Описание порядка работы Хайстекс Акура и сравнительный анализ с другими решениями по миграции из реестра ПО

Этапы	Хайстекс Акура	Другие решения по миграции из реестра ПО	Проблемы других решений/ вопросы
Предварительная настройка			
	Развертывание серверной части из преднастроенного образа на целевой площадке.	Развертывание из установочных пакетов на подготовленную администратором ВМ.	Перед развертыванием из установочных пакетов необходима заранее подготовить ВМ руками администратора.
	Инициализация установки, создание учетной записи администратора.		
	Создание подключения к API целевой площадки, автоматическая валидация подключения.		
	(опционально) Установка собственного сертификата HTTPS. По-умолчанию также будет использоваться HTTPS, но защищенное самоподписанным сертификатом.	(опционально) Администратор создает HTTPS прокси и настраивает решение для его использования. По умолчанию используется незащищенное соединение HTTP.	По умолчанию используется незащищенный протокол HTTP. А для защиты канала связи требуется настройка дополнительного компонента.
Подготовка к репликации			
	Создание customer с привязкой к целевой площадке для репликации.	Создание проекта.	
		Создание целевых машин на целевой площадке.	Большой объем работы на первом же этапе. Потребление вычислительных мощностей на целевые машины еще до начала репликации. Машина запущены постоянно, а не только в момент тестирования или фейловера. (нужно резервировать большое количество compute).
		Проверка/обеспечение сетевой связности с целевыми машинами: - от контроллера до порта tcp/22 (ssh, Linux) или tcp/445 (Windows) - от целевой машины до HTTP/HTTPS порта контроллера.	**Проблемы с безопасностью:** 1) Контроллер должен находится в том же сетевом контуре, что и целевые машины. Двусторонняя связь контроллер↔машина более сложна в маршрутизации.
	Проверка/обеспечение сетевой связности от исходной площадки до HTTPS порта контроллера.	Проверка/обеспечение сетевой связности с исходными машинами: - от контроллера до порта tcp/22 (ssh, Linux)	2) Необходимо выставить наружу управляющие порты текущего окружения, усложняет настройку, если машины на

		или tcp/445 (Windows) - от исходной машины до HTTP/HTTPS порта контроллера - (предположение) от исходной машины до целевой машины.	исходной площадке не имеют публичных адресов. 3) Требование прямой связи источник->приемник сложно в маршрутизации и может быть заблокировано службой безопасности или потребовать большого количества согласований. 4) Любое изменение адресов требует пересогласования и переоткрытия портов.
		Ввод и сохранение данных учетной записи администратора для доступа к исходной машине, которые будут использованы контроллером в дальнейшем.	5) Хранение учетных записей администратора от машин, к которым есть доступ извне (см. пункты выше).
		Ввод и сохранение данных учетной записи администратора для доступа к целевой машине, которые будут использованы контроллером в дальнейшем.	6) Хранение учетных записей администратора от машин, к которым есть доступ извне (см. пункты выше).
	(опционально, при использовании репликации на уровне гипервизора VMware) Ввод и сохранение данных учетной записи администратора для работы агента репликации VMware, которые будут использоваться агентом развернутым на целевой площадке для подключения к API VMware. Для обеспечения большей безопасности возможно задание данных учетной записи на самом агенте, без сохранения на сервере.		
Установка агента и начало репликации (внутренние агенты репликации)			
	Выбор и скачивание инсталлятора нужного агента репликации (в зависимости от операционной системы).	Заведение записи об исходной машине, с указанием типа операционной системы, платформы виртуализации, IP и порта для доступа к ней, учетных данных администратора машины.	Много ручной работы, метод ускорения - заполнение таблицы инвентаризации.
		Заведение записи о целевой машине, с указанием типа операционной системы, платформы виртуализации, IP и порта для	Много ручной работы, метод ускорения - заполнение таблицы инвентаризации.

		доступа к ней, учетных данных администратора машины.	
		Заведение записи о паре машин источник→приемник.	Много ручной работы при заведении записи о паре машин источник→приемник.
		Валидация пары источник→приемник, в процессе которой на обе машины передается модуль проверки, который после сбора данных отправляет данные в контроллер.	Проблема безопасности: Соединение контроллер→источник и контроллер→приемник с использованием учетных данных администратора. С точки зрения сетевой маршрутизации это весьма сложный процесс.
	В состав дистрибутива агента включены драйверы для 100+ версий Linux-based ОС. Также для Linux агента возможна автоматическая компиляция драйвера с использованием DKMS.	По результатам проверки обнаруженные операционные системы показываются в интерфейсе, далее нужен запрос к разработчикам для получения драйверов для конкретной версии Linux-based ОС.	Встречается проблема, когда нужен драйвер для получения драйверов для конкретной версии Linux-based ОС. Необходимость обращения к разработчикам задерживает процесс.
	Установка агента репликации на реплицируемую машину. Возможна массовая инсталляция агентов администратором с использованием Ansible/Active Directory.	Мало информации в публичном доступе. После валидации пары источник→приемник становятся доступна инициализация репликации, то есть установка контроллером агента репликации.	
	(автоматически) Регистрация машины на контроллере, появление записи о машине в интерфейсе управления.		
	(опционально) Указание целевой Availability Zone и типа дисков.	Мало информации в публичном доступе. Указание сопоставления дисков на исходной и целевой машине.	Требуются знания особенностей конфигурации ПО на исходной машине.
	Начало репликации по команде в UI.	Мало информации в публичном доступе. Начало репликации по команде в UI.	
Инкрементальные репликации			
	Доступны в любой момент по команде или расписанию.	Доступны в любой момент по команде или расписанию.	
	Репликация производится на отдельные диски, с созданием точки восстановления в виде снапшотов дисков.	Мало информации в публичном доступе. Репликация производится на целевую машину. Точек восстановления нет. Есть вероятность расхождения состояния данных между источником и приемником, если на приемнике производятся какие-то изменения/тестирование.	Возникают сомнения относительно консистентности реплики в случае изменений данных на приемнике (которые точно будут, потому что приемник включен).
Подготовка к переключению			

	Генерация заготовки плана миграции из метаданных среплицированных машин.	Мало информации в публичном доступе. Пары источник→приемник объединяются в группы.	
	Донастройка плана миграции указанием привязки воссоздаваемых машин к нужным сетям и размера машин.		
	(опционально) Указание порядка запуска групп машин.	Мало информации в публичном доступе. Указание порядка запуска групп машин.	
	Возможны тестовые запуски планов миграции, в процессе которых по указанным параметрам из точек восстановления создаются машины на целевой площадке. В большинстве целевых облаков не нужно останавливать репликацию для проведения проверки. Вычислительные ресурсы целевой площадки потребляются только в период проведения проверки.	Мало информации в публичном доступе. Проверка работы и целостности данных может быть произведена на машине-приемнике, которая включена все время. При этом репликация не должна идти.	Можно столкнуться с проблемой, когда проверка блокирует репликацию, нет точки восстановления. А потребление вычислительных ресурсов на целевой площадке для целевых машин, даже если в данный момент идет репликация.
Переключение			
	Инициация последней инкрементальной репликации.	Мало информации в публичном доступе. Инициация последней инкрементальной репликации.	
	Запуск протестированного на прошлом этапе плана восстановления.		
	Команда на отвязывание воссозданных машин от контроллера.	Мало информации в публичном доступе. Запрет на дальнейшую репликацию с источника.	