Описание политик стандартной ролевой модели

1. Общее описание

При создании тенанта создается древовидная структура каталогов. Для управления доступом каждому каталогу сопоставляется роль.

Стандартная ролевая модель определяет два набора ролей – пользовательский (для пользователей системы ЦУП 2.0) и административный (для администраторов системы ЦУП 2.0).

Пользовательский набор ролей в тенанте (ветвь секретов АС):

1. Владелец ТУЗ зоны АС.
2. Аудитор зоны АС.
3. Владелец ТУЗ блока.
4. Владелец ТУЗ пространства имен.
5. Владелец ТУЗ проектной области/доп. пространства.
6. Пользователь проектной области/доп. пространства.
7. Просмотрщик проектной области/доп. пространства.

Административный набор ролей:

1. Суперадмин.
2. Админ.
3. В разработке

2. Описание связывания пользователей Active Directory с ролями в тенанте ЦУП 2.0

Чтобы управлять назначением политик на конкретных пользователей, используется следующая схема:

1. Для каждой роли в Active Directory создается группа.
2. Для каждой роли в ЦУП 2.0 создается external group, на которую назначается политика, соответствующая роли.
3. Каждая группа в ЦУП 2.0 связывается с соответствующей группой в AD.
4. Администратор ЦУП 2.0 помещает пользователя в группу AD, которая соответствует необходимой роли.

5. Пользователь логинится с использованием учетных данных Active Directory и получает токен с правами, назначенными на все группы, которые связаны с группами AD, в которые входит пользователь.

3. Описание пользовательских политик доступа

Для каждой из перечисленных ролей создается политика доступа, которая определяет права доступа на соответствующий каталог и все вложенные в него каталоги. Политика именуется таким образом, чтобы отражать конкретную роль (ссылка на раздел «Создание политики при помощи файла» в инструкции по выдаче прав).

Примечания:

а) постфиксы в именах политик “ao”, “ac” и “aa” означают, что политика принадлежит роли “ao” - “Owner”(Владелец), “ac” - “Consumer” (Пользователь) и “aa” – “Auditor” (Аудитор, просмотрщик списка секретов)

б) постфиксы <ad_name> в именах external group – обозначают сегмент, для которого создается группа, для сегментов “a” - “alpha”, “s” - “sigma”, “o” - “omega” и “d” - “delta”. **Важно!** Постфиксы могут быть переопределены в настройках.

Роль	Политика

Владелец ТУЗ зоны АС	**Наименование политики**:
	
	{имя_тенанта}_a_ao
	
	Наименование external group:
	
	{имя_тенанта}_a_ao_<ad_name>
	Текст:
	path "/{имя_тенанта}/as/*" {
	
	capabilities = ["create", "read", "update", "delete", "list"]
	
	}

Аудитор зоны АС	**Наименование политики**:
	
	{имя_тенанта}_a_aa
	
	Наименование external group:
	
	{имя_тенанта}_a_aa_<ad_name>
	Текст:
	path "/{имя_тенанта}/as/*" {
	
	capabilities = ["list"]
	
	}

Владелец ТУЗ блока	**Наименование политики**: {имя_тенанта}_a_{имя_блока}_ao **Наименование external group**:

	{имя_тенанта}_a_{имя_блока}_ao _<ad_name>
	Текст:
	path "/{имя_тенанта}/as/{имя_блока}*" {
	
	capabilities = ["create", "read", "update", "delete", "list"]
	
	}

Владелец ТУЗ пространства имен	**Наименование политики**:
	
	{имя_тенанта}_a_{имя_блока}_{имя_пространства}_ao
	
	Наименование external group:
	
	{имя_тенанта}_a_{имя_блока}_{имя_пространства}_ao_<ad_name>
	Текст:
	path "/{имя_тенанта}/as/{имя_блока}/{имя_пространства}/*" {
	
	capabilities = ["create", "read", "update", "delete", "list"]
	
	}

Владелец ТУЗ проектной области/доп. пространства	**Наименование политики**:
	
	{имя_тенанта}_a_{имя_блока}_{имя_пространства}_{имя_доп_пространства}_ao
	Наименование external group:
	
	{имя_тенанта}_a_{имя_блока}_{имя_пространства}_{имя_доп_пространства}_ao_
	<ad_name>
	
	Текст:
	path
	"/{имя_тенанта}/as/{имя_блока}/{имя_пространства}/{имя_доп_пространства}/*" {
	
	capabilities = ["create", "read", "update", "delete", "list"]
	
	}

Пользователь проектной области/доп. пространства	**Наименование политики**:
	
	{имя_тенанта}_a_{имя_блока}_{имя_пространства}_{имя_доп_пространства}_ac
	
	Наименование external group:
	
	{имя_тенанта}_a_{имя_блока}_{имя_пространства}_{имя_доп_пространства}_ac_
	<ad_name>
	
	Текст:
	path
	"/{имя_тенанта}/as/{имя_блока}/{имя_пространства}/{имя_доп_пространства}/*" {
	
	capabilities = ["read", "list"]
	
	}

Просмотр проектной	**Наименование политики**: {имя_тенанта}_a_{имя_блока}_{имя_пространства}_{имя_доп_пространства}_aa **Наименование external group**:

области/доп пространства	{имя_тенанта}_a_{имя_блока}_{имя_пространства}_{имя_доп_пространства}_aa_<ad_name>
	
	Текст:
	path "/{имя_тенанта}/as/{имя_блока}/{имя_пространства}/{имя_доп_пространства}/*" {
	
	capabilities = ["list"]
	
	}