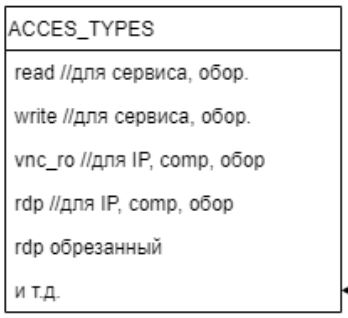
права доступа, Инвентаризация

Инвентаризация: Контроль доступа

Черновик учета доступа пользователей к ресурсам.

Access Types

Таблица типов доступа которые можно предоставить от объекта к субъекту. Вероятно надо сделать поля, к каким типам ресурсов (субъектов) применимы

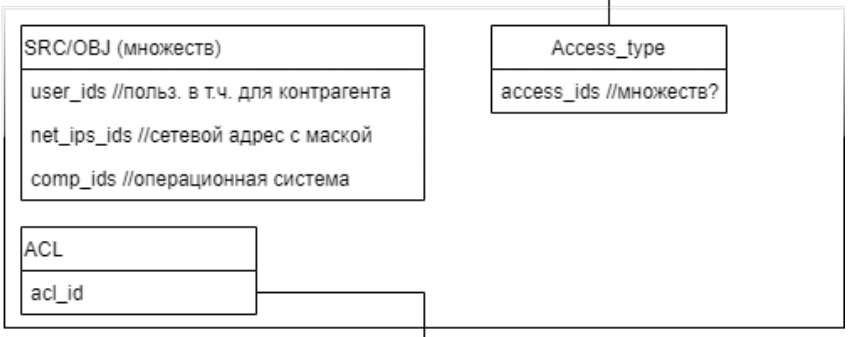


Access Control Entry

Запись о доступе конкретного объекта: пользователя, компьютера, сетевого диапазона

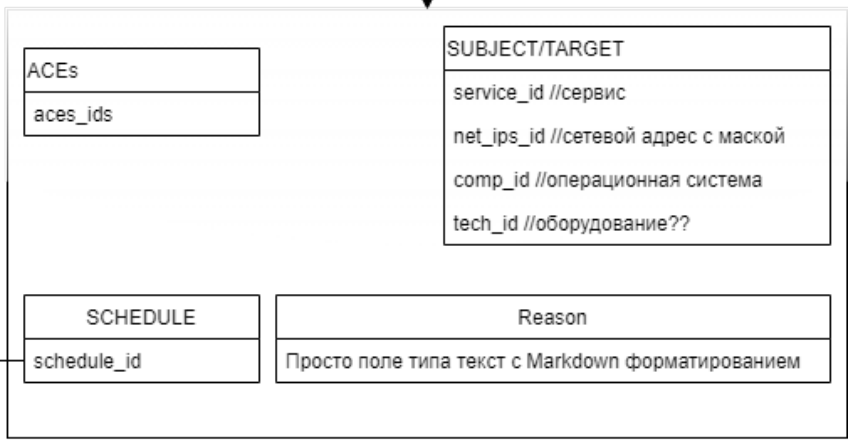
Конкретным способом (чтение/запись/протокол и т.п.). Способы - просто названия из списка, который можно пополнять

прикрепляется к ACL



Access Control List

Список доступов (ACE) к какому либо **ресурсу** в течение какого либо **времени** на каком то **основании**



Schedule

Используем стандартные объекты типа расписание, но в интерфейсе подавляем часть, обеспечивающую ежедневное и еженедельные расписания. Оставляем только периоды включения и выключения

Если расписание не объявлено - ACL действует всегда.
Если объявлено, то только на время из расписания (по умолчанию расписание - пустое. Т.е. до добавления первого периода включения ACL не действует)

Schedule Period

Собственно стандартные объекты рабочих/нерабочих периодов в расписании.

Вероятно поле комментарий надо сделать тоже в Markdown. А может хватит и так. В него нужно вносить основание для продления доступа на новый период (номер СЗ)

Получается при получении служебки на предоставление доступа группе пользователей

- к удаленному доступу (пользователь → сервис Wireguard)
- к своему компу по RDP (пользователь,ip → ОС по RDP)

Будет порождаться грядка ACL:

- 1шт на доступ пользователей к сервису
- Nшт на доступ [VPN IP пользователя, учетки пользователя] по RDP к целевой ОС

Все они будут связаны через расписание. Что довольно странно Но получается, что в расписании есть все необходимые поля для этого и если других полей не нужно, то дополнительная сущность будет избыточной (тут приходит Оккам и угрожает бритвой)

Также получается что основание предоставления доступа можно вписывать двояко (есть поле в самом ACL и в каждом периоде предоставления)

Работать с самими ACL в чистом виде вероятно будет неудобно, хотя мало где работа с ACL идет отдельно от субъектов. В нашем случае можно будет наверно сделать таблицу

объект	**доступ**	**субъект**	**активность ACL (в наст время исходя из расписания)**
Пупкин	RDP обрезанный	PUPKIN-IA	активен

и по ней искать/просматривать доступы конкретных людей к конкретным ресурсам также очевидно что предоставленные доступы будет видно на страничке объекта и ресурса

Доступ к сложным объектам наверно надо будет реализовывать через ресурсы-сервисы (которые сами по себе комплексный объект, включающий в себя и ОС и оборудование и субсервисы). Ну т.е. если мы в кластер терминалов добавили еще один сервер - не должно быть необходимо переделывать все ACL. Нужно добавить сервер в сервис и все. Попробуем на первое время так ограничиваться. Если этого будет мало - там посмотрим в сторону сборных таргетов/ресурсов.