Руководство к разработке архитектуры аварийного восстановления (DR)

SOFTPROM
softprom.com • info@softprom.com

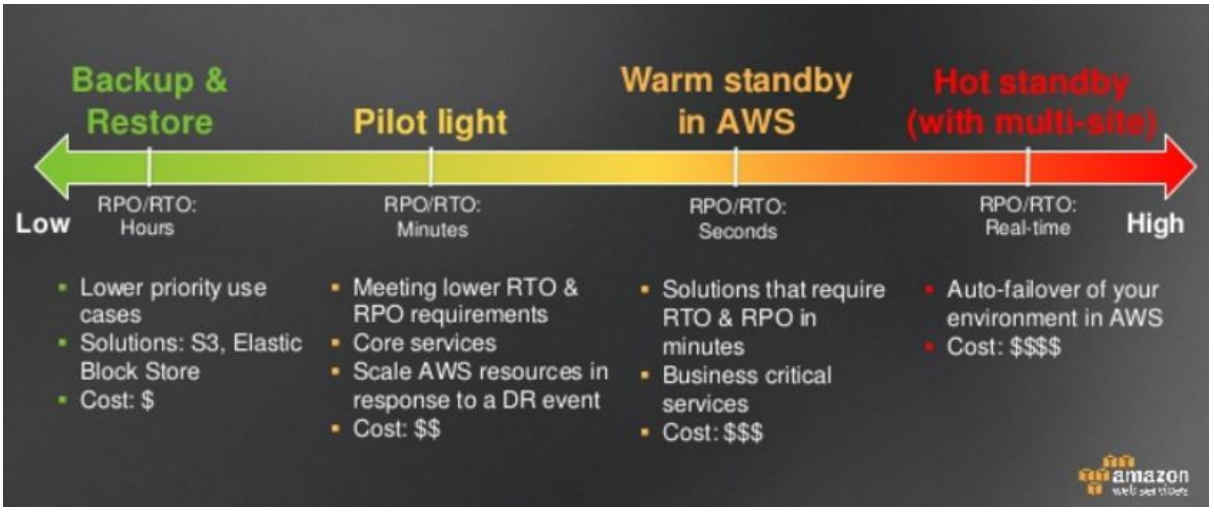
amazon web services | Partner Network
ADVANCED CONSULTING PARTNER

2020

Руководство к разработке архитектуры аварийного восстановления (DR)

Разработка архитектуры аварийного восстановления может быть применима как для гибридной среды, т.е основные мощности расположены в on-premise дата центре, а в облаке находятся резервные копии, образы для быстрого развертывания, готовые к запуску резервные или разделяющие нагрузку с on-premise работающие инфраструктуры. Так и для полность работающей в облаке AWS инфраструктуры, но имеющей резервирование в разных регионах AWS.

Определяющими факторами для разработки архитектуры аварийного восстановления будут требуемые бизнесом параметры RPO(точка восстановления)/RTO(время восстановления).



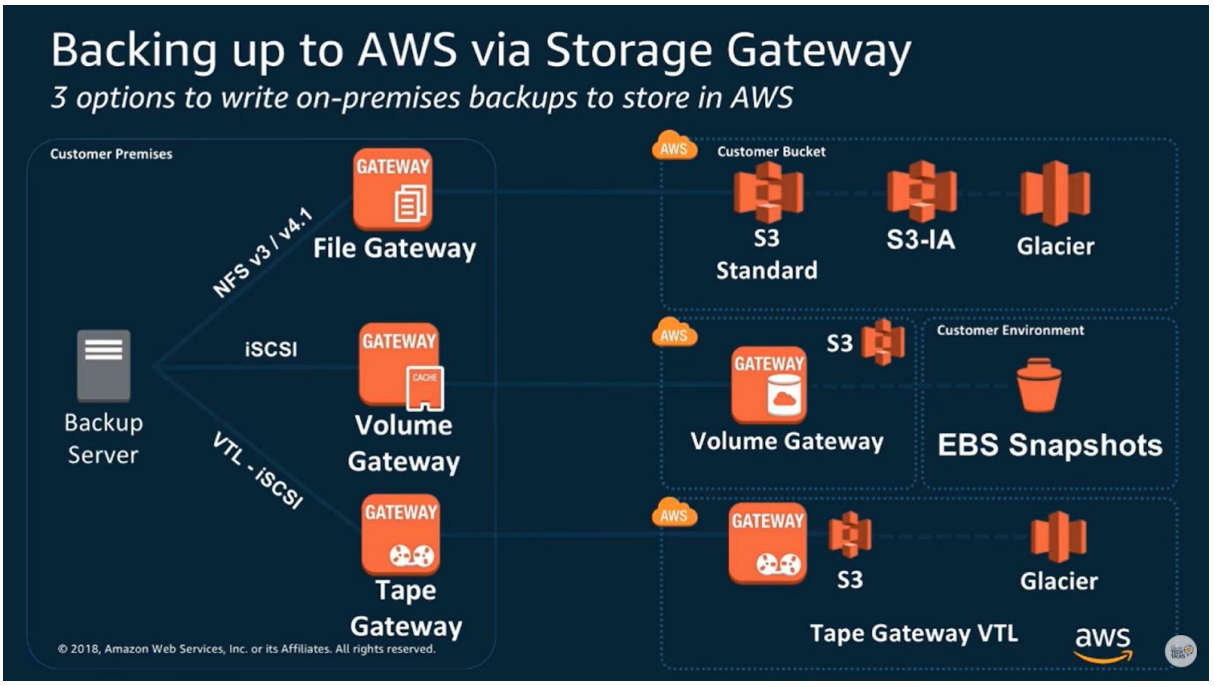
Также немаловажным фактором выбора модели аварийного восстановления будет ее стоимость.

Сценарии аварийного восстановления в AWS

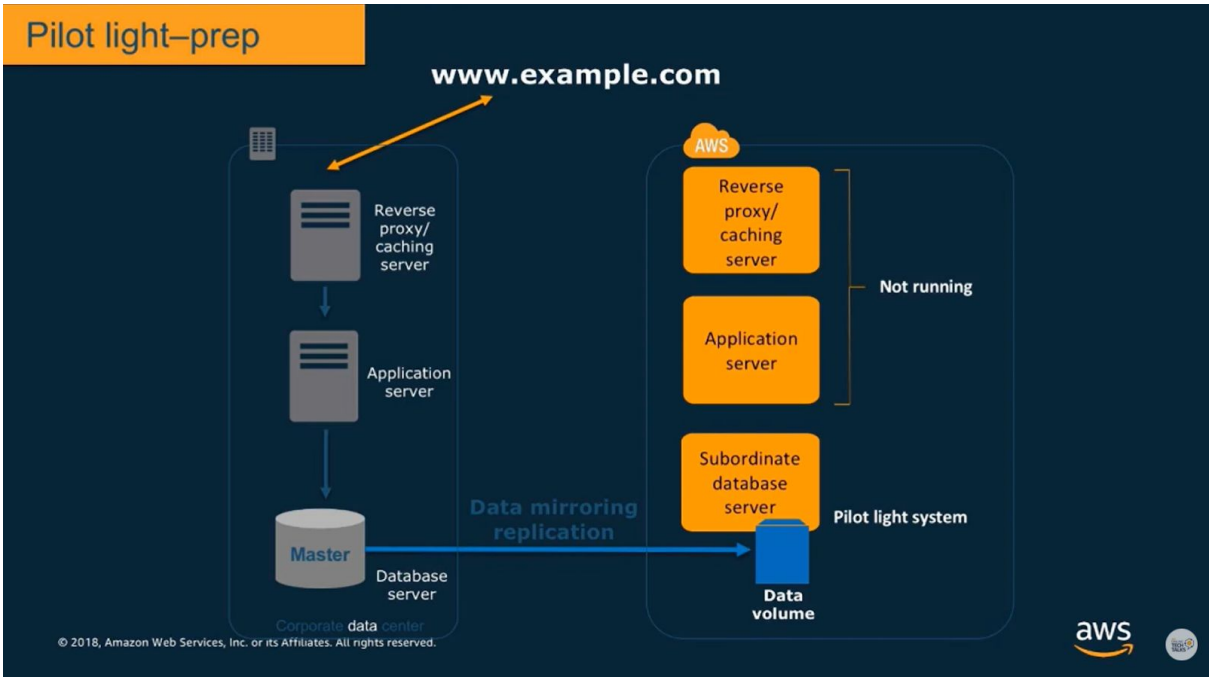
Выбор сценария аварийного восстановления зависит от приоритетов вашего бизнеса, параметров RTO/RPO и стоимости развертывания соответствующего сценария.

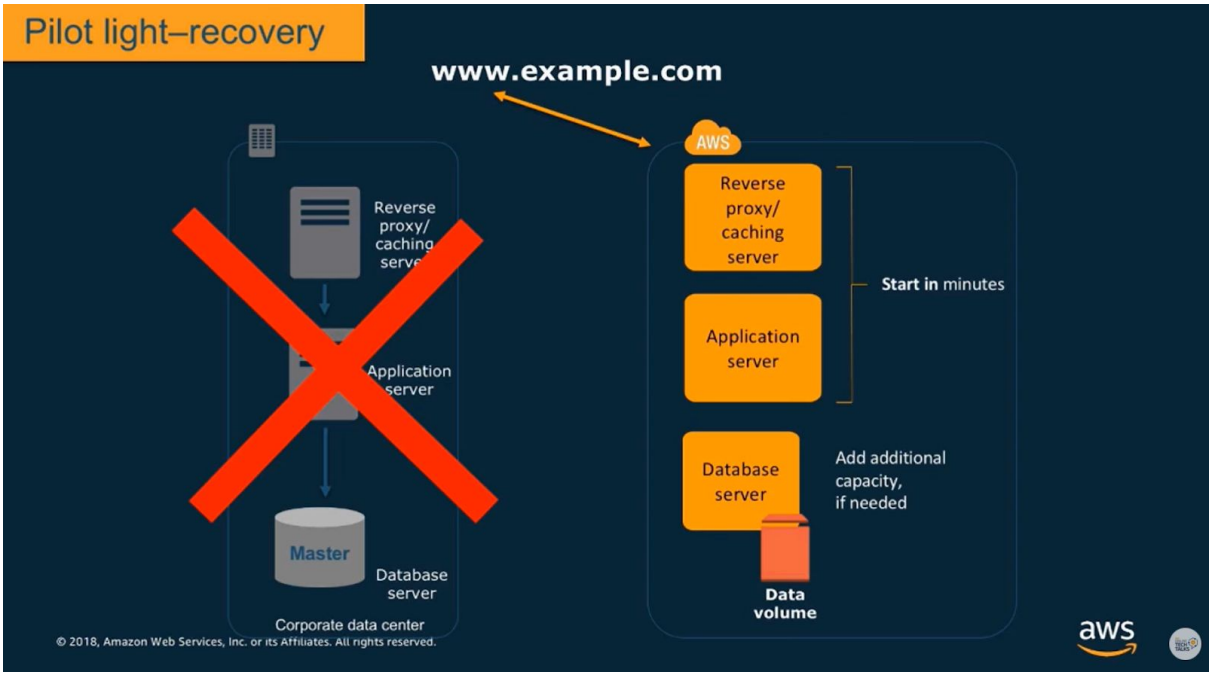
В AWS можно использовать следующие сценарии аварийного восстановления:

- ***Backup and restore.*** Критически важные для бизнеса данные могут регулярно бэкапиться в AWS S3. Объектное хранилище AWS S3 может быть использовано для надежного и безопасного хранения бэкапов и позволяет быстро извлекать данные для дальнейшего восстановления в рабочую инфраструктуру.

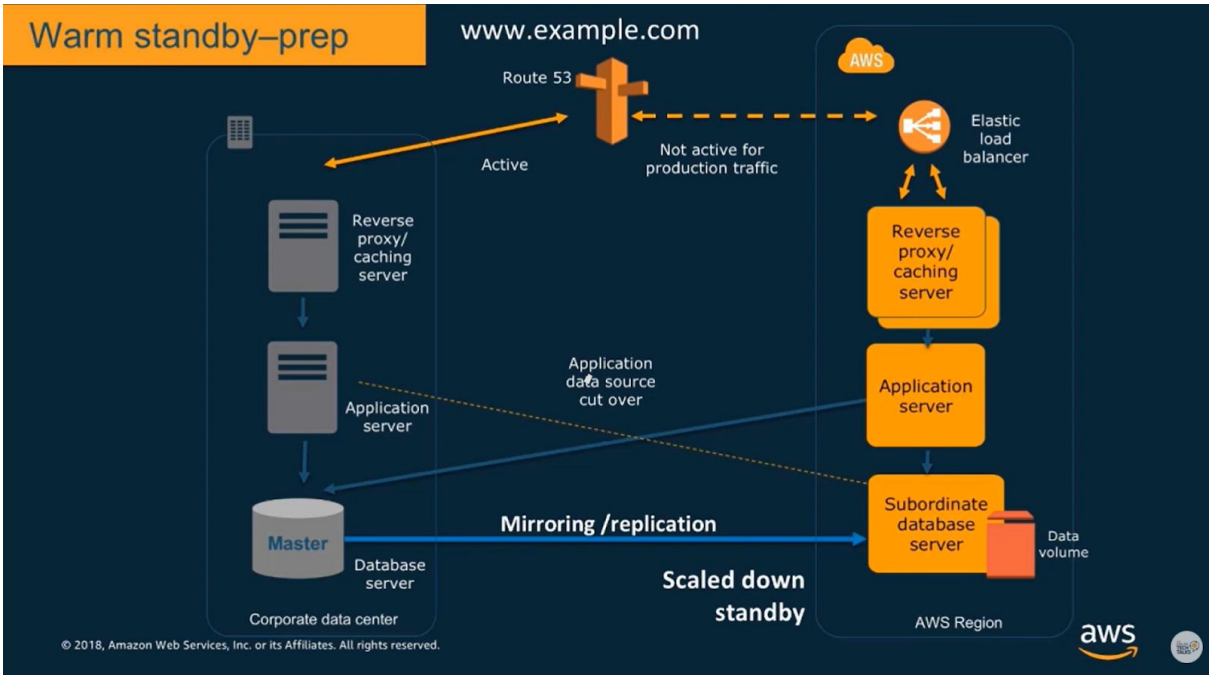


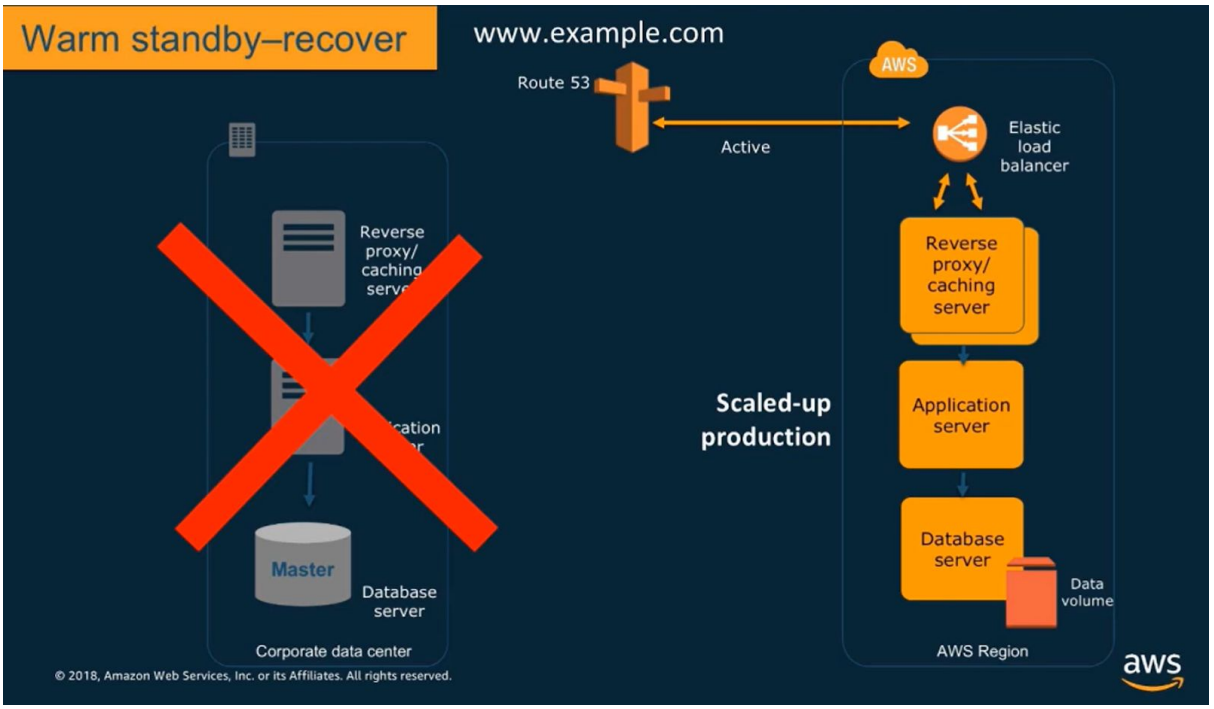
- ***Pilot light.*** Этот сценарий аварийного восстановления подразумевает, что у вас развернуть аналог рабочей виртуальной среды в уменьшенном и выключенном, замороженном виде. Предполагается, что постоянно следите за актуальностью резервной пилотной инфраструктуры. Вы можете быстро восстановить и запустить наиболее важные компоненты инфраструктуры на базе AWS, используя подготовленные образы машин Amazon (AMI) и snapshots Amazon EBS. Метод Pilot light более эффективен, чем стратегия резервного копирования и восстановления, поскольку он значительно сокращает время, затрачиваемое на восстановление.





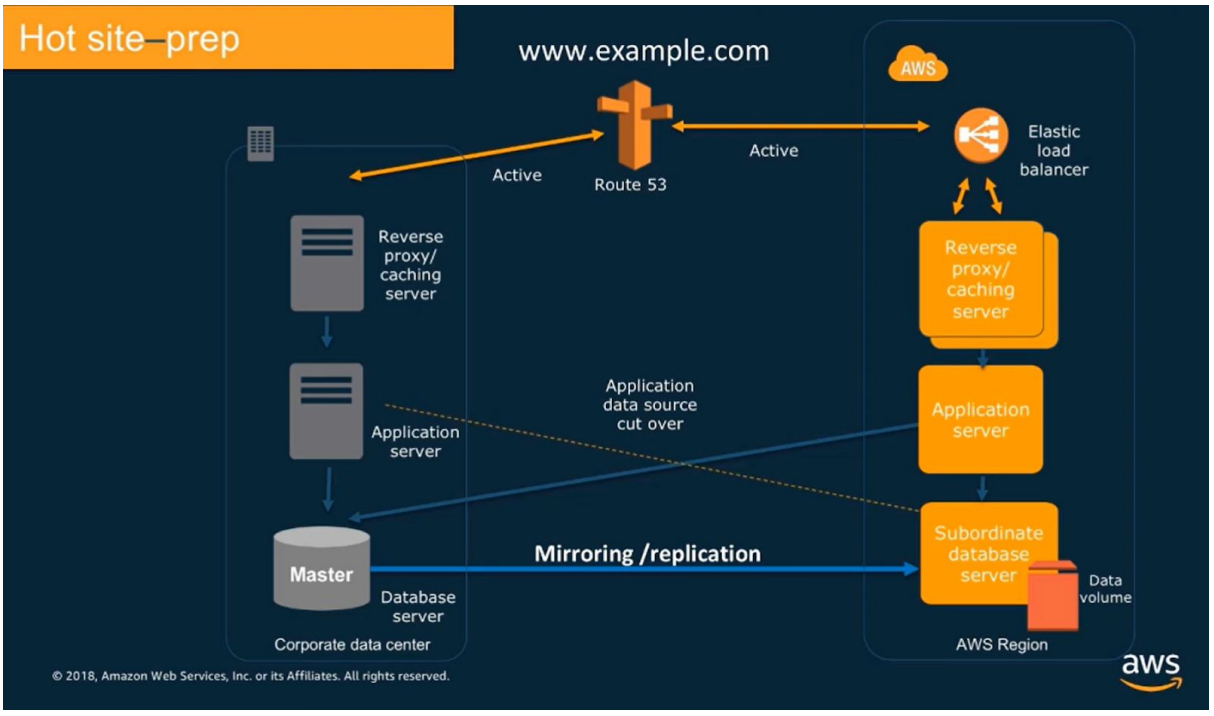
- ***Warm standby.*** Этот сценарий аварийного восстановления предполагает, что в облаке всегда работает уменьшенная версия вашей основной рабочей инфраструктуры. Во время аварийного восстановления облачную версию можно быстро масштабировать до требуемых параметров, которые соответствуют рабочим нагрузкам и минимизировать время простоя.Рисунок №6-7





- ***Multi-site deployment (“hot standby”).*** Этот сценарий предполагает инсталляцию рабочей инфраструктуры в разных местах, например в on-premise дата центре и в AWS, или в разных регионах AWS. Все эти клоны инфраструктуры постоянно активны, они распределяют трафик и рабочие нагрузки между собой и осуществляется постоянная репликация данных и основных компонентов. Если авария затронет одно из мест инсталляции, у вас сохранится работающая инфраструктура, готовая справится с рабочими нагрузками. Для реализации этого сценария используется Amazon EC2 Auto Scaling. Благодаря одновременной

работе нескольких виртуальных инфраструктур время восстановления и параметры RTO/RPO будут минимальны. Однако, такой сценарий аварийного восстановления будет наиболее дорогостоящим решением.

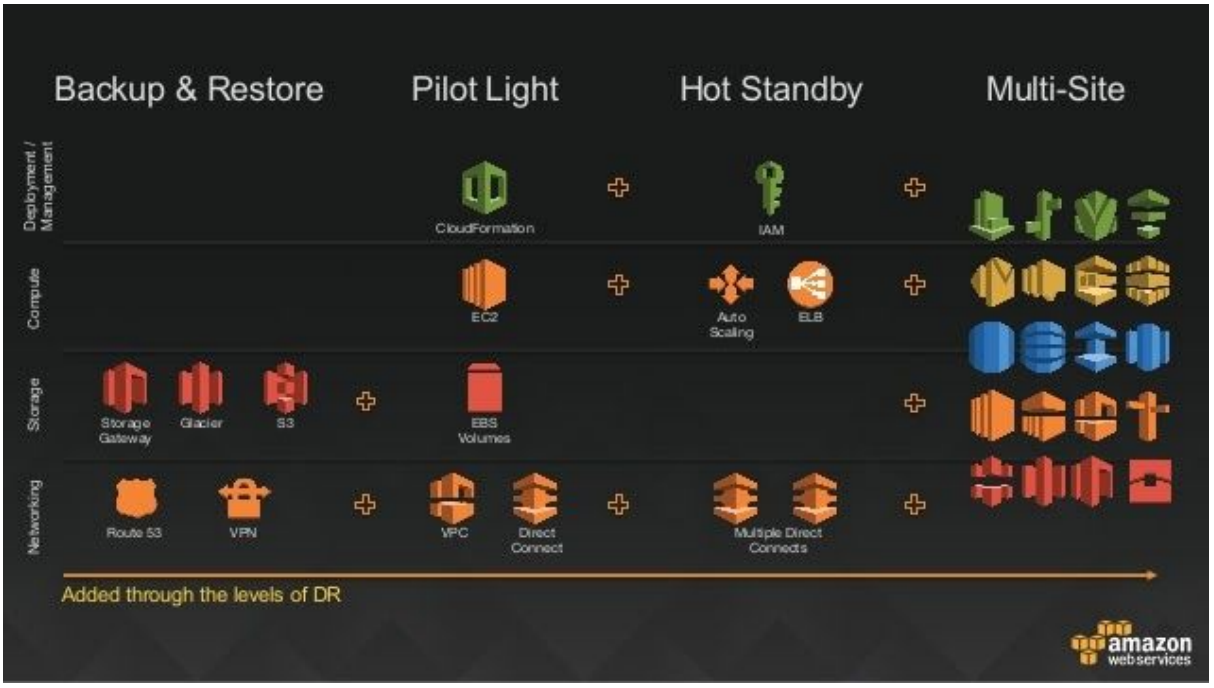


В контексте аварийного восстановления следует также упомянуть следующие функции:

- ***Replication.*** Для обеспечения высокой доступности может быть реализована репликация между разными регионами AWS. Здесь критически важные данные и системные компоненты реплицируются в любой другой выбранный вами регион AWS. Если в первичную базу данных вносятся какие-либо изменения, данные будут обновляться мгновенно (синхронная репликация) или с небольшой задержкой (асинхронная репликация). Эти два типа репликации служат разным бизнес-потребностям.
- ***Failback***. Во время процесса аварийного восстановления рабочая нагрузка поврежденного первичного экземпляра инфраструктуры будет перемещена на рабочий вторичный экземпляр. После восстановления первичного экземпляра вы можете восстановить данные перенаправив репликацию с рабочего вторичного экземпляра на восстановленный первичный и вернуть ему приоритет.
- ***Multiple AWS regions.*** Каждый регион AWS - это отдельная и независимая область, предназначенная для хранения экземпляров или данных. Для успешного аварийного восстановления вы можете

использовать хранение данных в двух или более регионах AWS, чтобы исключить воздействие крупномасштабных катастроф.

На рисунке ниже представлены сервисы AWS применяемые при разных сценариях аварийного восстановления.



Лучшие практики аварийного восстановления в AWS

- ***Testing***. После развертывания решения аварийного восстановления следует его протестировать. Тестирование можно проводить по запросу или по расписанию, чтобы проверить, работает ли ваш план аварийного восстановления должным образом и достигаются ли требуемые RTO/RPO. С этой целью можно использовать AWS CloudFormation для развертывания сред необходимых для работы приложений в Amazon EC2. Вы можете создать шаблоны ваших ресурсов, которые позволят вам моделировать компоненты инфраструктуры в вашей облачной среде и управлять ими. Периодическое тестирование позволит вам проверить, что все компоненты аварийного восстановления правильно спланированы и организованы, а требуемые RTO/RPO будут выполнены, когда это потребуется.
- ***Monitoring and alerting***. Чтобы предотвратить все возможные проблемы в вашей инфраструктуре, необходимо наладить процесс мониторинга и своевременного оповещения. Это позволит быстро обнаружить возникающие угрозы и вовремя на них отреагировать. Amazon CloudWatch система мониторинга в AWS позволяющая отслеживать все

происходящие события в облачной инфраструктуре и настраивать сигналы тревоги и уведомлений, когда определенные показатели достигают критического уровня.

- ***Regular backup and replication***. Крайне важно регулярно выполнять резервное копирование и репликацию, чтобы у вас была актуальная резервная инфраструктура для аварийного переключения. После переключения на инфраструктуру аварийного восстановления следует продолжать выполнять регулярное резервное копирование и репликацию. Хранение этих резервных копий и реплик в отдельных удаленных местах позволит избежать риска возникновения единой точки отказа. AWS может запускать регулярные тесты аварийного восстановления, чтобы проверить состояние вашей инфраструктуры аварийного восстановления.
- ***Use of AWS tools and techniques***. Придерживаясь передовых методов аварийного восстановления, необходимо внедрить группы восстановления или стеки приложений. Таким образом, вы сможете организовать восстановление вашей инфраструктуры должным образом - например, критически важные для бизнеса приложения должны быть восстановлены в первую очередь, так как они имеют наивысший приоритет.

10 советов при создании плана аварийного восстановления в AWS

1. Храните бэкапы томов AWS EBS в разных зонах/регионах AWS
2. Используйте мультизонное размещение инстансов AWS EC2 и RDS
3. Данные в AWS S3 размещайте в разных регионах и синхронизируйте
4. В AWS DynamoDB используйте репликацию данных между регионами AWS
5. Подойдите ответственно к сохранению конфиденциальности доступа к “рутовому” аккаунта (AWS Root Credentials). Настоятельно рекомендуется активировать MFA в “рутовом” аккаунте.
6. Определите ваши RTO/RPO
7. Выберите правильный план аварийного восстановления
8. Идентифицируйте критически важные приложения и разработайте для них план аварийного восстановления
9. Тестируйте вашу реализацию аварийного восстановления
10. Для большей гибкости используйте решения других компаний в сфере аварийного восстановления (DR)