SA New Auth

Проблема

На настоящий момент логины и пароли на доступы на каждую железку задаются независимо, что приводит к ряду неудобств:

- При вводе новых железок приходится каждый раз вбивать логин и пароль для доступа, даже если используются системы аутентификации RADIUS и TACACS+ и логины и пароли для группы железа совпадают
- При изменении логина и пароля на RADIUS приходится изменять множество записей в базе руками
- Нет возможности использовать логины и пароли текущего пользователя (например, в sa.managedobject > console)

Предлагаемое решение

Auth Profile

Вводим сущность AuthProfile, как множество Managed Object с совпадающими реквизитами доступа

Поле	Тип	Constraint	Описание
id	INTEGER	NOT NULL PRIMARY KEY	Уникальный идентификатор
name	VARCHAR	NOT NULL UNIQUE	Уникальное название AuthProfile
type	VARCHAR	NOT NULL	Тип профиля. Одно из: • localgroup – локальная база пользователей для железки, при этом в пределах группы логины и пароли совпадают (административное ограничение) • radius – RADIUS authentication • tacplus – TACACS+ authentication • ldap - LDAP authentication
user	VARCHAR		Имя пользователя, используется NOC по умолчанию
password	VARCHAR		Пароль
super_password	VARCHAR		Пароль на дополнительные функции, в случае необходимости (enable для Cisco)
snmp_ro	VARCHAR		SNMP RO community
snmp_rw	VARCHAR		SNMP RW community

Доработка ManagedObject

В таблицу sa_managedobject добавляется поле

Поле	Тип	Constraint	Описание
auth_profile_id	INTEGER	REFERENCES sa_authprofile	Ссылка на AuthProfile

Алгоритм определения логина и пароля для доступа к железке

- Если тип auth_profile_id IS NULL – используем логины и пароли, заданные в sa_managedobject
- В противном случае используем логины и пароли из auth profile

Авторизация пользователей в консоли

Добавляем коллекцию noc.console_credentials

Поле	Тип	Описание
_id	ObjectId	Идентификатор записи
user	int	Идентификатор пользователя NOC
auth_profile	int	Идентификатор auth profile
managed_object	int	Идентификатор managed object'a (только для пустых auth_profile_id)
user	str	Имя пользователя
password	str	Пароль

В профиле пользователя необходимо добавить поле

Поле	Тип	Constraint	Описание
save_console_password	BOOLEAN		Сохранять ли пароли в консоли

Для определения имени пользователя и пароля для доступа на железку

- Если auth_profile пустое, ищем запись в noc.console_credentials по user и managed_object
- Если auth_profile непустое, то ищем запись в noc.console_credentials по user и auth_profile
- Если сохраненный пароль не найден - спрашиваем
- Если в профиле пользователя установлен save_console_password - сохраняем пароль в noc.console_credentials

Доработки SAE

В таблице map_task придется добавить поле credentials, с возможностью задавать логины и пароли для запуска скрипта

Дальнейшее развитие

Возможно создание каналов синхронизации для noc-sync для автоматического provisioning RADIUS и TACACS+ для централизованного управления учетными записями через NOC