46-2.0.202006.1.vmls_54_HVM gp
启动时间	2022-11-02 23:13:25 UTC

API 客户端配置

API	aws ec2 describe-instances --filter "Name=instance-id,Values=i-077529d975a549911f"
-----	--

The screenshot shows the AWS GuardDuty console interface. On the left, a sidebar navigation includes 'Findings' (selected), 'Usage', 'Mitigate scans', 'Settings', 'Logs', 'AWS Inspector', 'AWS Firewall', 'AWS Network Firewall', 'Accounts', 'What's new', and 'Partners'. The main area is titled 'Findings' with a sub-section 'Suspicious findings'. It lists several findings with columns for 'Finding type', 'Resource', 'Last seen', and 'Count'. Some findings are expanded to show more details like instance IDs and timestamps. To the right, there are tabs for 'Instance tags', 'Network interfaces', 'Private IP addresses', 'Security groups', 'Actions', 'Actor', and 'Additional information'. The 'Actions' tab is currently selected, showing a single action entry for a Denial of Service (DoS) event. The 'Actor' tab shows the guarddutyactivity role. The 'Additional information' tab shows threat intelligence details for the IP 10.0.11.185.

4 参考资料

亚马逊云科技官网的 GuardDuty 的 POC 测试方法
<https://github.com/awslabs/amazon-guardduty-tester>

6.4 GuardDuty 与 NACL 和 WAF 联动来实现 IPS (可选)

本节可选。

如果需要基于 DuardDuty 的发现结果，自动触发相应的自动化响应，可以与 VPC NACL 和 WAF 联动，以达到 IPS 的效果。具体实现方法可参考如下官方博客内容。

how to use [Amazon GuardDuty](#) to automatically update the [AWS Web Application Firewall](#) Web Access Control Lists (WebACLS) and [VPC Network Access Control Lists](#) (NACLS) in response to GuardDuty findings. After GuardDuty detects a suspicious activity, the solution updates these resources to block communication from the suspicious host while you perform additional investigation and remediation.

<https://aws.amazon.com/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/>

7 七层网络访问控制

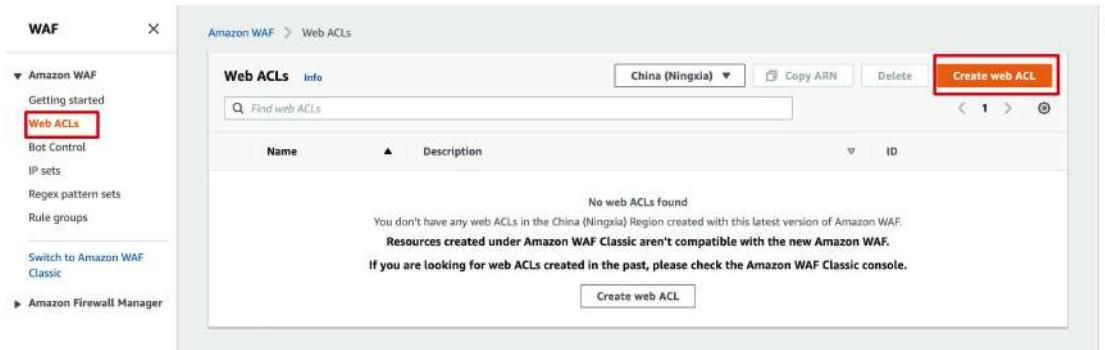
WAF 可以针对七层即 HTTP 层流量进行精细化访问控制，XSS 和 SQLI 等攻击拦截。

具体部署可以参考如下官方博客，亚马逊云科技 WAF 部署小指南(一) WAF 原理、默认部署及日志存储：

<https://aws.amazon.com/cn/blogs/china/aws-waf-deployment-guide-1-waf-principle-default-deployment-and-log-storage/>

7.1 创建 Web ACL

1. 打开 WAF 控制台并导航到 Web ACL 列表页，创建 Web ACL



2. 填写 ACL 名称



3. 添加规则

Amazon WAF > Web ACLs > Create web ACL

Add rules and rule groups

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by 亚马逊云科技. You can also write your own rules and use your own rule groups.

Rules

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

Name	Action
Add managed rule groups	Add my own rules and rule groups

No rules.
You don't have any rules added.

4. 几个免费的托管规则都选上，OS 类型的规则按实际情况选即可

Name	Capacity	Additional fees	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This is useful if you are using third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.	100	No	<input checked="" type="button"/> Add to web ACL <input type="button"/> Edit
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.	25	No	<input checked="" type="button"/> Add to web ACL <input type="button"/> Edit
Anonymous IP list This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to hide out viewers that may be trying to hide their identity from your application.	50	No	<input checked="" type="button"/> Add to web ACL <input type="button"/> Edit

5. 没匹配上规则的默认都放行

1975/1500 WCU

Default web ACL action for requests that don't match any rules

Default action

Allow
 Block

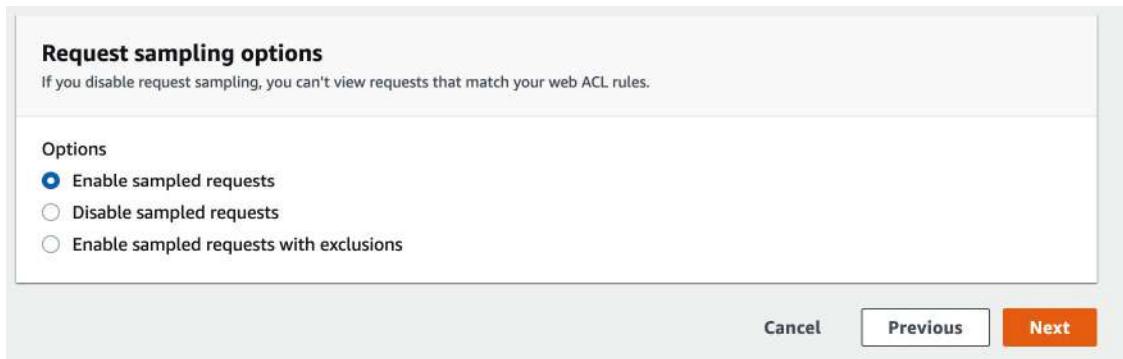
Token domain list - optional

Enable the use of tokens across multiple protected applications by entering the application domains here. Tokens are used by the Challenge and CAPTCHA rule actions, the application integration SDKs, and the ATP and Bot Control managed rule groups. [Learn more](#)

Add token domain
You can add 10 more domains.

Cancel Previous **Next**

6. 允许 sampled 请求



7. 创建好的 ACL

Name	Description	ID
ACL_MLPS	acl for mlps	742bedfa-89d6-468a-98a1-893a4f525198

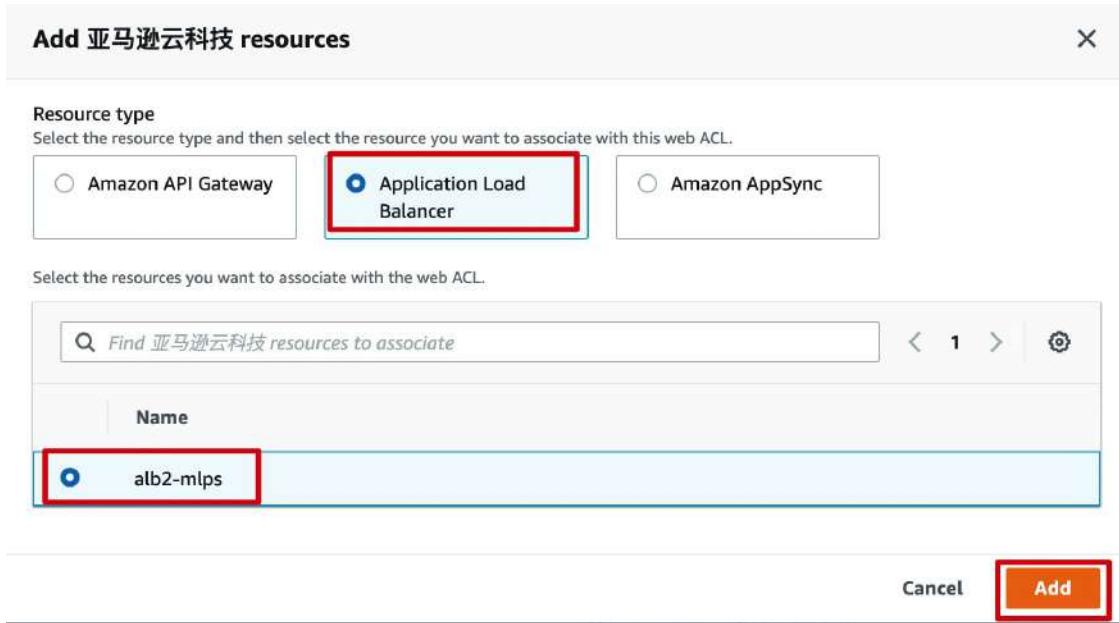
7.2 Web ACL 关联到 ALB

把这个 ACL 关联到我们之前创建好的 ALB 上：

1. 打开刚创建的 ACL，并切换到关联的亚马逊云科技资源的 tab 页，

Name	Resource type	Region
No results There are no results to display		

2. 在资源页，切换到负载均衡 alb，选择之前创建好的 alb 实例



7.3 日志保存在 S3 中

1. 在 S3 中创建一个新 bucket, 名称必须以“aws-waf-logs-”开头, 我们起名 aws-waf-logs-mlps
2. 然后在 WAF 的 ACL 设置中, 开启日志、并保存到新创建的 s3 bucket 中

3. 选择日志保存到 S3, 下拉选择我们创建好的 bucket 名称

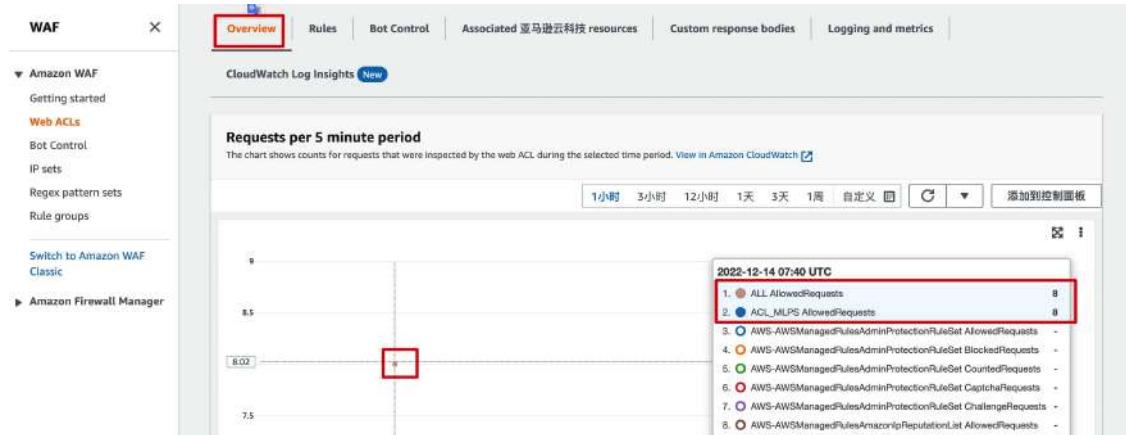
7.4 验证效果

7.4.1 正常 URL

- 先通过正常 url 访问 web 页面，可以正常返回，并在 ACL 里可以看到正常的请求和响应；在 S3 的 WAF bucket 里能看到日志。

<http://alb2-mlps-1585054.cn-northwest-1.elb.amazonaws.com.cn:8088/SamplePage.php>

- 然后查看 ACL 的 overview :



- 在查看 WAF 的 bucket

The screenshot shows the AWS S3 console. On the left, there's a sidebar with '存储桶' (Bucket) selected, followed by '接入点', '对象 Lambda 接入点', '批处理操作', 'S3 的 Access 分析器', '此账户的“阻止公有访问”设置', 'Storage Lens', '控制面板', and 'Amazon Organizations 设置'。The main area shows a file path: 'Amazon S3 > 存储桶 > aws-waf-logs-mlps > AWSLogs/ > 763469878584/ > WAFLogs/ > cn-northwest-1/ > ACL_MLPS/ > 2022/ > 12/ > 14/ > 07/ > 40/ > 763469878584_waflogs_cn-northwest-1_ACL_MLPS_20221214T0740Z_9bec3747.log.gz'.

The file properties are displayed on the right:

- 对象概览**: 拥有者: 8124f50c765406e7ff8a8146574aabe54370a962c4dfe86def55c6eb4801b466; 亚马逊云科技 区域: 中国(宁夏) cn-northwest-1; 上次修改时间: 2022-12-14 07:40:28 UTC.
- S3 URI**: s3://aws-waf-logs-mlps/AWSLogs/763469878584/WAFLogs/cn-northwest-1/ACL_MLPS/2022/12/14/07/40/763469878584_waflogs_cn-northwest-1_ACL_MLPS_20221214T0740Z_9bec3747.log.gz
- Amazon Resource Name (ARN)**: arn:aws:s3::aws-waf-logs-mlps/AWSLogs/763469878584/WAFLog

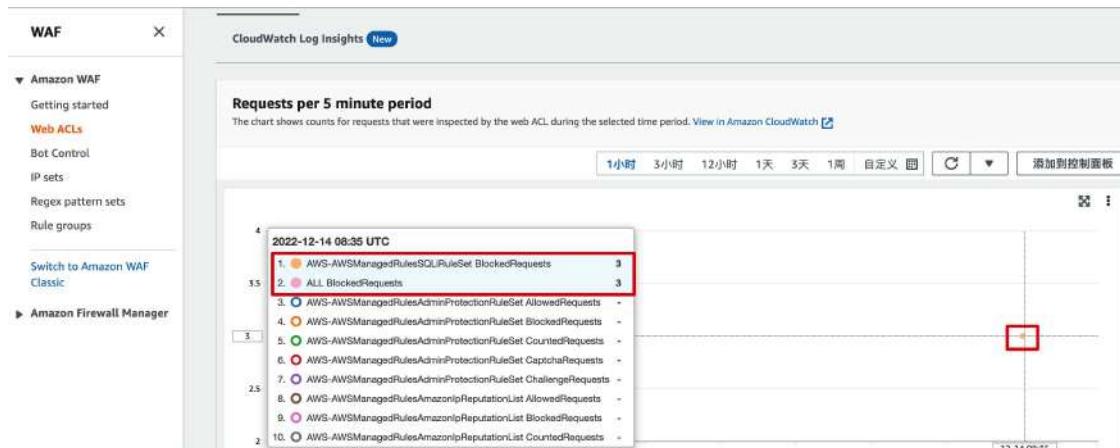
7.4.2 SQL 注入

- 模拟 SQL 注入的请求，会收到阻断响应；alb 的地址换成自己的 alb 地址，端口改成真实的端口：

```
curl --header 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36 Edg/97.0.1072.69' -X POST "alb2-mlps-1585054.cn-northwest-1.elb.amazonaws.com.cn:8088" -F "user='AND 1=1;"
```

- 执行 url 的响应

3. 查看拦截图表



8 安全运维

云服务器 EC2 的运维，可以通过云原生工具亚马逊云科技 System Manager 里的 Session Manager 来实现，也可以通过堡垒机来实现。

等保三级是必选项，等保二级可选。

8.1 Session Manager 方式

亚马逊云科技 System Manager 的 Session Manager 组件，可以实现类似堡垒机的双因子认证、分配权限、运维会话管理及运维日志审计等功能。

使用亚马逊云科技 System Manager，需要在 EC2 上安装 SSM agent。亚马逊云科技部分 AMI 默认是安装了 SSM agent 的，不需要再安装；如果您使用的 AMI 没有自带，需要安装 SSM agent。

可以在如下链接查哪些 AMI 默认支持了 SSM Agent：

<https://docs.aws.amazon.com/systems-manager/latest/userguide/ami-preinstalled-agent.html>

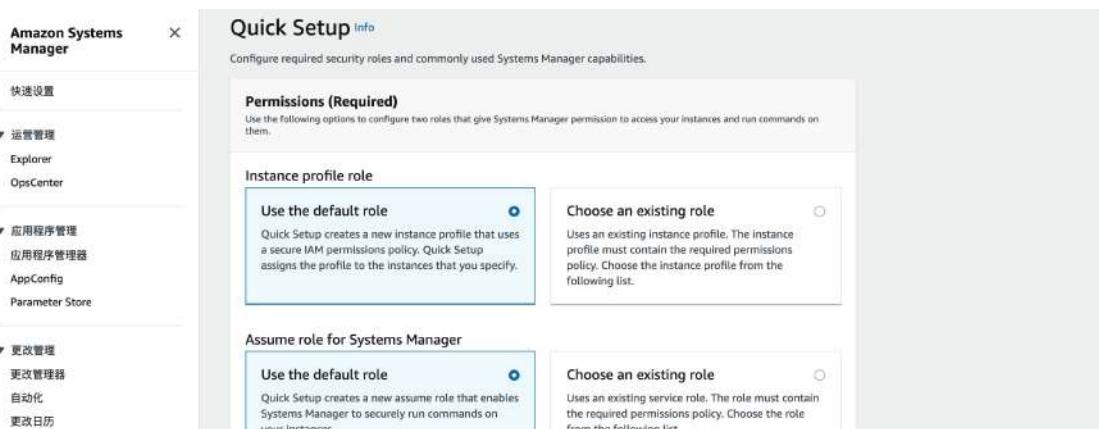
等保中对运维管理（堡垒机）的技术要求项主要包括对运维人员的双因子认证、运维日志记录及审计日志保存 180 天。基于如上要求，Session Manager 经历如下的配置后，可以满足等保的需求。

8.1.1 配置 Systems Managers

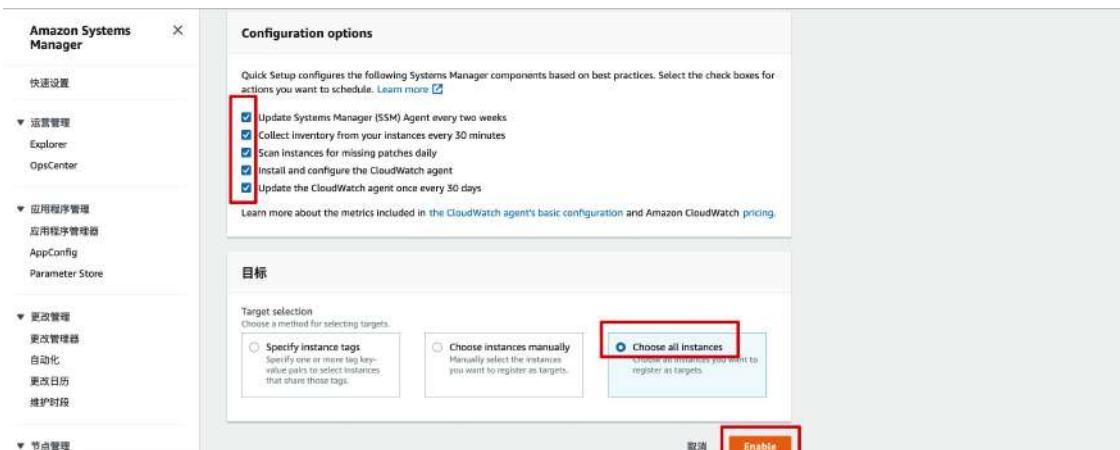
1. 在管理控制台导航到 Systems Manager 控制台，开始配置



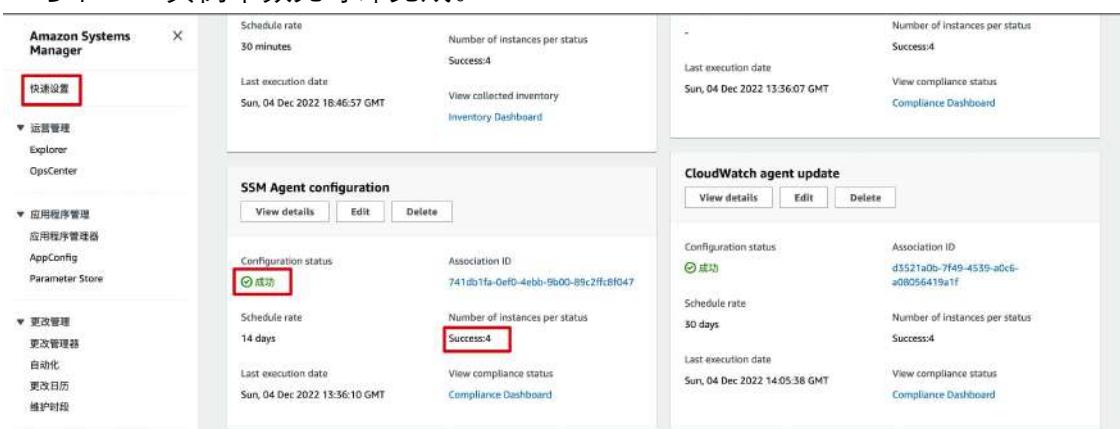
2. permission 选择默认的



3. 配置选项把 SSM agent 和 CloudWatch agent 都安装上，选择所有实例，然后“Enable”



4. 等待快速设置完成，这个时间在几十分钟左右；待 SSM Agent 配置完成的个数与账号下 EC2 实例个数先等即完成。



8.1.2 安装 SSM Agent

- 大部分主流 AMI 自带了 SSM Agent，不需要再安装。已经自带 SSM Agent 的 AMI 列表：https://docs.amazonaws.cn/en_us/systems-manager/latest/userguide/ami-preinstalled-agent.html
- 对于未带 SSM Agent 的 AMI，需要手工安装。如果需要，可以通过如下方案安装：<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-install-ssm-agent.html>
- 已经手工安装过 SSM Agent 的 AMI，可以制作自定义镜像，以后的实例通过自定义镜像来创建，这样免去后续示例手工安装 agent 的工作。

本示例中用的 AMI 都是自带 SSM agent 的，不需要再安装。

8.1.3 Session Manager 配置

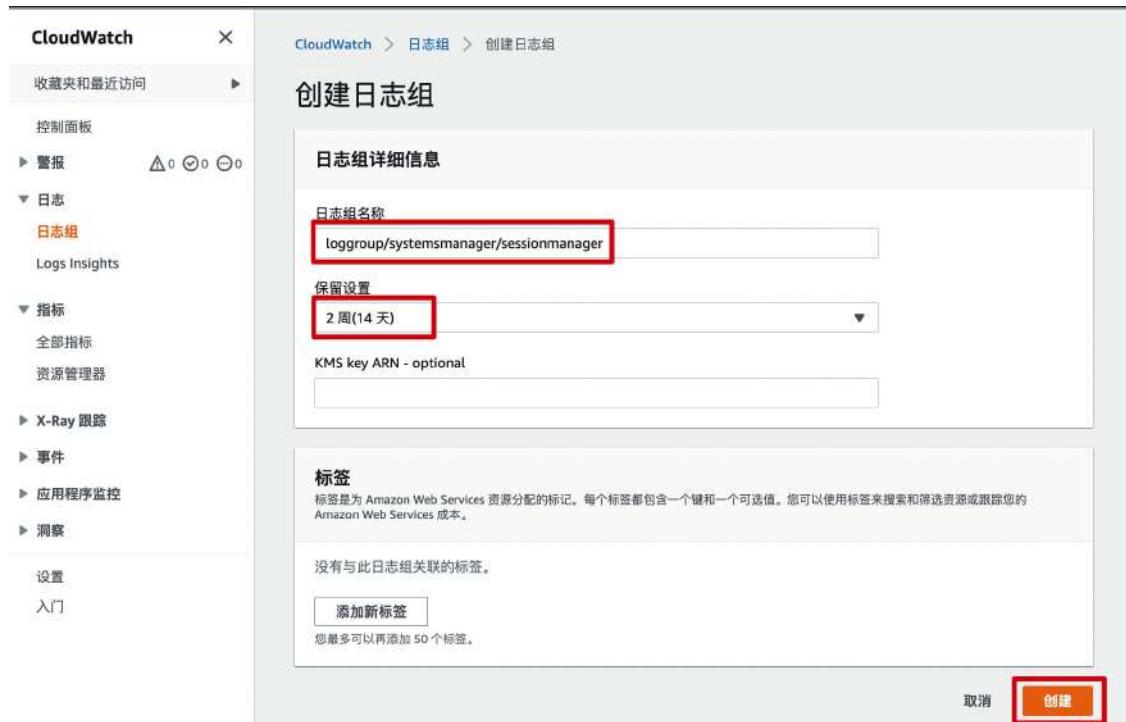
为了便于运维动作的审计，需要把运维操作日志从 Session Manager 中保存到 CloudWatch Logs 中，保存 180 天。

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-logging.html>

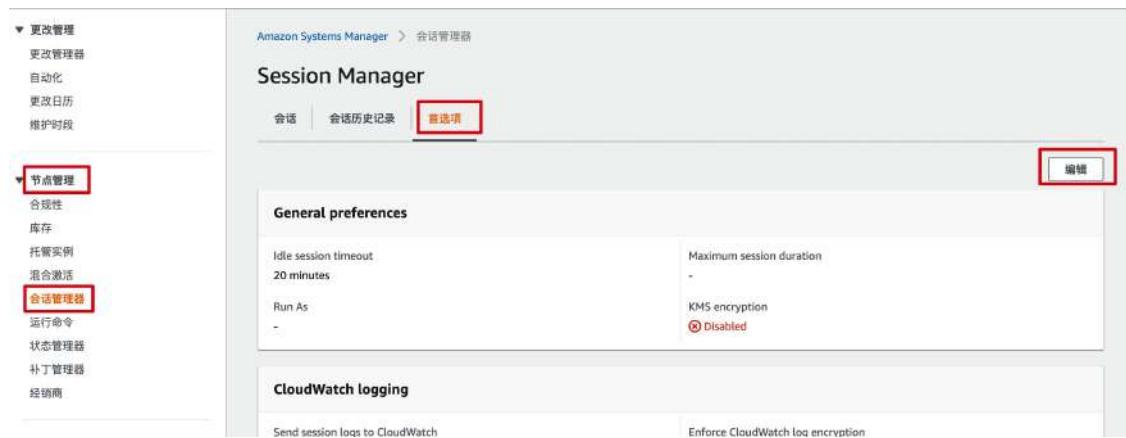
- 创建日志组，在 CloudWatch 控制台导航到日志列表，



- 设置日志组的名称和保存时间



3. 然后开始配置 Session Manager 的配置项。在 Systems Manager 控制台下，节点管理下的会话管理，“首选项”tab 页下点“编辑”



4. 设置会话 idle 状态的超时时间 60 分钟；开启会话的 kms 加密，密钥选择之前创建的密钥。

General preferences

Idle session timeout
Specify the amount of time that a user can be inactive before a session ends. The value must be 1-60 minutes.
60 minutes

Maximum session duration
The maximum duration of a session before it terminates. The duration must be between 1 and 1,440 minutes. Changes to duration apply to new sessions and do not affect active sessions.
 Enable maximum session duration

KMS encryption
You can add Amazon Key Management Service (Amazon KMS) key encryption to the default TLS 1.2 encryption used to protect session data. This data is transmitted between your managed instances and users' local machines. For pricing information, see [Amazon Key Management Service pricing](#).

Enable KMS encryption
KMS key option
 Select a KMS key
 Enter a KMS key ARN
KMS key
alias/kms_mlps

[Create new key](#)

5. 开启 CloudWatch logging

指定会话的操作系统用户
By default, sessions are launched using the credentials of a system-generated ssm-user account. On Linux instances, you can launch sessions using the credentials of an operating system account by tagging an IAM user or role. [IAM 控制台](#)
 为 Linux 实例启用运行方式支持

CloudWatch logging
You can stream or send session logs to a CloudWatch logs log group that you choose, and encrypt log data for all sessions in your account. Session logs should be used for debugging and troubleshooting purposes. [了解详情](#). For pricing information, see [Amazon CloudWatch pricing](#).

Enable
Choose your preferred logging option
 Stream session logs (Recommended)
Session data streams continuously to CloudWatch logs during your sessions. The session data is structured in JSON format.
 Upload session logs
Session data is sent to CloudWatch logs at the end of your session.

6. 日志组不需要加密，选择刚创建好的日志组

Enforce encryption
 Allow only encrypted CloudWatch log groups
CloudWatch 日志组
输入要将会话日志上传到的日志组的名称。
 从列表中选择日志组
 在文本框中输入日志组名称

CloudWatch 日志组

日志组	加密	事件过期时间	指标筛选器	存储的字节
loggroup/systemsmanager/sessionmanager	未加密	2 周 (14 天)	0	0

S3 logging
You can store and encrypt log data for all sessions in your account in an S3 bucket that you choose. Session logs should be used for debugging and troubleshooting purposes. [了解详情](#). For pricing information, see [S3 pricing](#).

Send session logs to S3
 Enable

7. 然后保存即可。

8.1.4 增加 EC2 profile 的权限

因为我们在上节的 Session Manager 的配置中增加了日志保存到 CloudWatch Logs 的选项，那么需要在 EC2 profile 对应的 role (AmazonSSMRoleForInstancesQuickSetup) 中增加 CloudWatch Logs 的权限 (CloudWatchLogsFullAccess)。

同时我们也开启了会话的 kms 加密，所以也需要在这个角色下增加一个内联策略，策略的内容是授权使用 kms。

1. 在 IAM 控制台的角色列表页下，找到 AmazonSSMRoleForInstancesQuickSetup 角色

The screenshot shows the AWS IAM Roles list page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. Under '访问管理' (Access Management), '角色' (Roles) is also selected and highlighted with a red box. The main area lists several roles, with 'AmazonSSMRoleForInstancesQuickSetup' being the one highlighted by a red box.

2. 在这个角色下，添加 CloudWatchLogsFullAccess 权限

The screenshot shows the details of the 'AmazonSSMRoleForInstancesQuickSetup' role. In the top navigation bar, the role name is highlighted with a red box. In the '权限' (Permissions) tab, a policy named 'CloudWatchLogsFullAccess' is listed and highlighted with a red box.

3. 创建内联策略

The screenshot shows the AWS IAM Policies list page. In the top right corner, there's a large red box around the '添加策略' (Add Policy) button. Below it, another red box highlights the '创建内联策略' (Create inline policy) link.

4. 填写权限 kms 使用的权限；这里可以做更细粒度的授权，比如只允许使用具体的 kms key；此处为了演示的简化，没指定具体的 kms key。



```

1. {
2.     "Version": "2012-10-17",
3.     "Statement": [
4.         {
5.             "Effect": "Allow",
6.             "Action": [
7.                 "kms:Encrypt",
8.                 "kms:Decrypt"
9.             ],
10.            "Resource": "*"
11.        }
12.    ]
13. }

```

安全: 0 错误: 0 警告: 0 建议: 0

5. 然后保存

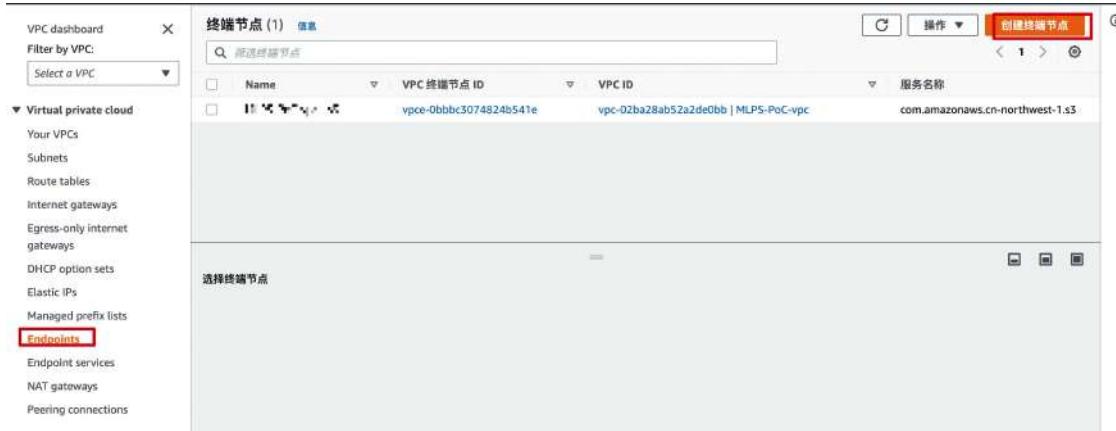


策略名称	类型	描述
AmazonSSMManagedInstanceCore	亚马逊云科技 托管	The policy for Amazon E
CloudWatchLogsFullAccess	亚马逊云科技 托管	Provides full access to C
kmsusage	客户内联	

8.1.5 创建到 Systems Manager 的接入端点

我们想 SSM Agent 通过 privateLink 来访问 Systems Manager 服务，而不是走 Internet，所以需要在 VPC 中创建接入 Systems Manager 服务的 interface endpoint。

1. 在 VPC 控制台的 endpoint 列表页，点击“创建终端节点”

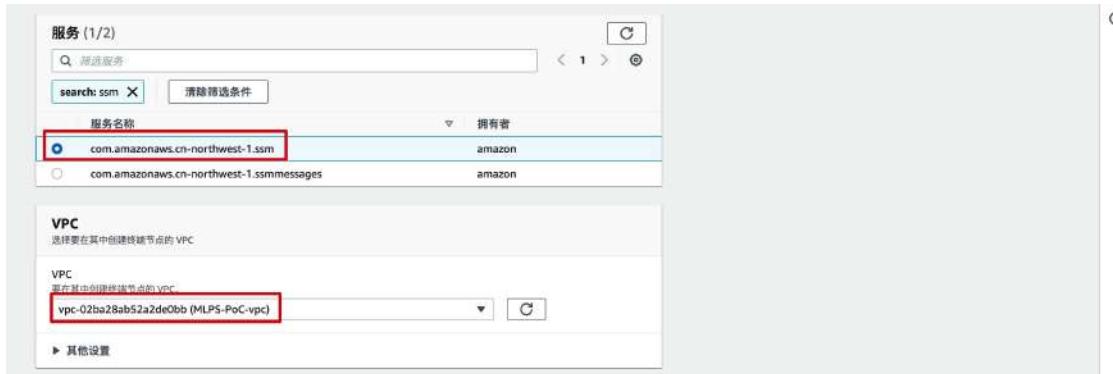


Name	VPC 终端节点 ID	VPC ID	服务名称
vpce-0bbb3074824b541e	vpc-02ba28ab52a2de0bb MLPS-PoC-vpc	com.amazonaws.cn-northwest-1.s3	

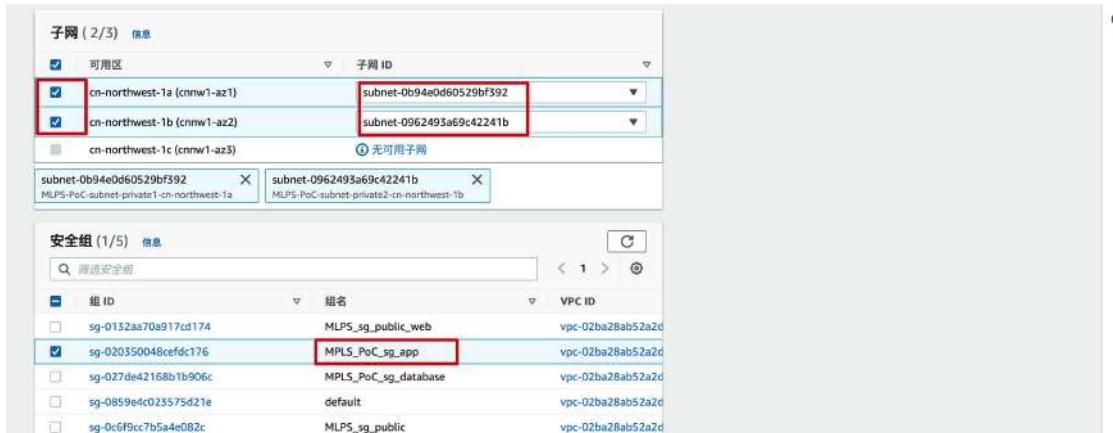
2. 先给 com.amazonaws.region.ssm 服务创建 endpoint, 填写 endpoint 名称, 选择 AWS 服务



3. 选择对应的服务, 和之前创建的 VPC



4. 选择两个 az 的部署 app 的 subnet, 和对应的安全组



5. 策略选择完全访问



6. 然后创建终端节点

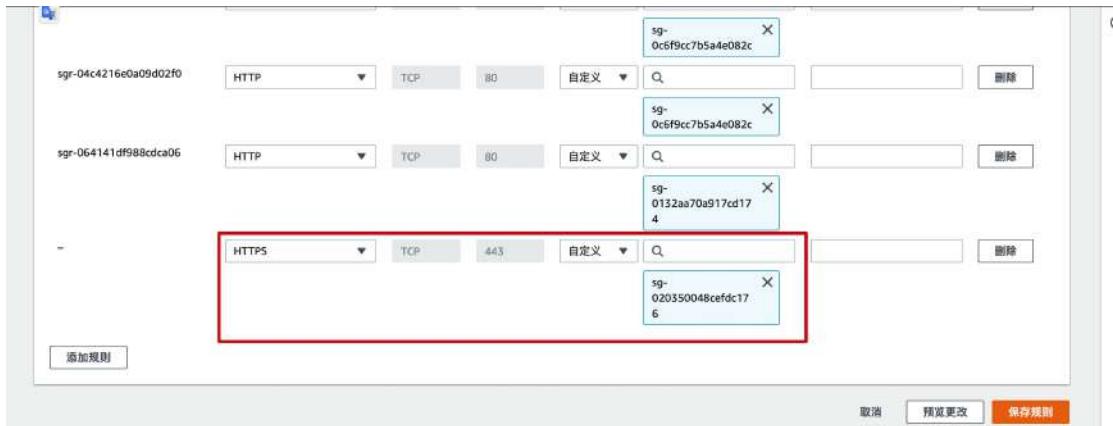


7. 用同样的方式，再创建 com.amazonaws.region.ec2messages、com.amazonaws.region.ssmmessages、com.amazonaws.region.kms、com.amazonaws.region.logs、com.amazonaws.region.ec2 几个 endpoint。

查看已经创建好的 endpoint，状态都是“可用”即可

终端节点 (7) <small>信息</small>						
	Name	VPC 终端...	VPC ID	服务名称	终端节点类型	状态
<input type="checkbox"/>	MPLPS-PoC-vpce-s3	vpce-0bbbc...	vpc-02ba28a...	com.amazonaws.cn-northwest-1.s3	Gateway	可用
<input type="checkbox"/>	MPLPS-PoC-vpce-ssm	vpce-0105c...	vpc-02ba28a...	com.amazonaws.cn-northwest-1.ssm	Interface	可用
<input type="checkbox"/>	MPLPS-PoC-vpce-ec2messages	vpce-041cc4...	vpc-02ba28a...	com.amazonaws.cn-northwest-1.ec2messages	Interface	可用
<input type="checkbox"/>	MPLPS-PoC-vpce-smmessages	vpce-08539...	vpc-02ba28a...	com.amazonaws.cn-northwest-1.smmessages	Interface	可用
<input type="checkbox"/>	MPLPS-PoC-vpce-kms	vpce-08690...	vpc-02ba28a...	com.amazonaws.cn-northwest-1.kms	Interface	可用
<input type="checkbox"/>	MPLPS-PoC-vpce-logs	vpce-00550...	vpc-02ba28a...	com.amazonaws.cn-northwest-1.logs	Interface	可用
<input type="checkbox"/>	MPLPS-PoC-vpce-ec2	vpce-02417...	vpc-02ba28a...	cn.com.amazonaws.cn-northwest-1.ec2	Interface	可用

8. 更新安全组规则：因为我们把 endpoint 放在了 app 所在的安全组里，部署 app 的 EC2 上的 agent 访问 SSM 等亚马逊云科技服务的时候使用的是 443 端口，所以需要在安全组中增加 443 的入站规则，来源是本安全组。



8.1.5 使用 Session Manager 运维 EC2 服务器

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-working-with.html>

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-getting-started.html>

1. 通过管理控制台导航好 system manager 控制台，然后节点管理下的会话管理器，启动会话

2. 选择一台 EC2 示例，然后启动会话，即可以 ssh 登录到 EC2 中；登录的默认账号的 ssm-user。

实例名称	实例 ID	代理版本	实例状态	可用区域	平台
windows2	i-058def963946534c1	3.1.1927.0	正在运行	cn-northwest-1a	Microsoft Windows Server 2019 Datacenter
app2	i-046a37dcda3ff24eb	3.1.1927.0	正在运行	cn-northwest-1a	Amazon Linux
app&mysqlclient	i-0a635650facdbf25f	3.1.1927.0	正在运行	cn-northwest-1b	Amazon Linux
jumpserver	i-05bf6b5ec81c349a3	3.1.1927.0	正在运行	cn-northwest-1a	Amazon Linux

3. ssh 进入到实例后，可以看到会话是加密的。然后执行几个命令，然后终止会话。

```
会话 ID: i-046a37dcda3ff25f
实例 ID: i-046a37dcda3ff25f
This session is encrypted using AWS KMS.

sh-4.2$ pwd
/usr/bin
sh-4.2$ cd -
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ ls
sh-4.2$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
        inet 10.0.141.79 netmask 255.255.240.0 broadcast 10.0.143.255
          inet6 fe80::45:35ff:fe03:e6d6 prefixlen 64 scopeid 0x20<link>
            ether 02:45:35:e3:e6:d6 txqueuelen 1000 (Ethernet)
              RX packets 547371 bytes 227875592 (217.3 MB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 424942 bytes 88198842 (84.1 MB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
              RX packets 0 bytes 0 (0.0 B)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 0 bytes 0 (0.0 B)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

sh-4.2$ ping www.baidu.com
PING www.a.shifen.com (39.156.66.14) 56(84) bytes of data.
64 bytes from 39.156.66.14 (39.156.66.14): icmp_seq=1 ttl=42 time=31.8 ms
64 bytes from 39.156.66.14 (39.156.66.14): icmp_seq=2 ttl=42 time=31.6 ms
^C
--- www.a.shifen.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 100ms
rtt min/avg/max/mdev = 31.647/31.743/31.840/0.202 ms
sh-4.2$
```

8.1.6 查看 CloudWatch Logs 中的运维日志

- 在 CloudWatch 的日志列表页下，点击进入之前创建的 sessionmanager 日志组，可以看到有一个日志流自动创建出来了

The screenshot shows the CloudWatch Logs interface. The left sidebar is collapsed, showing options like '收藏夹和最近访问项', '控制面板', '警报', '日志' (which is selected and highlighted in red), '指标', '全部指标', '资源管理器', 'X-Ray 跟踪', '事件', '应用程序监控', and '消息'. The main area displays the 'loggroup/systemsmanager/sessionmanager' log group details. The top navigation bar includes '操作' (Actions), '在 Logs Insights 中查看' (View in Logs Insights), and a search bar. Below the title, there's a section for '日志流详细信息' (Log Stream Details) with tabs for '日志流' (Log Stream), '指标筛选条件' (Metrics Filter Conditions), '订阅筛选条件' (Subscription Filter Conditions), 'Contributor Insights', and '标签' (Tags). The '日志流' tab is active. It shows one log stream: 'I-0daa4de32004886b8' (highlighted with a red box), with a timestamp of '2022-12-05 03:39:23 (UTC+08:00)'. There are also buttons for '刷新' (Refresh), '删除' (Delete), '创建日志流' (Create Log Stream), and a search bar for 'Search all log streams'.

2. 查看详细的日志事件

3. 可以看到执行 ifconfig 命令的详细日志事件信息

附录参考资料：

最佳实践 : Replacing a Bastion Host with Amazon EC2 Systems Manager :

<https://aws.amazon.com/blogs/mt/replacing-a-bastion-host-with-amazon-ec2-systems-manager/>

限制某个 IAM user 只可以操作具体的 3 个 EC2 实例的示例：

https://docs.aws.amazon.com/systems-manager/latest/userguide/security_iam_id-based-policy-examples.html#security_iam_id-based-policy-examples-view-documents-tags

基于标签控制对 Systems Manager 资源的访问

https://docs.aws.amazon.com/zh_cn/systems-manager/latest/userguide/security_iam_id-based-policy-examples.html#security_iam_id-based-policy-examples-view-documents-tags

8.2 堡垒机方式

安恒基于亚马逊云科技平台实现了半 SaaS 化、按量付费的堡垒机产品，可以通过云市场购买。

https://awsmarketplace.amazonaws.cn/marketplace/pp/prodview-ail6ri54g3qcg?sr=0-2&ref_beagle&applicationId=AWSMPContessa

9 主机安全

主机安全主要包括漏洞扫描、主机端口暴露、恶意软件和病毒查杀、补丁管理、高级威胁检测等。亚马逊云科技在主机安全方面功能拆分在不同的产品服务中，包括 Inspector 的 CVE 漏洞扫描和端口暴露、Patch Manager 的补丁管理、GuardDuty 的恶意软件检测和高级威胁检测等；但亚马逊云科技没有病毒查杀功能。

亚马逊云科技的 Inspector 和 GuardDuty 的恶意软件检测功能在中国区还没有正式发布，预计 2023 年 6 月 30 日发布。

安恒的主机安全 EDR 产品与亚马逊云科技云平台做了深度融合适配，SaaS 模式模式并支持按量付费。

主机安全在等保中是归类在安全计算环境中。在安全计算环境中，除了如上安全内容外，也包括主机和网络实例的监控及 OS 加固等内容，对应参考 8.1 和 8.4 章节内容。

9.1 主机监控与告警

CloudWatch 的 Workshop 参考资料：

<https://catalog.us-east-1.prod.workshops.aws/workshops/a8e9c6a6-0ba9-48a7-a90d-378a440ab8ba/en-US>

每个账号都提供一定免费监控和 Alarms 的额度，具体可以参考定价说明文档。

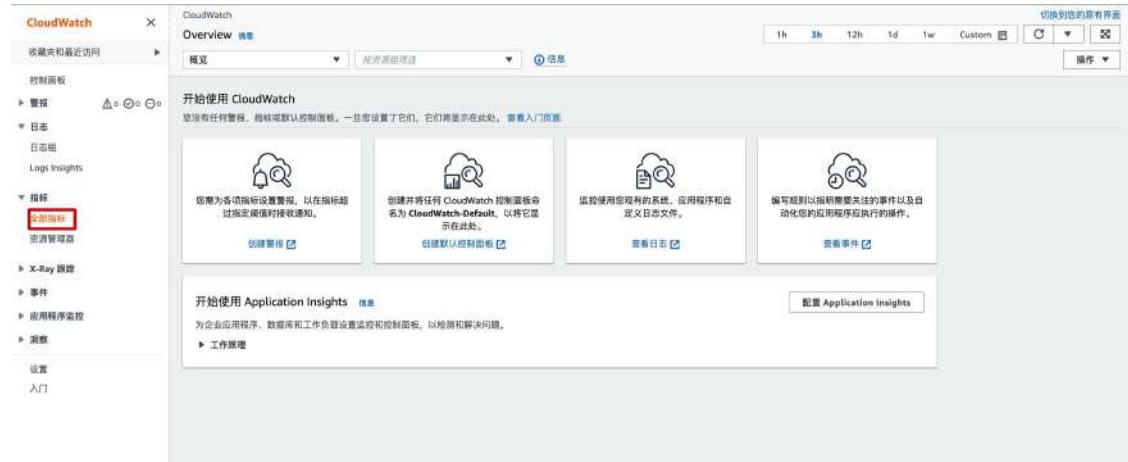
Alarms: 10/month/customer for free. 5000 per region per account.

API requests: 1,000,000/month/customer for free.

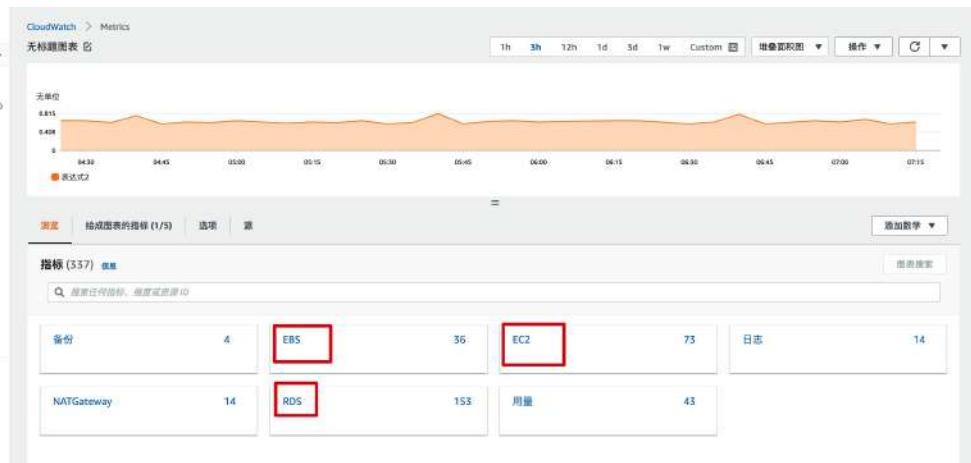
Amazon SNS email notifications: 1,000/month/customer for free.

CloudWatch 的 Metrics（监控指标）默认支持了常用的云资源的监控指控，包括 EC2、EB2 和 RDS 等。

通过亚马逊云科技管理控制台，找到 CloudWatch 服务；然后点击“指标”下的“全部指标”，



然后可以看到系统默认支持的各种资源：



9.2 安恒主机安全 EDR

安恒的 EDR SaaS 版，后端服务部署在亚马逊云科技中国区；可通过云市场开通使用：
https://awsmarketplace.amazonaws.cn/marketplace/pp/prodview-53manr4dkevwo?sr=0-7&ref_=beagle&applicationId=AWSMPContessa

9.3 亚马逊云科技主机安全服务

9.3.1 CVE 漏洞检测 Inspector

中国区未发布。

9.3.2 恶意软件检测 GuardDuty Malware Detection

中国区未发布。

亚马逊云科技官方 POC 测试（Global Region）：
<https://github.com/awslabs/amazon-guardduty-tester>

9.3.3 补丁管理 Patch Manager

How do I create VPC endpoints so that I can use Systems Manager to manage private EC2 instances without internet access

https://aws.amazon.com/premiumsupport/knowledge-center/ec2-systems-manager-vpc-endpoints/?nc1=h_ls

9.4 OS 加固

OS 加固，这部分可以参考如下资料进行，主要设计 OS 的账号及权限等内容。

<http://etutorials.org/Linux+systems/secure+linux-based+servers/Chapter+3.+Hardening+Linux/Section+3.1.+OS+Hardening+Principles/>

10 数据安全

10.1 敏感数据加密

等保中对数据库中的敏感数据有明确的加密保护要求，最常用的做法是把 RDS 数据库的整盘进行加密。如果是新创建的数据库，可以在创建过程的配置参数中设置整盘加密；如果是已有的未加密的 RDS 数据库，可以通过给数据库创建快照、复制快照并加密、然后从快照恢复数据库的方式来加密数据库。可参考如下亚马逊云科技官方的 hands on 实操文档，加密一个未加密 RDS 数据库的方法：

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

对于 EC2 的数据库 EBS 和 S3 的数据加密，等保中没有强制要求；如果需要可以参考如下实操文档，使用 KMS 对 RDS、S3 和 EBS 加密的 workshop：

<https://catalog.us-east-1.prod.workshops.aws/workshops/aad9ff1e-b607-45bc-893f-121ea5224f24/en-US>

10.2 RDS 密钥轮转（可选）

亚马逊云科技 Secret Manager 支持密钥的自动轮转，相关方法论的参考资料：

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/manage-credentials-using-aws-secrets-manager.html>

如果您使用 RDS 的时候使用了 RDS Proxy，那么使用 Secret Manager 是必选项。

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-proxy.html>

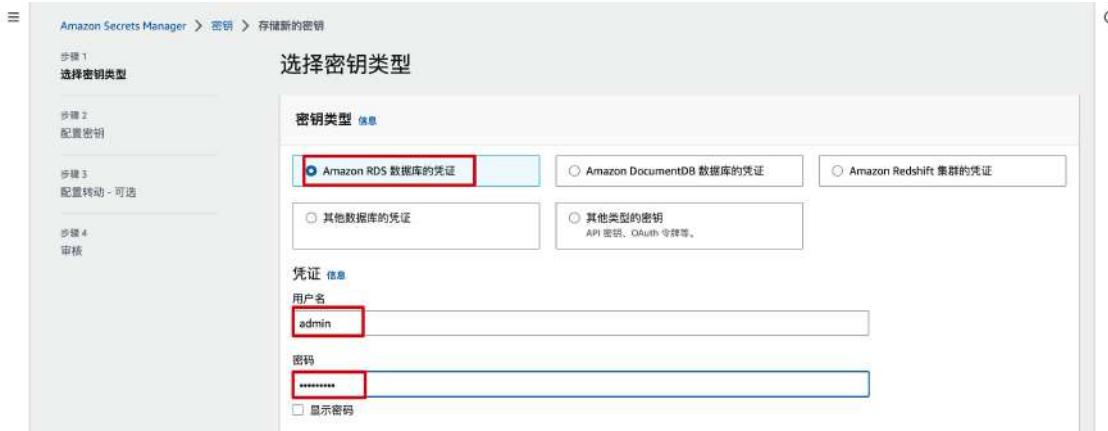
数据库密钥论证是测评项之一，不是高风险项。

10.2.1 创建密钥

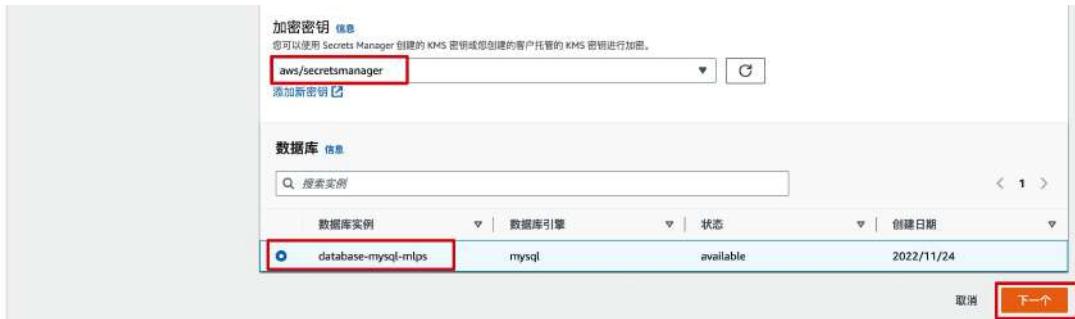
1. 通过控制台导航到 Secrets Manager 控制台的密钥列表页，开始创建新的密钥



2. 选择 RDS 数据库的凭据，输入数据库的用户名和密码



3. 加密密钥选择系统提供的默认的密钥，因为这个密钥是免费使用的；选择之前创建的数据库实例



4. 填写密钥名称



5. 设置开启自动轮转，每 11 个月轮转一次



6. 创建轮转的 lambda 函数



7. 然后确认即可，在密钥列表页可以看到刚创建好的密钥



10.2.2 使用密钥

在具体的应用中，可以使用任何编程语言的亚马逊云科技 SDK 的 GetSecretValue 来获取密钥。然而，我们推荐使用客户端的缓存机制来缓存密钥，这样可以提高速度和降低成本。

连接数据库的缓存方法可以参考如下链接：

https://docs.aws.amazon.com/secretsmanager/latest/userguide/retrieving-secrets_jdbc.html

10.3 网站 HTTPS

域名使用证书，证书可以托管在 ACM 服务中。

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/SSL-on-amazon-linux-ami.html>

10.3.1 申请证书

1. 在 ACM 控制台，请求申请证书



2. 填写域名

Amazon Certificate Manager > 证书 > 请求公有证书

请求公有证书

域名
为您的证书提供一个或多个域名。

完全限定域名 信息

为此证书添加另一个名称
您可以向此证书添加其他名称。例如，如果要请求“www.example.com”的证书，您可能需要添加名称“example.com”，以便客户可以通过任一名称访问您的站点。

验证方法 信息
选择验证此所有权的方法。

DNS 验证 - 推荐
如果尚未完成或无法修改证书请求中指定的 DNS 配置，请选择此选项。

电子邮件验证
如果尚未完成或无法获得修改证书请求中指定的 DNS 配置的权限，请选择此选项。



3. 查看证书



此时的证书处于“待验证”状态，需要验证。



我们申请证书的时候选择的是通过 DNS 解析验证，也就是 ACM 给这个申请创建来一个 CNAME 的名称和记录，我们把这个信息在自己的域名解析系统中创建一个 CNAME 解析记录，然后 ACM 会自动验证解析结果。

4. 找到 CNAME 名称和值，然后拷贝下来

Amazon Certificate Manager (ACM)

域 (1)

域	状态	续订状态	类型	CNAME 名称	CNAME 值
awsliyangln.com	-	-	CNAME	_d1d4a3f0a053b6c91ff64213f759391.awsliyangln.com	_0ab4f6320bb620a62b7ea0f7257e7677.cgcvtb.acm-validation.s.amazonaws.cn

详细信息

使用中 否	序列号 0dc1ae554f20:f0:a8:e0:b8:35.cc:61:1:dad:7a	请求时间 十二月 04, 2022, 11:41:31 (UTC+08:00)	续订资格 不符合条件
域名 awsliyangln.com	公钥信息 RSA 2048	颁发时间 十二月 04, 2022, 11:46:05 (UTC+08:00)	
其他名称的数量			

验证域所有权

在 Amazon 证书颁发机构(CA)为您的站点颁发证书之前, Amazon Certificate Manager (ACM) 必须证明您对请求中指定的所有域名具有所有权或控制权。您可以选择在请求证书时通过域名系统(DNS)验证或电子邮件验证来证明自己的所有权。验证仅适用于 ACM 颁发的公有信任证书。对于导入的证书或私有 CA 签名的证书, ACM 不对其域所有权进行验证。

了解更多信息

5. 在域名解析系统中创建 CNAME 记录

域名解析

解析设置

解析设置 awsliyangln.com

解析记录列表

主机记录	记录类型	解析请求来源	记录值	TTL	状态	备注	操作
_d1d4a3f0a053b6c91ff64213f759391	CNAME	默认	_0ab4f6320bb620a62b7ea0f7257e7677.cgcvtb.acm-validation.s.amazonaws.cn	10 分钟	正常		修改 暂停 删除 备注 生效检测

6. 过几分钟，可以在 ACM 控制台上看到我们申请的证书已经是“已颁发”状态

Amazon Certificate Manager (ACM)

证书 (2)

证书 ID	域名	类型	状态	使用中	续订资格
ccf05066-82ee-4c93-96a5-18db5497a83f	*.awsliyangln.com	Amazon 已颁发	已颁发	否	不符合条件

10.3.2 配置 HTTPS 访问

1. 在 EC2 控制台的 ALB 列表页，找到之前创建的 alb 示例

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Target Groups

EC2 > 负载均衡器

负载均衡器 (1)

名称	DNS 名称	状态	VPC ID	可用区	类型
alb-mpls	alb-mlps-388779185.cn-northwest-1.elb.amazonaws.com.cn	Active	vpc-02ba28ab52a2de0bb	2 可用区	application

2. 新添加一个 HTTPS 监听器

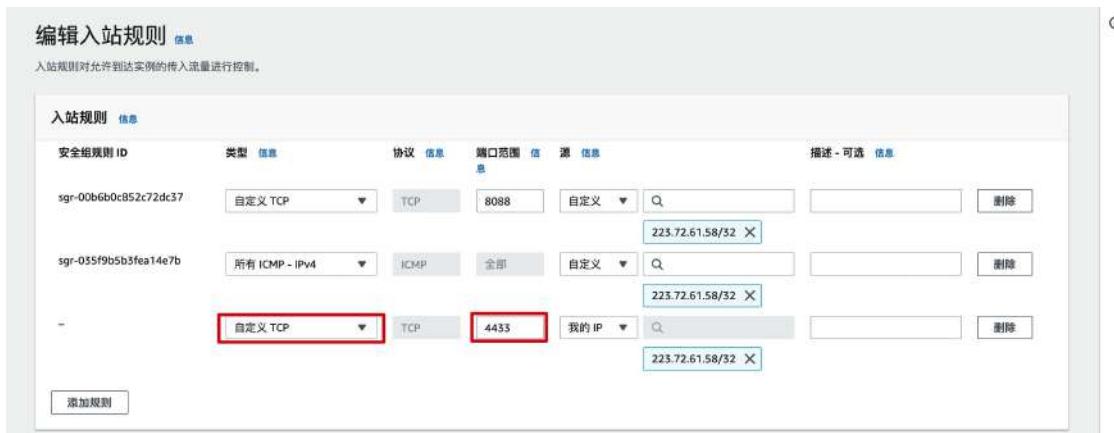
3. 协议选择 HTTPS，端口填 4433；默认端口是 443，因为需要备案才能打开，所以演示的时候使用 4433，正常生产环境请使用 443.

4. 默认操作选择“转发至”之前创建的目标组

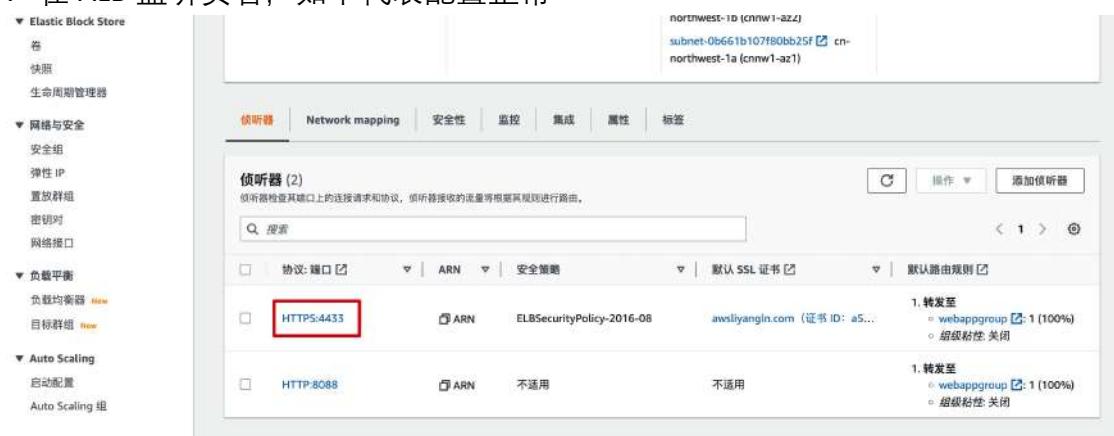
5. 安全策略选择默认的，证书选择上一节在 ACM 中创建好的证书；然后点击“添加”按钮



6. 在 ALB 所在的安全组中，增加一个入职规则；生产环境直接添加 HTTPS（443）即可；我们这演示添加的是 443 端口



7. 在 ALB 监听页看，如下代表配置正常



10.3.3 验证 HTTPS 访问

通过 https 协议来访问 web 站点

<https://web.awsliyangIn.com:4433/SamplePage.php>

The screenshot shows a web browser window with the URL <https://web.awsliyangIn.com:4433/SamplePage.php> in the address bar. The page title is "Sample page". Below the title, there are two input fields: "NAME" and "ADDRESS", each with a dropdown arrow icon. To the right of these fields is a button labeled "Add Data". Below the input fields is a table with three rows:

ID	NAME	ADDRESS
1	zhang san1	beijing1
2	li si1	tianjin1
3	wang wu	shanghai

10.4 网页防篡改

1. 容器环境网页防篡改：https://docs.bridgecrew.io/docs/bc_k8s_21
2. EC2 环境网页防篡改：

<https://aws.amazon.com/premiumsupport/knowledge-center/efs-enable-read-write-access/>

The following are two common issues that prevent you from writing to your file system:

- The mount option in the /etc/fstab file is set to read-only access.
- The associated AWS Identity and Access Management (IAM) policy indicates read-only access, or root access disabled.

Example 2: Grant read-only access:<https://docs.aws.amazon.com/efs/latest/ug/iam-access-control-nfs-efs.html>

11 数据库审计

RDS 数据库日志审计，可以通过开启数据库日志并保存到 CloudWatch Logs 中。日志在 CloudWatch Logs 中设置保持 7 天，用于日常排查问题使用（可以按自己实际需要调整，比如 2 天或 14 天等都可以）。日志从 CloudWatch Logs 中导出到 S3 中，设置保存 180 天，确保要求日志至少保留半年。日志如果不想从 CloudWatch Logs 导出到 S3，直接在 CloudWatch Logs 中保持 180 天也是可以的，只是价格略有不同。

RDS 日志默认只开通了 error 日志，审计日志需要通过开启配置来自行打开；不同数据库引擎开启审计日志的方式有所不同。

11.1 开启审计日志配置

11.1.1 RDS MySQL

开启 mysql 的 audit log 参考文档：

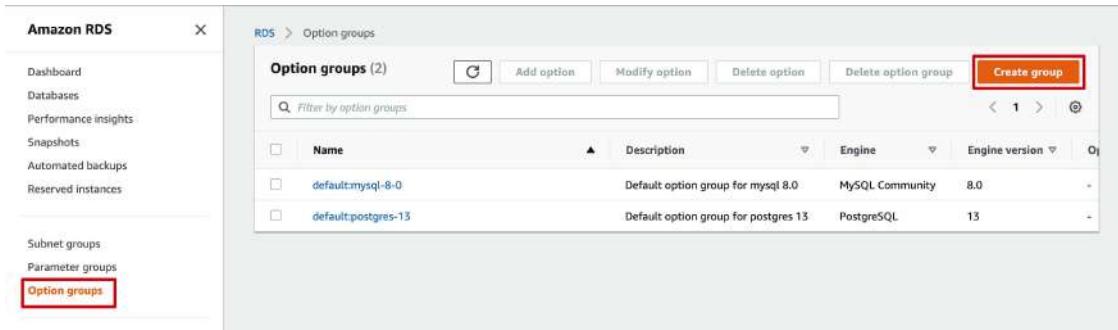
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.MySQL.Options.AuditPlugin.html>

RDS MySQL 数据库的审计日志依赖于 MariaDB Audit Plugin 插件。MariaDB Audit Plugin 插件可以通过 RDS 的 Option groups。所以我们先在 RDS 控制台的 Option group 中打开这个插件，然后再在下节中配置 RDS 输出审计日志到 CloudWatch Logs。

11.1.1.1 创建 Option group

在管理控制台导航到 RDS 控制台的 Option groups 列表页。我们创建一个新的 Option group。

1. 创建一个新的 Option group



The screenshot shows the AWS RDS console with the 'Option groups' page open. On the left sidebar, the 'Option groups' link is highlighted with a red box. The main area displays a table of existing option groups:

Name	Description	Engine	Engine version
default:mysql-8-0	Default option group for mysql 8.0	MySQL Community	8.0
default:postgres-13	Default option group for postgres 13	PostgreSQL	13

A red box highlights the 'Create group' button at the top right of the table header.

2. 设置 Option group 的名称和各种参数

Amazon RDS

RDS > Option groups > Create

Create option group

Option group details Info

Name	mlps-mysql-8-0
Description	This Option group is used for mlps
Engine	mysql
Major Engine Version	8.0

Cancel **Create**

3. 编辑刚创建的 Option group

Amazon RDS

RDS > Option groups

Option groups (3)

Name	Description	Engine	Engine version	Options
default:mysql-8-0	Default option group for mysql 8.0	MySQL Community	8.0	-
default:postgres-13	Default option group for postgres 13	PostgreSQL	13	-
mlps-mysql-8-0	This Option group is used for mlps	MySQL Community	8.0	-

4. add Option

Amazon RDS

RDS > Option groups

Options

Name	Persistent	Permanent	Port	Security groups	Version	Settings
No Options found						

Add option

Tags (0)

Tags	Value
You don't have any tags associated with this resource.	

Add tags

5. 选择审计插件

Amazon RDS

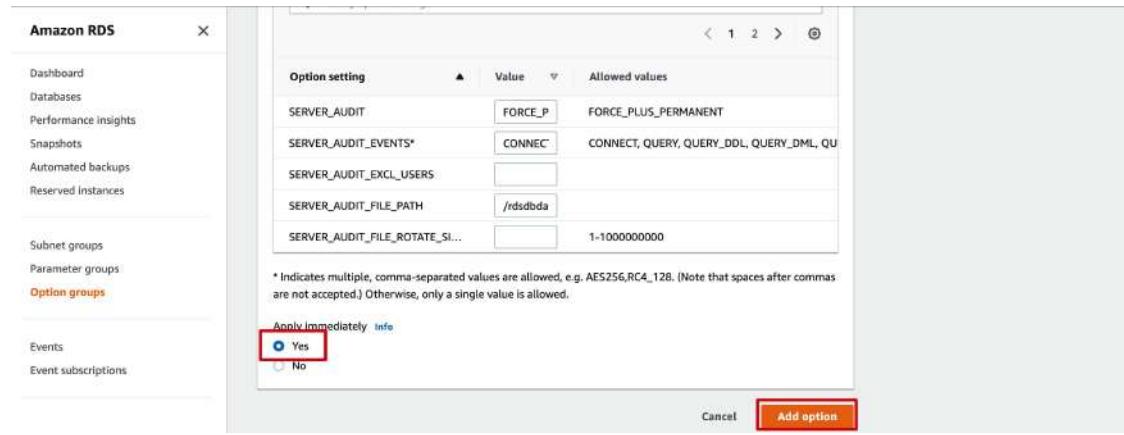
RDS > Option groups > Add option

Add option

Option details

Option group name	mlps-mysql-8-0
Option name	Info
Choose the option that you want to add to this group.	
MARIADB_AUDIT_PLUGIN	

6. option settings 参数默认，勾选立即应用

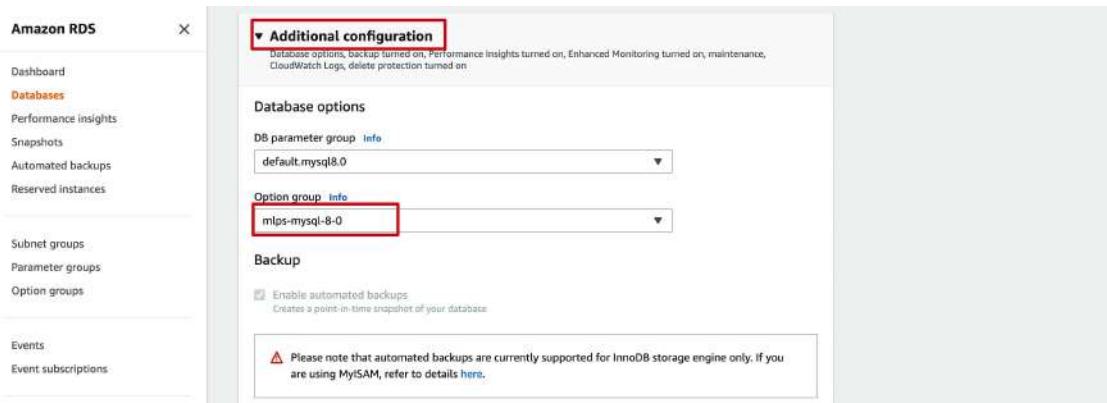


11.1.1.2 RDS 更换 Option group

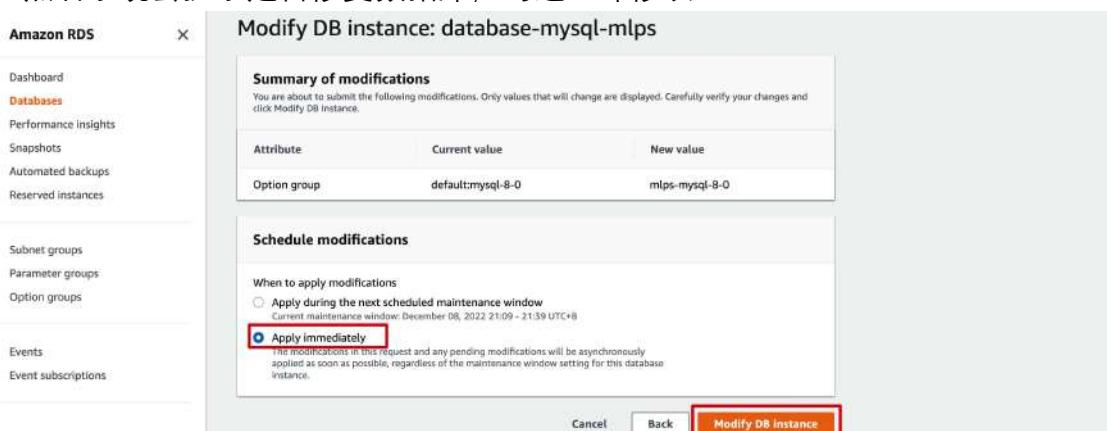
1. 在 Databases 列表页，找到我们的 MySQL 数据库

2. 点击“Modify”按钮

3. 到 additionally configuration 配置项上，选择我们上一节创建的 Option group，替换掉 default Option group。



4. 然后系统会提示是否修复数据库，勾选立即修改



11.1.2 RDS PostgreSQL

开启 PG 的审计日志模块， Using pgAudit to log database activity

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.PostgreSQL.CommonDBATasks.Extensions.html#Appendix.PostgreSQL.CommonDBATasks.pgaudit>

数据库审计功能使用 pgaudit 请参考这个操作指导：

<https://aws.amazon.com/cn/premiumsupport/knowledge-center/rds-postgresql-pgaudit/>

11.1.3 DynamoDB

DynamoDB 的管理事件日志和数据事件日志，都可以通过配置来保存到 CloudTrail 里，进而备份到 S3 中进行集中审计。

- DynamoDB 的管理事件日志，在创建 CloudTrail 的跟踪时，只要开启的整体的管理事件，即可开通，不需要单独配置。

- DynamoDB 的数据事件日志，在创建 CloudTrail 的跟踪时，需要在开启数据事件且单独勾选上 DynamoDB 的数据事件才可以。

具体参考帮助文档：

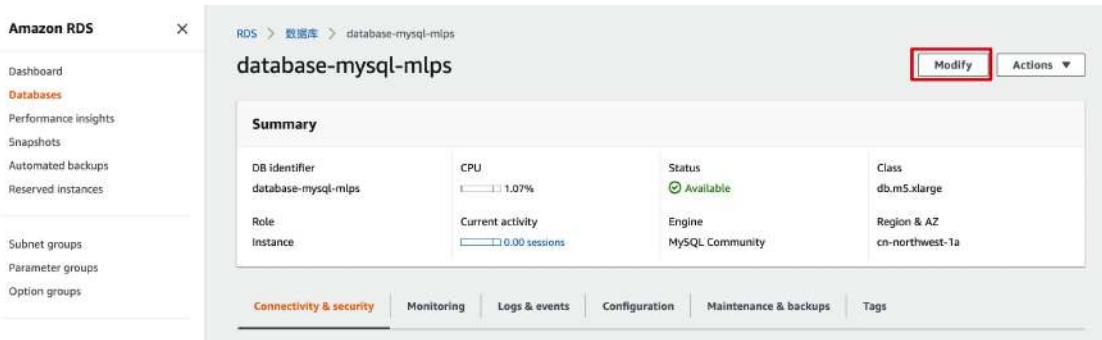
https://docs.amazonaws.cn/en_us/amazondynamodb/latest/developerguide/logging-using-cloudtrail.html

11.2 日志发送到 CloudWatch Logs

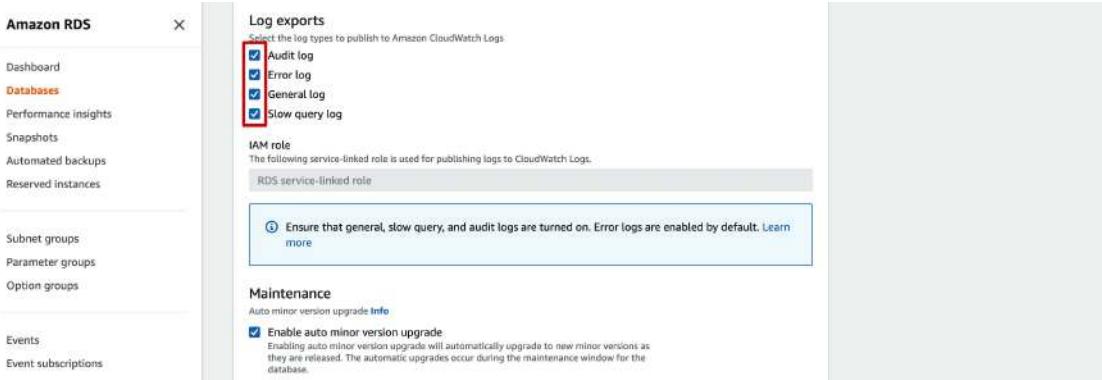
将数据库日志发布到 Amazon CloudWatch Logs：

https://docs.amazonaws.cn/AmazonRDS/latest/UserGuide/USER_LogAccess.Procedural.Upload.toCloudWatch.html

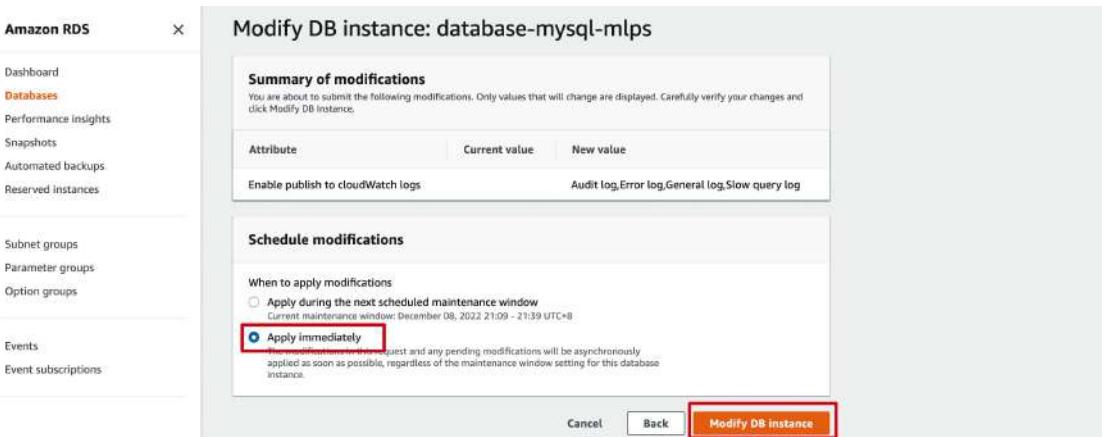
1. 修改数据库实例的配置，打开各种日志



2. 勾选上 log export 的 4 个选项



3. 然后选立即应用即可



11.3 验证效果

11.3.1 造数据库日志

1. 访问我们之前搭建的网站，这样可以造出数据库的读取日志

<https://web.awsliyangln.com:4433/SamplePage.php>

← → ⌂ 🔒 web.awsliyangln.com:4433/SamplePage.php

Sample page

NAME	ADDRESS
<input type="text"/>	<input type="text"/>

ID	NAME	ADDRESS
1	zhang san1	beijing1
2	li si1	tianjin1
3	wang wu	shanghai

2. 插入几条数据，这样可以造出写入数据库的日志

← → ⌂ 🔒 web.awsliyangln.com:4433/SamplePage.php

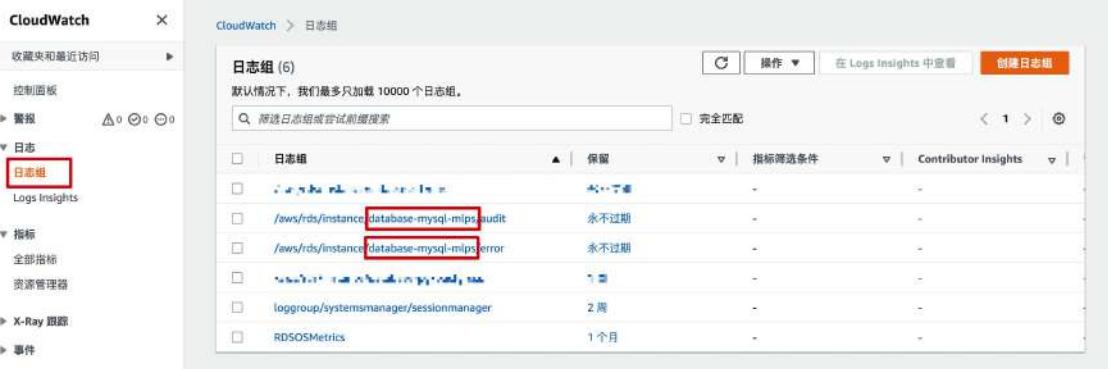
Sample page

NAME	ADDRESS
wang er	tianjin2

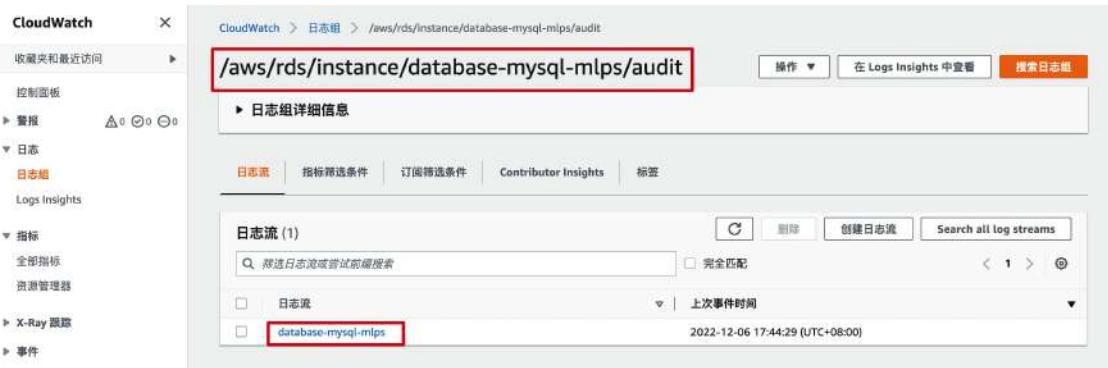
ID	NAME	ADDRESS
1	zhang san1	beijing1
2	li si1	tianjin1
3	wang wu	shanghai
4		

11.3.2 在 CloudWatch Logs 中查看日志

1. 管理控制台导航到 CloudWatch 下的日志组列表页，可以看到我们的数据库实例的 2 个日志组。刚更新完数据库实例的 Option Group 后需要等几分钟。



- 进入 audit 日志组，可以看到对应我们 RDS 实例的日志流，进去可以看具体的日志了；可以进行各种筛选动作。



- ### 3. 查看日志详细内容



12 云安全中心

对于云环境中的各种安全设备（也叫安全产品、安全服务），默认都是同一控制台 Console 的。Security Hub 作为云上的安全中心，支持各安全产品的安全事件 (findings) 的统一管理，各安全产品都支持一键配置同步 findings 到 Security Hub 服务中。

12.1 统一管理安全事件

在 Security Hub 中统一管理云上的安全事件；Security Hub 支持一键开启 enable：
<https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-settingup.html>

如下示例说明 GuardDuty 与 Security Hub 的集成，即把安全检测结果 findings 发送到 Security Hub 中。

12.1.1 开通 Config 服务

Security Hub 服务依赖 Config 服务，所以在开通 Secret Hub 服务之前，先开通 Config 服务。

1. 通过亚马逊云科技管理控制台，导航到 Config 服务控制台；



2. 设置配置选项

设置 Amazon Config

步骤 1: 设置

步骤 2: 规则
步骤 3: 审核

设置

指定希望 Amazon Config 记录的亚马逊云科技 资源类型、要将文件发送到的 Amazon S3 存储桶，以及要将通知发送到的 Amazon SNS 主题。请在开始之前查看定价页面。

要记录的资源类型

选择您希望 Amazon Config 记录其配置更改的资源的类型。默认情况下，Amazon Config 会记录所有受支持资源的配置更改。您还可以选择记录此区域中支持的全局资源的配置更改。

包含此区域中支持的所有资源

包含全局资源 (例如 Amazon IAM 资源) ?

Amazon S3 存储桶*

您的存储桶将接收配置历史记录和配置快照文件，其中包含 Amazon Config 记录的资源的详细信息。

创建存储桶

从您的账户选择一个存储桶

从另一账户选择存储桶 ?

存储桶名称* config-bucket-763469878584 / 前缀 (可选) / AWSLogs/763469878584/Config/cn-northwest-1

Amazon SNS 主题

将配置更改和通知流式传输到 Amazon SNS 主题。

Amazon Config 角色*

向 Amazon Config 授予对您的亚马逊云科技 资源的只读访问权限，以便它记录配置信息；并向 Amazon Config 授予将此信息发送到 Amazon S3 和 Amazon SNS 的权限。

创建 Amazon Config 服务相关角色

从您的账户选择一个角色

3. 设置规则，选择默认即可，即不选择 config 规则；具体规则在 Security Hub 里选择。

设置 Amazon Config

步骤 1: 设置
步骤 2: 规则
步骤 3: 审核

Amazon Config 规则

Amazon Config 可以根据您定义的规则来检查资源的配置。请选择以下一个或多个规则以开始操作。设置 Amazon Config 后，您可以自定义这些规则、设置 Amazon Config 提供的其他规则或者创建自己的规则。

按规则名称、标签或描述筛选

查看 1 - 9 条 亚马逊云科技 托管规则，总共 118 条 > >

全选 118 | 全部清除

account-part-of-organizations	acm-certificate-expiration-check	alb-http-drop-invalid-header-enabled
该规则会检查 亚马逊云科技 账户是否属于某个 Amazon Organizations 组织。如果账户不属于某个 Amazon Organizations 组织或 Amazon Organizations 组织主账户 ID 与规则参数	查看是否已标记您账户中的 ACM 证书以便其在指定天数内过期。ACM 提供的证书会自动续订。ACM 不会自动续订您导入的证书。	检查规则是否评估了 亚马逊云科技 Application Load Balancers (ALB)，以确保它们已被配置为丢弃 http 头。如果 routing.http.drop_invalid_header_fields.enable
Organizations . Account	ACM	ELBv2 . Http headers
alb-http-to-https-redirection-check	api-gw-associated-with-waf	api-gw-cache-enabled-and-encrypted
查看是否已在 Application Load Balancer 的所有 HTTP 侦听器上配置了 HTTP 到 HTTPS 重定向。如果 Application Load Balancer 的一个	Checks if an Amazon API Gateway API stage is using an Amazon WAF Web ACL. This rule is NON_COMPLIANT if an Amazon WAF Web	查看 Amazon API Gateway 阶段中的所有方法是否都已启用和加密缓存。如果 Amazon API Gateway 阶段的任何方法未配置到缓存或缓存

4. 审核，然后确认

以上，Config 服务开通完成。

12.1.2 开通 Security Hub 服务

- 通过 AWS 管理控制台导航到 Security Hub 产品，也有 30 天免费试用



2. “安全性标准”建议选择“亚马逊云科技基础安全最佳实践 v1.0.0”。

安全性标准在等保里是没有明确要求的；为了提高您的云环境的安全基线，建议选择“亚马逊云科技基础安全最佳实践 v1.0.0”。“亚马逊云科技基础安全最佳实践 v1.0.0”是亚马逊基于多年的安全实践总结的最佳实践；这些规则只是做检测、告警，对业务没有影响。



3. 启用 Security Hub



4. 查看摘要



以上，Security Hub 开通完成。

12.2 GuardDuty 集成 Security Hub

GuardDuty 的威胁检测结果 findings 自动发送到 Security Hub 中：

<https://docs.aws.amazon.com/guardduty/latest/ug/securityhub-integration.html#securityhub-integration-sending-findings>

12.3 管理控制台的其他访问控制

附录参考资料：

IAM user 可以限定 IP 地址：

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-ip.html

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/restrict-access-to-aws-apis-for-iam-identity-center-and-iam-users-through-trusted-source-ip-ranges.html>

基于 console 登陆失败次数限制登陆：

<https://github.com/xiangqua/aws-console-lockout>

13 日志集中审计

日志集中审计是等保中非常重要的检测项。亚马逊云科技上集中日志审计的几个方式：

- CloudWatch Logs，云原生的 service，使用简便，默认集成的云服务多；本章节主要介绍这种方式。
- LOG Hub，亚马逊云科技中国区的一个 solution，可以一键部署，需要开通客户账号下的 opensearch 等服务，有一定基础成本，适合体量大的客户。具体可参考：
<https://www.amazonaws.cn/solutions/log-hub/>
- 客户自建，用亚马逊云科技 opensearch、或基于 EC2 自建 ELK、或 S3，适合运维动手能力强、有专人维护的客户。

CloudWatch Log 服务，是亚马逊云科技提供给的全托管日志服务。CloudWatch Logs 使您能够将所有系统、应用程序和亚马逊云科技服务中的日志集中在一个高度可扩展的单个服务中。您可以轻松地查看日志、在日志中搜索特定错误代码或模式、根据特定字段筛选日志，或者安全地将这些日志归档以供将来分析。

详细说明如下：

<https://docs.amazonaws.cn/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>

亚马逊云科技原生服务的日志，默认支持保存在 CloudWatch Logs 服务中的有：

<https://docs.amazonaws.cn/AmazonCloudWatch/latest/logs/aws-services-sending-logs.html>

等保要求日志需要保存 6 个月；为了降低存储成本，可以把 CloudWatch Logs 中的日志，导出到 S3 中进行长期存储。建议在 CloudWatch Logs 中保存 2 周，用来做分析使用；然后导出到 S3 中，为审计使用。

使用说明：

<https://docs.amazonaws.cn/AmazonCloudWatch/latest/logs/S3ExportTasksConsole.html>

Application 和 OS 的日志保存到 CloudWatch Logs 的操作说明：

- EC2 的系统和应用日志收集到 CloudWatch Logs 中：
<https://aws.amazon.com/cn/blogs/china/cloudwatch-agent-in-cloudwatch-ec2-rom/>
- CloudWatch Log 系统级日志收集配置方法：
<https://docs.aws.amazon.com/prescriptive-guidance/latest/implementing-logging-monitoring-cloudwatch/system-level-cloudwatch-configuration.html>

Container 容器日志收集到 CloudWatch Logs：

<https://aws.amazon.com/blogs/devops/send-ecs-container-logs-to-cloudwatch-logs-for-centralized-monitoring/>

本章节是介绍操作系统 OS 和应用 Application 的日志收集，其他部分在对应的章节中，CloudTrail log 在第 5 章，WAF log 在第 7 章，Session Manager log 在第 8 章，RDS audit log 在第 11 章。



13.1 安装 CloudWatch Agent

我们是通过 Systems Manager 的初始配置启动了 CloudWatch Agent 的安装，所以不需要再安装。

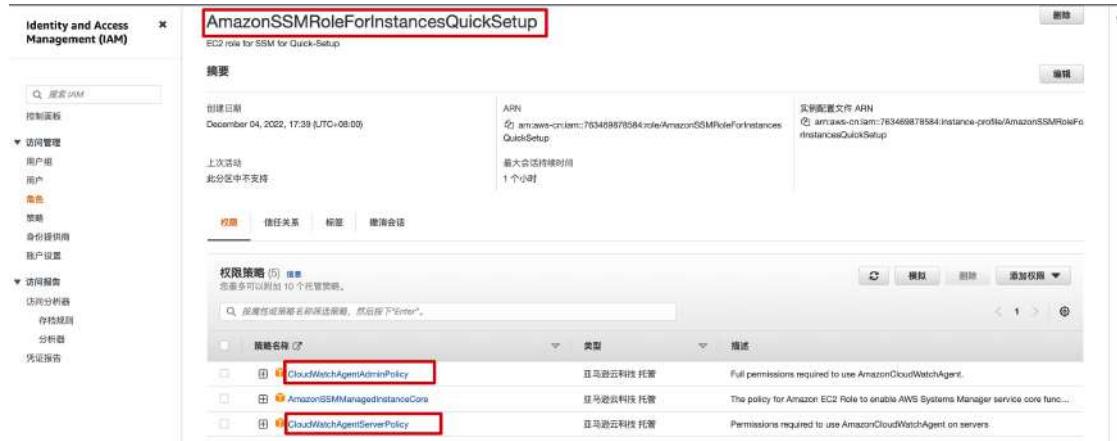
在 EC2 服务器的 /opt/aws/ 目录下如果有 amazon-cloudwatch-agent 文件就代表安装过了。

如果没有安装过，可以参考这个文档说明：

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/installing-cloudwatch-agent-commandline.html>

为了能让部署在 EC2 上的 CloudWatch Agent 能创建日志流、上传日志及使用 Systems Manager 的 Parameters Store 功能，需要给给 EC2 instance profile 增加权限。我们这个实例中的 EC2 instance profile 是在启动 Systems Manager 时创建的，AmazonSSMRoleForInstancesQuickSetup，所有的 EC2 实例都是一样的。

我们在这个 profile 中增加 CloudWatchAgentServerPolicy and CloudWatchAgentAdminPolicy 两个策略。



13.2 配置 CloudWatch Agent

CloudWatch Agent 运行前需要一个配置文件，用来指定收集哪些 Metrics 和 Logs。
先通过 Wizard 来创建需要监控哪些内容的配置文件，配置一台 EC2 实例；然后把配置文件上传的 Systems Manager 的 Parameters Store 中，后续实例的配置都可以直接使用 Parameters Store 中的配置文件。

13.2.1 通过 Wizard 配置

通过 Wizard 创建配置文件的参考文档：

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-cloudwatch-agent-configuration-file-wizard.html>

1. 通过 Session Manager 登录到一台 application ec2，然后执行如下命令：
`sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard`

```
[root@ip-10-0-147-215 bin]# sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
=====
= Welcome to the Amazon CloudWatch Agent Configuration Manager =
=
= CloudWatch Agent allows you to collect metrics and logs from =
= your host and send them to CloudWatch. Additional CloudWatch =
= charges may apply.
=====
On which OS are you planning to use the agent?
1. linux
2. windows
3. darwin
default choice: [1]:  
  
Trying to fetch the default region based on ec2 metadata...
Are you using EC2 or On-Premises hosts?
1. EC2
2. On-Premises
default choice: [1]:  
  
Which user are you planning to run the agent?
1. root
2. cwagent
3. others
default choice: [1]:  
1  
Do you want to turn on StatsD daemon?
1. yes
2. no
default choice: [1]:  
2
```

```
Do you want to monitor metrics from CollectD? WARNING: CollectD must be installed or the Agent will fail to start
1. yes
2. no
default choice: [1]:  
2  
Do you want to monitor any host metrics? e.g. CPU, memory, etc.
1. yes
2. no
default choice: [1]:  
1  
Do you want to monitor cpu metrics per core?
1. yes
2. no
default choice: [1]:  
1  
Do you want to add ec2 dimensions (ImageId, InstanceId, InstanceType, AutoScalingGroupName) into all of your metrics if the info is available?
1. yes
2. no
default choice: [1]:  
1  
Do you want to aggregate ec2 dimensions (InstanceId)?
1. yes
2. no
default choice: [1]:  
2
```

```
Would you like to collect your metrics at high resolution (sub-minute resolution)? This enables sub-minute resolution for all metrics, but you can customize
for specific metrics in the output json file.
1. 1s
2. 10s
3. 30s
4. 60s
default choice: [4]:  
4  
Which default metrics config do you want?
1. Basic
2. Standard
3. Advanced
4. None
default choice: [1]:  
2
```

2. 填写要收集的日志文件路径、日志组名称和日志流名称，日志保存 14 天。

```
Log file path:  
/var/log/audit/audit.log  
Log group name:  
default choice: [audit.log]  
/oslogs/log/audit  
Log stream name:  
default choice: [{instance_id}]  
  
Log Group Retention in days  
1. -1  
2. 1  
3. 3  
4. 5  
5. 7  
6. 14  
7. 30  
8. 60  
9. 90  
10. 120  
11. 150  
12. 180  
13. 365  
14. 400  
15. 545  
16. 731  
17. 1827  
18. 2192  
19. 2557  
20. 2922  
21. 3288  
22. 3653  
default choice: [1]:  
6
```

总收集的日志：

OS 日志：

/var/log/audit/audit.log
/var/log/messages
/var/log/secure

httpd 日志：

/var/log/httpd/access_log
/var/log/httpd/error_log

日志组名称：

/oslogs/log/audit
/oslogs/log/messages
/oslogs/log/secure
/applicationlogs/log/httpd/access_log
/applicationlogs/log/httpd/error_log

Log stream name:

default choice: [{instance_id}]

3. 配置文件保存到 parameter store

```
Do you want to store the config in the SSM parameter store?
1. yes
2. no
default choice: [1]:
1
What parameter store name do you want to use to store your config? (Use 'AmazonCloudWatch-' prefix if you use our managed AWS policy)
default choice: [AmazonCloudWatch-linux]
AmazonCloudWatch-linux-mlps
Trying to fetch the default region based on ec2 metadata...
Which region do you want to store the config in the parameter store?
default choice: [cn-northwest-1]

Which AWS credential should be used to send json config to parameter store?
1. ASIA3DQS2U4IWCHR5D (From SDK)
2. Other
default choice: [1]:

Successfully put config to parameter store AmazonCloudWatch-linux-mlps.
Program exits now.
sh-4.2$
```

4. 启动 Agent

在这个目录下 /opt/aws/amazon-cloudwatch-agent/bin，执行命令：

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:config.json
```

```
root@ip-10-0-147-215 bin# pwd
/opt/aws/amazon-cloudwatch-agent/bin
root@ip-10-0-147-215 bin# sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:config.json
**** processing amazon-cloudwatch-agent ****
/opt/aws/amazon-cloudwatch-agent/bin/config-downloader --output-dir /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d --download-source file:config.json --mode ec2 --multi-config /opt/aws/amazon-cloudwatch-agent/etc/common-config.toml
I|g-josn I| Trying to detect region from ec2
D| [EC2] Found active network interface
Successfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
/opt/aws/amazon-cloudwatch-agent/bin/config-translator --input /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json --input-dir /opt/aws/amazon-cloudwatch-agent/etc/common-config.toml --multi-config default
2023/12/07 11:22:31 I| Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2023/12/07 11:22:31 I| Valid JSON config schema.
I| Detecting run_as user...
I| Trying to detect region from ec2
D| [EC2] Found active network interface
No custom configuration found.
Configuration validation first phase succeeded
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
Redirecting to /bin/systemctl stop amazon-cloudwatch-agent.service
Redirecting to /bin/systemctl restart amazon-cloudwatch-agent.service
|root@ip-10-0-147-215 bin#
```

备注：linux 上 log 的说明，按运维实际需求增加。

/var/log/syslog：它和/etc/log/messages 日志文件不同，它只记录警告信息，常常是系统出问题的信息。

/var/log/messages：包括整体系统信息，其中也包含系统启动期间的日志。此外，还包括 mail, cron, daemon, kern 和 auth 等内容

/var/log/user.log：记录所有等级用户信息的日志。

/var/log/auth.log：包含系统授权信息，包括用户登录和使用的权限机制等。

/var/log/daemon.log：包含各种系统后台守护进程日志信息。

/var/log/kern.log：包含内核产生的日志，有助于在定制内核时解决问题。

13.2.2 使用 parameter store 配置

1. 在 Systems Manager 的 Parameter Store 列表页中，可以看到我们通过 Wizard 创建的配置文件

The screenshot shows the 'Parameter Store' section of the Amazon Systems Manager console. On the left, there's a navigation sidebar with 'Parameter Store' selected. The main area displays a table titled '我的参数' (My Parameters) with one item listed:

名称	层	类型	上次修改日期
AmazonCloudWatch-linux-mlps	标准	String	Thu, 08 Dec 2022 07:00:3

2. 切换到 Systems Manager 的运行命令 Run Command 列表页，点击运行命令

The screenshot shows the 'Run Command' section of the Amazon Systems Manager console. On the left, 'Run Command' is selected under '节点管理'. The main area shows a table with no results:

命令 ID	状态	请求日期	文档名称	注释	# 目标	# 错误	# 提交超时	# 完成
当前没有执行任何命令。								

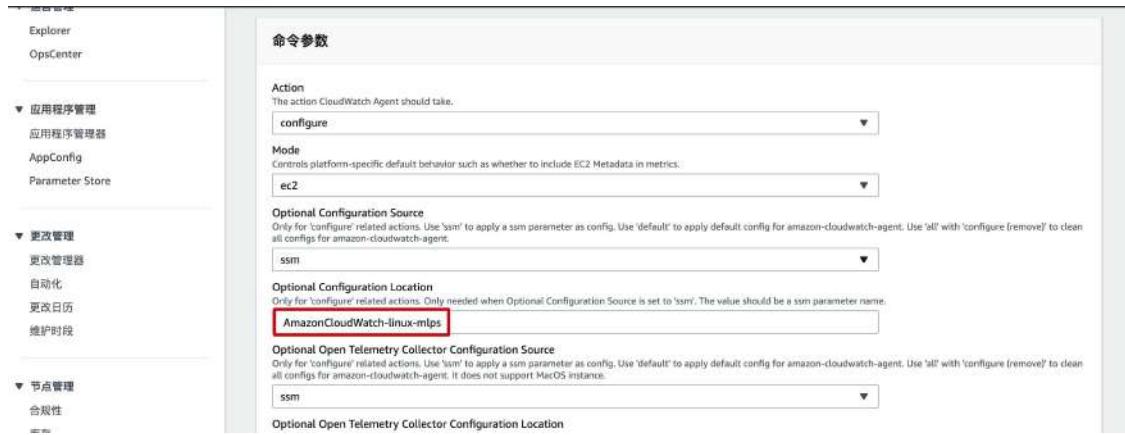
3. 运行命令文档选择 AmazonCloudWatch-ManageAgent,

The screenshot shows the configuration page for a specific command. The left sidebar has 'Run Command' selected under '节点管理'. The main area is titled '运行命令' (Run Command) and shows the '命令文档' (Command Document) section. A search bar shows '搜索: AmazonCloudWatch-ManageAgent'. The results table shows one item:

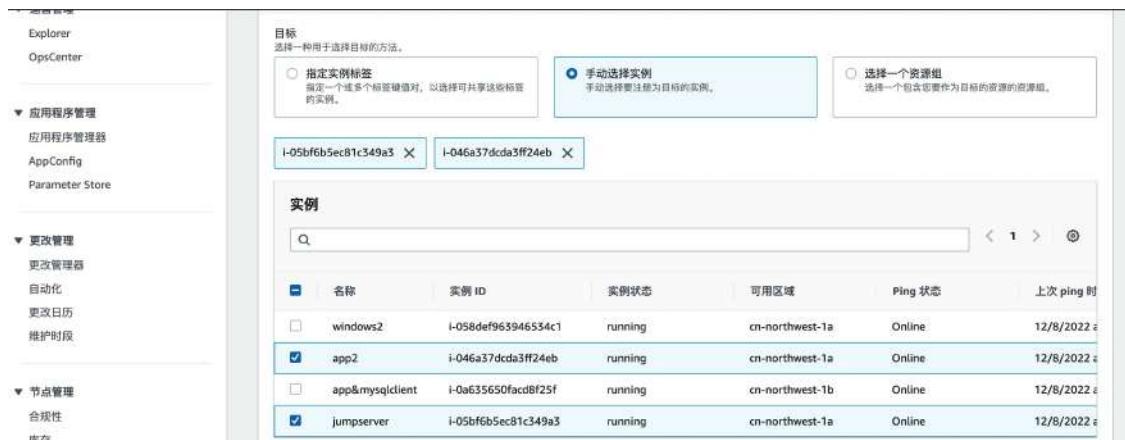
名称	所有者	平台类型
AmazonCloudWatch-ManageAgent	Amazon	Windows, Linux

Below the table, the description reads: 'Send commands to Amazon CloudWatch Agent'.

4. 配置文件名称选择用 Wizard 创建配置文件时候的名称 AmazonCloudWatch-linux-mlps，其他参数默认



5. 选择在哪些目标 EC2 实例上执行，可以选多个



6. 其他参数默认，启动运行



7. 过几秒钟，刷新一下

实例 ID	实例名称	状态	详细状态	开始时间	完成时间
i-046a37dcda3ff24eb	ip-10-0-141-79.cn-northwest-1.compute.internal	成功	成功	Thu, 08 Dec 2022 07:12:05 GMT	Thu, 08 Dec 2022 07:12:06 GMT
i-05bf6b5ec81c549a3	ip-10-0-6-86.cn-northwest-1.compute.internal	成功	成功	Thu, 08 Dec 2022 07:12:05 GMT	Thu, 08 Dec 2022 07:12:07 GMT

13.3 验证集中日志效果

- 打开 CloudWatch 控制台的日志组列表，可以看到我们上节创建的日志组

日志组	保留
/applicationlogs/log/httpd/access_log	2 周
/oslogs/log/audit	2 周

- 查看/oslogs/log/audit 日志组，有 3 个 EC2 示例的日志流

日志流	上次事件时间
i-0a635650facd8f25f	2022-12-08 15:30:06 (UTC+08:00)
i-046a37dcda3ff24eb	2022-12-08 15:30:06 (UTC+08:00)
i-05bf6b5ec81c549a3	2022-12-08 15:30:06 (UTC+08:00)

- 查看日志流的详细信息

CloudWatch

收藏夹和最近访问

控制面板

▶ 警报

▼ 日志

日志组

Logs Insights

▼ 指标

全部指标

资源管理器

▶ X-Ray 跟踪

▶ 事件

▶ 应用程序监控

▶ 洞察

CloudWatch > 日志组 > /onlog/log/audit > l-0a635650facd8f25f

日志事件

您可以使用下面的筛选条件栏搜索和匹配日志事件中的术语、短语或值。详细了解筛选条件模式

筛选事件

清除 1m 30m 1h 12h 自定义 Display

时间戳 消息

我们目前未找到较早的事件。 查看

▶ 2022-12-08T15:40:53.058+08:00	type=SERVICE_START msg=audit[1670482204.036:15788]: pid=1 uid=0 ouid=4294967295 ses=4294967295 msg='unit..'
▶ 2022-12-08T15:40:53.058+08:00	type=SERVICE_STOP msg=audit[1670482204.036:15788]: pid=1 uid=0 ouid=4294967295 ses=4294967295 msg='unit..'
▼ 2022-12-08T15:40:53.058+08:00	type=USER_ACCT msg=audit[1670482201.154:15789]: pid=17736 uid=0 ouid=4294967295 ses=4294967295 msg='op=..'
	type=USER_ACCT msg=audit[1670482201.154:15789]: pid=17736 uid=0 ouid=4294967295 ses=4294967295 msg='op=..'
▶ 2022-12-08T15:40:53.058+08:00	type=CRED_ACQ msg=audit[1670482201.154:15790]: pid=17736 uid=0 ouid=4294967295 ses=4294967295 msg='op=..'
▶ 2022-12-08T15:40:53.058+08:00	type=LOGIN msg=audit[1670482201.154:15791]: pid=17736 uid=0 ouid=4294967295 uid=0 tty=(none) old-s..
▶ 2022-12-08T15:40:53.058+08:00	type=USER_START msg=audit[1670482201.154:15792]: pid=17736 uid=0 ouid=0 ses=2191 msg='op=PAM:session_op..'
▶ 2022-12-08T15:40:53.058+08:00	type=CRED_REFR msg=audit[1670482201.158:15793]: pid=17736 uid=0 ouid=0 ses=2191 msg='op=PAM:setcred gra..'
▶ 2022-12-08T15:40:53.058+08:00	type=CRED_DISP msg=audit[1670482201.162:15794]: pid=17736 uid=0 ouid=0 ses=2191 msg='op=PAM:setcred gra..'

查看 application 的日志

CloudWatch

收藏夹和最近访问

控制面板

▶ 警报

▼ 日志

日志组

Logs Insights

▼ 指标

全部指标

资源管理器

▶ X-Ray 跟踪

▶ 事件

▶ 应用程序监控

▶ 洞察

CloudWatch > 日志组 > /onlog/log/audit > l-0a635650facd8f25f

我们目前未找到较早的事件。 自动重试已暂停。 [Resume](#)

▶ 2022-12-08T17:16:41.210+08:00	10.0.24.95 - - [08/Dec/2022:09:16:41 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:16:49.211+08:00	10.0.7.109 - - [08/Dec/2022:09:16:44 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:17:01.211+08:00	10.0.24.95 - - [08/Dec/2022:09:16:56 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:17:19.210+08:00	10.0.7.109 - - [08/Dec/2022:09:17:14 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:17:39.210+08:00	10.0.24.95 - - [08/Dec/2022:09:17:26 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:17:49.210+08:00	10.0.7.109 - - [08/Dec/2022:09:17:44 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:18:00.211+08:00	10.0.24.95 - - [08/Dec/2022:09:17:56 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:18:20.210+08:00	10.0.7.109 - - [08/Dec/2022:09:18:15 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:18:31.210+08:00	10.0.24.95 - - [08/Dec/2022:09:18:26 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:18:49.210+08:00	10.0.7.109 - - [08/Dec/2022:09:18:45 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:19:01.210+08:00	10.0.24.95 - - [08/Dec/2022:09:18:56 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:19:19.210+08:00	10.0.7.109 - - [08/Dec/2022:09:19:15 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:19:31.210+08:00	10.0.24.95 - - [08/Dec/2022:09:19:26 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:19:49.210+08:00	10.0.7.109 - - [08/Dec/2022:09:19:45 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:20:01.210+08:00	10.0.24.95 - - [08/Dec/2022:09:19:54 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:20:20.210+08:00	10.0.7.109 - - [08/Dec/2022:09:20:15 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
▶ 2022-12-08T17:20:26.296+08:00	10.0.24.95 - - [08/Dec/2022:09:20:25 +0000] "GET /SamplePage.php HTTP/1.1" 200 1045 "-" "Mozilla/5.0 (..
▼ 2022-12-08T17:20:31.210+08:00	10.0.24.95 - - [08/Dec/2022:09:20:26 +0000] "GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"
10.0.24.95 - - [08/Dec/2022:09:20:26 +0000]	"GET / HTTP/1.1" 200 29 "-" "ELB-HealthChecker/2.0"

复制 Back to top

14 备份

数据库的备份可以使用亚马逊云科技 Backup 服务，支持本 Region 备份和跨 Region 备份。

等保二级中备份可选。

数据库异地备份可以通过亚马逊云科技 Backup 实现：

https://docs.amazonaws.cn/en_us/aws-backup/latest/devguide/cross-region-backup.html

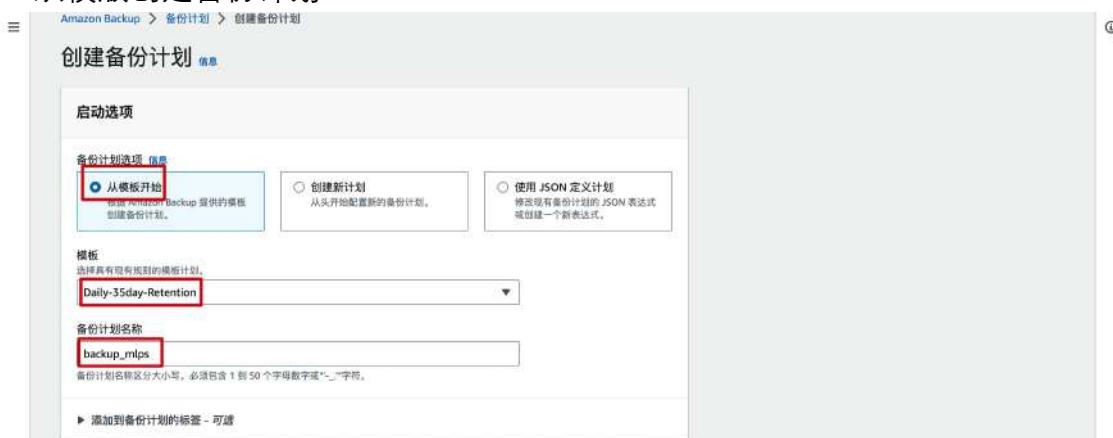
Backup workshop : <https://catalog.us-east-1.prod.workshops.aws/workshops/74237958-77c8-4e7f-a02f-ae201a04d759/en-US/aws-backup-lab>

14.1 创建备份计划

1. 通过 Backup 控制台的备份计划列表页，创建备份计划



2. 从模版创建备份计划



3. 选择默认的备份规则



3. 创建好的备份计划



14.2 创建备份角色

在 IAM 控制台，创建一个角色 role，名称是 self-AWSServiceRoleForBackup；然后给这个 role 分配两个 policy，用来执行备份任务和从备份中恢复。这个新建的 role 在下一步分配备份资源的时候会使用。



The screenshot shows the AWS IAM console with the 'AWSBackupServiceRolePolicyForRestore' and 'AWSBackupServiceRolePolicyForBackup' policies highlighted in red boxes. These policies provide AWS Backup permissions to the respective roles.

14.2 分配备份资源

1. 打开备份计划，开始分配备份资源

The screenshot shows the Amazon Backup console with the '分配资源' (Assign Resources) button highlighted in red. This button is used to assign resources to the backup plan.

2. 填写资源名称 RDS，选择备份的角色 self-AWSServiceRoleForBackup

The screenshot shows the '分配资源' (Assign Resources) configuration screen for the RDS resource. The 'self-AWSServiceRoleForBackup' role is selected in the dropdown menu, highlighted with a red box.

3. 根据特定的资源类型，选择 RDS 的具体实例



4. 然后保存即可，在备份计划的资源分配上就可以看到刚添加的资源

名称	IAM 角色 ARN	创建时间
RDS	arn:aws-cn:iam::763469878584:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup	2022年12月16日, 上午 1:21

14.3 设置备份到异地 region

通过备份规则，可以选择备份的异地目的地 region；

1. 导航到备份规则

名称	备份保管库	目标备份保管库
DailyBackups	Default	-

2. 编辑备份规则

摘要
备份规则名称 DailyBackups
频率 每日
开始时间范围 在上午 05:00 UTC
时长 8 小时
时长 7 天

3. 复制目的地选择北京，因为当前的 region 是宁夏



14.4 查看备份结果

我们创建的备份任务是每天执行一次，所以这个需要等大概一天。

1. 查看备份作业，每天会自动创建一个作业，执行完成即代表完成了一次备份

备份作业 ID	状态	资源 ID	资源类型	创建时间
9F70E8E1-329E-882F-AD65-2398E8EACAE8	已完成	database-mysql-mlps	RDS	2022年12月17日,下午1:00 (UTC+08:00)

2. 查看本 Region（宁夏）的备份保管库

备份保管库名称	保管库锁定状态	恢复点	KMS 加密密钥 ID
Default	-	1	13be237c-ee82-441c-8b73-992f3d01a800

3. 在备份保管库中，查看恢复点，可以看到有一个刚今天刚创建的恢复点，也就是一个成功的备份

The screenshot shows the Amazon Backup console interface. On the left, there's a navigation sidebar with options like '控制面板', '备份保管库' (which is highlighted with a red box), '备份计划', '受保护的资源', '作业', and '设置'. The main area has a title 'Amazon Backup' and a '摘要' (Summary) section. It displays details such as '备份保管库名称: Default', '创建日期: 2022年8月29日, 下午 4:50 (UTC+08:00)', and 'KMS 加密密钥 ID: 13be237c-eaa2-441c-8b73-992f3d01a800'. Below this is a '恢复点 (1)' (Snapshot (1)) section with a table. The table has columns: 备份 ID, 状态, 资源 ID, 资源类型, 备份类型, and 创建时间. One row is shown: 'vbackup:job-9f70ebe1-329e-8b2f-ad65-2398ebeacae8' (status: 已完成 - Completed), 'database-mysql-mlps', 'RDS', '快照 - Snapshot', and '2022年12月17日, 下午'.

4. 查看异地 Region (北京) 的备份保管库中是否有成功的备份

This screenshot shows the Amazon Backup console in the Beijing Region. The interface is similar to the one above, with a sidebar and a main summary section. The 'Default' vault is selected. The '恢复点 (1)' section shows a single snapshot row with a status of '已完成' (Completed). The table columns and data are identical to the screenshot from the US West (Oregon) Region.