云享家 | 医疗和金融行业在AWS平台的合规配置

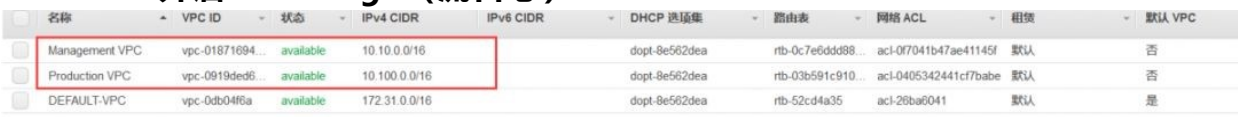
原创：陆叶 BespinGlobal 1周前

1 为什么要做系统合规审计?

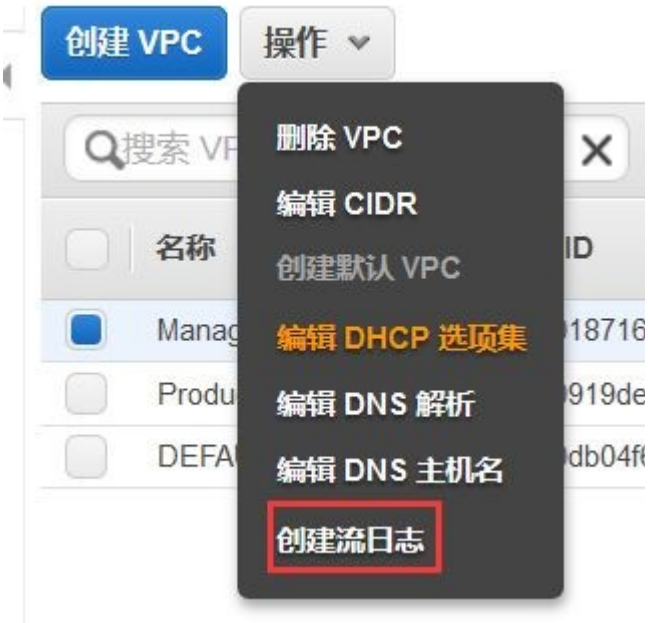
MSP服务各种行业客户，如医疗、金融、保险等行业对数据的安全和私密性有着更高的要求。比如美国《1996 年健康保险流通与责任法案》(HIPAA) 这项立法的目的在于使美国工人在跳槽或失业后更容易继续享受健康保险。该法案还推动电子健康记录的采用，以便通过加强信息共享来提高美国医疗保健系统的效率和质量。在推动采用电子病历的同时，HIPAA 还加入了相关规定来保障受保护健康信息 (PHI) 的安全性和隐私性。下面介绍几项AWS就HIPAA的几项合规配置。

2 配置内容和要求

2.1 VPC 开启flow logs（流日志）



1） 选择创建日志



2） 在红框选择试验环境提供的参数，两个VPC同一个操作

2.2 Cloudwatch 创建UnauthorizedAttemptCount 监控报警

创建cloudwatch报警策略

报警邮件验证

- 创建完成会发一封邮件到邮件列表确认订阅

- 确认后：

- 报警邮件

2.3 EC2 卷加密

步骤：

- 对未加密卷进行快照

1） 在【卷】面板对需要做加密的卷创建快照，打快照注意快照的区域要和实例一致。

- 复制快照并创建加密卷

2） 打完的快照因为是未加密的，所以要复制一份快照，在复制快照时进行加密。

3） 使用加密快照创建一个卷，注意区域和标签。

- **加密卷：**

- 连接加密卷

4） 选择新建的卷，连接到实例，然后把未加密的卷断开，并删除未加密卷。

- 卷挂载情况:

2.4 S3 bucket 创建delete事件notify和静态文件加密

1） Bucket情况

创建bucket的删除事件监控

2） 在bucket 属性选择【事件】

先创建SQS队列

加密bucket rest文件

3） 选择概述里的文件夹，如果没有文件夹创建一个。

更多里面选择更改加密。

4） 选择AES-256或者AWS-KMS并选择秘钥，保存。

3 总结

上面介绍了合规要求中加密和报警策略配置，后续再对其他内容进行介绍。

相 关 阅 读

云享家 | 基于AWS云平台的IDS联合监控分析
云享家 | 多面手完善AWS CloudWatch监控图表
云享家 | AWS CloudWatch如何集成微信报警

阅读原文