**Управление политиками аутентификации**

Для работы с политиками аутентификации (authentication policy) с помощью утилиты samba-tool используется группа подкоманд domain auth policy.

**Общие сведения**

Политики аутентификации (authentication policy) определяют правила аутентификации учетных записей пользователей, компьютеров и сервисных учетных записей в доменах Active Directory (AD). Правила аутентификации могут применяться для контроля входа в операционную систему на определенных компьютерах в домене, а также для контроля доступа к службам, которые выполняются от имени сконфигурированных в AD учетных записей.

Например, с помощью политик аутентификации учетные записи пользователей с расширенными полномочиями могут быть привязаны к компьютерам, с которых выполняются задачи администрирования, а учетные записи рядовых пользователей — к их рабочим станциям.

Политики аутентификации могут назначаться пользователям непосредственно или с использованием силосов (silo). Силос может применять либо одну и ту же политику к разным типам учетных записей, либо разные политики к учетным записям пользователей, компьютеров и сервисов.

Механизм действия политик основан на расширениях протокола Kerberos и влияет на формирование как билетов TGT (Ticket-Granting Ticket) — для аутентификации пользователей при входе в операционную систему и аутентификации учетных записей при доступе к службам, так и билетов ST (Service Ticket) — для аутентификации учетных записей при доступе к службам.

Если политика применяется при выдаче билета TGT учетной записи, выполняющей аутентификацию, то такой билет TGT становится невозобновляемым (non-renewable) и к нему может применяться дополнительное ограничение на срок действия.

В рамках политики определяются критерии, которым должны удовлетворять учетные записи, выполняющие аутентификацию, и компьютеры, на которых выполняется аутентификация. При этом при аутентификации учетной записи в билеты TGT и ST добавляется специальное утверждение (claim), например, характеризующее силос, в который входит учетная запись, или основанное на атрибутах этой учетной записи .

Учетные записи, к которым применяются политики, могут как быть, так и не быть членами группы Protected Users.

**Получение списка политик аутентификации в домене**

Формат вызова:

samba-tool domain auth policy list [-H <URL>] [options]

Подкоманда выводит простой список политик аутентификации, доступных в контейнере CN=AuthN Policies,CN=AuthN Policy Configuration,CN=Services,CN=Configuration,DC=domain,DC=name, либо (при передаче параметра --json) — подробную информацию по каждой из настроенных политик аутентификации в формате JSON.

**Параметры**

Параметры вызова:

* -H URL|--URL=URL — адрес сервера LDAP; может содержать указание на протокол, имя хоста и номер порта;
* --json — вывод атрибутов политик аутентификации в формате JSON.

**Примеры**

Пример получения списка политик аутентификации в домене:

samba-tool domain auth policy list

AuthPolicy1

AuthPolicy2

AuthPolicy3

**Получение информации о политике аутентификации**

Формат вызова:

samba-tool domain auth policy view [-H <URL>] [options]

Подкоманда выводит атрибуты политики аутентификации с указанным CN (--name) в формате JSON.

**Параметры**

Параметры вызова:

* -H URL|--URL=URL — адрес сервера LDAP; может содержать указание на протокол, имя хоста и номер порта;
* --name=NAME (обязательный) — CN политики аутентификации, атрибуты которой требуется вывести.

**Примеры**

Пример получения атрибутов политики аутентификации:

samba-tool domain auth policy view \

--name=AuthPolicy1

{

"cn": "AuthPolicy1",

"distinguishedName": "CN=AuthPolicy1,CN=AuthN Policies,CN=AuthN Policy Configuration,CN=Services,CN=Configuration,DC=elles,DC=inno,DC=tech",

"dn": "CN=AuthPolicy1,CN=AuthN Policies,CN=AuthN Policy Configuration,CN=Services,CN=Configuration,DC=elles,DC=inno,DC=tech",

"instanceType": 4,

"msDS-AuthNPolicyEnforced": true,

"msDS-StrongNTLMPolicy": 0,

"msDS-UserAllowedToAuthenticateFrom": "O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/cn:20c7656fcc182bba == \"WIN1\"))",

"name": "AuthPolicy1",

"objectCategory": "CN=ms-DS-AuthN-Policy,CN=Schema,CN=Configuration,DC=elles,DC=inno,DC=tech",

"objectClass": [ "top", "msDS-AuthNPolicy" ], "objectGUID": "ab8f1da8-c6d3-4446-86c8-e59cf86c706f"}

**Создание политики аутентификации**

Формат вызова:

samba-tool domain auth policy create [-H <URL>] [options]

Подкоманда создает в контейнере AuthN Policies в каталоге новую политику аутентификации на основе переданных атрибутов.

Политика может создаваться в двух режимах:

* в режиме аудита (--audit) — политика фактически не применяется к объектам в домене; выполняется логирование потенциальных событий успешного или неуспешного выполнения аутентификации в соответствии с параметрами политики;
* в режиме применения (--enforce) — политика применяется к объектам в домене в соответствии с заданными параметрами (по умолчанию).

Атрибуты, описывающие правила аутентификации, могут устанавливаться следующими способами:

* присвоение выражения SDDL соответствующему атрибуту с помощью параметра подкоманды create;

Примеры выражений:

* + пример выражения для задания правила на основе утверждения:

O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/cn:20c7656fcc182bba == \"WIN1\"))

* + пример выражения для задания правила на основе членства в группе:

O:SYG:SYD:(XA;OICI;CR;;;WD;(Member\_of\_any {SID(S-1-5-21-1159061634-2679507100-403793082-2122)}))

* + пример выражения для задания правила на основе принадлежности силосу:

O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo == "AuthSilo1"))

* указание CN группы или силоса с помощью параметров отдельных подкоманд computer-allowed-to-authenticate-to, service-allowed-to-authenticate-from и др.

**Параметры**

Параметры вызова:

* -H URL|--URL=URL — адрес сервера LDAP; может содержать указание на протокол, имя хоста и номер порта;
* --name=NAME(обязательный) — CN политики аутентификации;
* --description=DESCRIPTION — описание для политики аутентификации;
* защита политики аутентификации от случайного удаления — одно из значений:
  + --protect — запрет на удаление политики аутентификации;
  + --unprotect — снятие запрета на удаление политики аутентификации;
* режим применения политики аутентификации — одно из значений:
  + --audit — режим логирования потенциальных событий успешного или неуспешного выполнения аутентификации в соответствии с параметрами политики;
  + --enforce — режим применения политики;
* --strong-ntlm-policy=Disabled|Optional|Required — значение для атрибута msDS-StrongNTLMPolicy;
* параметры правила для учетной записи компьютера:
  + --computer-tgt-lifetime-mins=TGT\_LIFETIME — срок действия билета TGT для учетной записи компьютера (значение в минутах в диапазоне от 45 до 2147483647);
  + --computer-allowed-to-authenticate-to=SDDL — строка с описанием разрешений в формате SDDL и условия доступа, которому должен удовлетворять пользователь для выполнения аутентификации в сервисе, работающем под учетной записью компьютера (сервер, рабочая станция);
* параметры правила для сервисной учетной записи:
  + --service-tgt-lifetime-mins=TGT\_LIFETIME — срок действия билета TGT для сервисной учетной записи (значение в минутах в диапазоне от 45 до 2147483647);
  + --service-allow-ntlm-auth — разрешить аутентификацию по протоколу NTLM, несмотря на ограничение доступа сервисной учетной записи определенными устройствами;
  + --service-allowed-to-authenticate-from=SDDL — строка с описанием разрешений в формате SDDL и условия доступа, которому должно удовлетворять устройство, используемое сервисной учетной записью для выполнения аутентификации;
  + --service-allowed-to-authenticate-to=SDDL — строка с описанием разрешений в формате SDDL и условия доступа, которому должен удовлетворять пользователь для выполнения аутентификации в сервисе, работающем под сервисной учетной записью;
* параметры правила для учетной записи пользователя:
  + --user-tgt-lifetime-mins=TGT\_LIFETIME — срок действия билета TGT для учетной записи пользователя (значение в минутах в диапазоне от 45 до 2147483647);
  + --user-allow-ntlm-auth — разрешить аутентификацию по протоколу NTLM, несмотря на ограничение доступа учетной записи пользователя определенными устройствами;
  + --user-allowed-to-authenticate-from=SDDL — строка с описанием разрешений в формате SDDL и условия доступа, которому должно удовлетворять устройство, используемое учетной записью пользователя для выполнения аутентификации;
  + --user-allowed-to-authenticate-to=SDDL — строка с описанием разрешений в формате SDDL и условия доступа, которому должен удовлетворять пользователь для выполнения аутентификации в сервисе, работающем под учетной записью пользователя.

**Примеры**

Пример создания политики аутентификации с указанием правила, определяющего, с какого устройства может выполнять аутентификацию пользователь, которому назначено данное правило:

samba-tool domain auth policy create \

--name=AuthPolicy1 \

--unprotect \

--enforce \

--user-allowed-to-authenticate-from="O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/cn:20c7656fcc182bba == \"WIN1\"))"

Created authentication policy: AuthPolicy1

**Изменение политики аутентификации**

Формат вызова:

samba-tool domain auth policy modify [-H <URL>] [options]

Подкоманда изменяет атрибуты политики аутентификации с указанным CN (--name) в соответствии с переданными значениями.

**Параметры**

Параметры вызова:

* -H URL|--URL=URL — адрес сервера LDAP; может содержать указание на протокол, имя хоста и номер порта;
* --name=NAME(обязательный) — CN политики аутентификации;
* --description=DESCRIPTION — описание для политики аутентификации;
* защита политики аутентификации от случайного удаления — одно из значений:
  + --protect — запрет на удаление политики аутентификации;
  + --unprotect — снятие запрета на удаление политики аутентификации;
* режим применения политики аутентификации — одно из значений:
  + --audit — режим логирования потенциальных событий успешного или неуспешного выполнения аутентификации в соответствии с параметрами политиками;
  + --enforce — режим применения политики;
* --strong-ntlm-policy=Disabled|Optional|Required — значение для атрибута msDS-StrongNTLMPolicy;
* параметры правила для учетной записи компьютера:
  + --computer-tgt-lifetime-mins=TGT\_LIFETIME — срок действия билета TGT для учетной записи компьютера (значение в минутах в диапазоне от 45 до 2147483647);
  + --computer-allowed-to-authenticate-to=SDDL — строка с описанием разрешений в формате SDDL и условия доступа, которому должен удовлетворять пользователь для выполнения аутентификации в сервисе, работающем под учетной записью компьютера (сервер, рабочая станция);
* параметры правила для сервисной учетной записи:
  + --service-tgt-lifetime-mins=TGT\_LIFETIME — срок действия билета TGT для сервисной учетной записи (значение в минутах в диапазоне от 45 до 2147483647);
  + --service-allow-ntlm-auth — разрешить аутентификацию по протоколу NTLM, несмотря на ограничение доступа сервисной учетной записи определенными устройствами;
  + --service-allowed-to-authenticate-from=SDDL — строка с описанием разрешений в формате SDDL и условия доступа, которому должно удовлетворять устройство, используемое сервисной учетной записью для выполнения аутентификации;
  + --service-allowed-to-authenticate-to=SDDL — строка с описанием разрешений в формате SDDL и условия доступа, которому должен удовлетворять пользователь для выполнения аутентификации в сервисе, работающем под сервисной учетной записью;

|  |  |
| --- | --- |
|  |  |

* параметры правила для учетной записи пользователя:
  + --user-tgt-lifetime-mins=TGT\_LIFETIME — срок действия билета TGT для учетной записи пользователя (значение в минутах в диапазоне от 45 до 2147483647);
  + --user-allow-ntlm-auth — разрешить аутентификацию по протоколу NTLM, несмотря на ограничение доступа учетной записи пользователя определенными устройствами;
  + --user-allowed-to-authenticate-from=SDDL — строка с описанием разрешений в формате SDDL и условия доступа, которому должно удовлетворять устройство, используемое учетной записью пользователя для выполнения аутентификации;

|  |  |
| --- | --- |
|  |  |

* + --user-allowed-to-authenticate-to=SDDL — строка с описанием разрешений в формате SDDL и условия доступа, которому должен удовлетворять пользователь для выполнения аутентификации в сервисе, работающем под учетной записью пользователя.

|  |  |
| --- | --- |
|  |  |

**Примеры**

Пример изменения атрибута --service-allowed-to-authenticate-from политики аутентификации:

samba-tool domain auth policy modify \

--name=AuthPolicy1 \

--service-allowed-to-authenticate-from="O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo == \"AuthSilo1\"))"

Updated authentication policy: AuthPolicy1

**Удаление политики аутентификации**

Формат вызова:

samba-tool domain auth policy delete [-H <URL>] [options]

Подкоманда удаляет политику аутентификации с указанным CN (--name), если для нее не установлен атрибут --protect. Если при вызове команды передается параметр --force, выполняется принудительное удаление политики аутентификации.

**Параметры**

Параметры вызова:

* -H URL|--URL=URL — адрес сервера LDAP; может содержать указание на протокол, имя хоста и номер порта;
* --name=NAME (обязательный) — CN политики аутентификации, которую требуется удалить;
* --force — принудительное удаление политики аутентификации.

**Примеры**

Пример удаления политики аутентификации:

samba-tool domain auth policy delete \

--name=AuthPolicy1

Deleted authentication policy: AuthPolicy1

**Установка атрибута computer-allowed-to-authenticate-to для политики аутентификации**

Формат вызова:

samba-tool domain auth policy computer-allowed-to-authenticate-to set [-H <URL>] [options]

Подкоманда устанавливает значение атрибута computer-allowed-to-authenticate-to для политики аутентификации с указанным CN (--name) в соответствии с требуемым сценарием аутентификации:

* для аутентификации в сервисе, работающем под учетной записью компьютера, пользователь должен состоять в группе, указанной с помощью параметра --by-group;

В этом случае в качестве значения атрибут получает автоматически сформированную строку в формате SDDL с описанием правила аутентификации, содержащую условия принадлежности группе и идентификатор безопасности (SID) группы.

* для аутентификации в сервисе, работающем под учетной записью компьютера, пользователь должен быть включен в силос, указанный с помощью параметра --by-silo.

В этом случае в качестве значения атрибут получает автоматически сформированную строку в формате SDDL с описанием правила аутентификации, содержащую условия принадлежности силосу и CN силоса.

**Параметры**

Параметры вызова:

* -H URL|--URL=URL — адрес сервера LDAP; может содержать указание на протокол, имя хоста и номер порта;
* --name=NAME (обязательный) — CN политики аутентификации, для которой требуется задать значение атрибута;
* --by-group — CN группы, в которой должен состоять пользователь для выполнения аутентификации в сервисе, работающем под учетной записью компьютера;
* --by-silo — CN силоса, в который должен быть включен пользователь для выполнения аутентификации в сервисе, работающем под учетной записью компьютера.

|  |  |
| --- | --- |
|  | Параметры --by-group и --by-silo являются взаимоисключающими. |

**Примеры**

Пример установки значения атрибута:

samba-tool domain auth policy computer-allowed-to-authenticate-to set \

--name=AuthPolicy1 \

--by-silo=AuthSilo1

Updated authentication policy: AuthPolicy1

Updated SDDL: O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo == "AuthSilo1"))

**Установка атрибута service-allowed-to-authenticate-from для политики аутентификации**

Формат вызова:

samba-tool domain auth policy service-allowed-to-authenticate-from set [-H <URL>] [options]

Подкоманда устанавливает значение атрибута service-allowed-to-authenticate-from для политики аутентификации с указанным CN (--name) в соответствии с требуемым сценарием аутентификации:

* для выполнения аутентификации устройство, используемое сервисной учетной записью, должно состоять в группе, указанной с помощью параметра --device-group;

В этом случае в качестве значения атрибут получает автоматически сформированную строку в формате SDDL с описанием правила аутентификации, содержащую условия принадлежности группе и идентификатор безопасности (SID) группы.

* для выполнения аутентификации устройство, используемое сервисной учетной записью, должно быть включено в силос, указанный с помощью параметра --device-silo.

В этом случае в качестве значения атрибут получает автоматически сформированную строку в формате SDDL с описанием правила аутентификации, содержащую условия принадлежности силосу и CN силоса.

**Параметры**

Параметры вызова:

* -H URL|--URL=URL — адрес сервера LDAP; может содержать указание на протокол, имя хоста и номер порта;
* --name=NAME (обязательный) — CN политики аутентификации, для которой требуется задать значение атрибута;
* --device-group — CN группы, в которой должно состоять устройство, используемое сервисной учетной записью, для выполнения аутентификации;
* --device-silo — CN силоса, в который должно быть включено устройство, используемое сервисной учетной записью, для выполнения аутентификации.

|  |  |
| --- | --- |
|  | Параметры --device-group и --device-silo являются взаимоисключающими. |

**Примеры**

Пример установки значения атрибута:

samba-tool domain auth policy service-allowed-to-authenticate-from set \

--name=AuthPolicy1 \

--device-silo=AuthSilo1

Updated authentication policy: AuthPolicy1

Updated SDDL: O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo == "AuthSilo1"))

**Установка атрибута service-allowed-to-authenticate-to для политики аутентификации**

Формат вызова:

samba-tool domain auth policy service-allowed-to-authenticate-to set [-H <URL>] [options]

Подкоманда устанавливает значение атрибута service-allowed-to-authenticate-to для политики аутентификации с указанным CN (--name) в соответствии с требуемым сценарием аутентификации:

* для аутентификации в сервисе, работающем под сервисной учетной записью, пользователь должен состоять в группе, указанной с помощью параметра --by-group;

В этом случае в качестве значения атрибут получает автоматически сформированную строку в формате SDDL с описанием правила аутентификации, содержащую условия принадлежности группе и идентификатор безопасности (SID) группы.

* для аутентификации в сервисе, работающем под сервисной учетной записью, пользователь должен быть включен в силос, указанный с помощью параметра --by-silo.

В этом случае в качестве значения атрибут получает автоматически сформированную строку в формате SDDL с описанием правила аутентификации, содержащую условия принадлежности силосу и CN силоса.

**Параметры**

Параметры вызова:

* -H URL|--URL=URL — адрес сервера LDAP; может содержать указание на протокол, имя хоста и номер порта;
* --name=NAME (обязательный) — CN политики аутентификации, для которой требуется задать значение атрибута;
* --by-group — CN группы, в которой должен состоять пользователь для выполнения аутентификации в сервисе, работающем под сервисной учетной записью;
* --by-silo — CN силоса, в который должен быть включен пользователь для выполнения аутентификации в сервисе, работающем под сервисной учетной записью.

|  |  |
| --- | --- |
|  | Параметры --by-group и --by-silo являются взаимоисключающими. |

**Примеры**

Пример установки значения атрибута:

samba-tool domain auth policy service-allowed-to-authenticate-to set \

--name=AuthPolicy1 \

--by-silo=AuthSilo1

Updated authentication policy: AuthPolicy1

Updated SDDL: O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo == "AuthSilo1"))

**Установка атрибута user-allowed-to-authenticate-from для политики аутентификации**

Формат вызова:

samba-tool domain auth policy user-allowed-to-authenticate-from set [-H <URL>] [options]

Подкоманда устанавливает значение атрибута user-allowed-to-authenticate-from для политики аутентификации с указанным CN (--name) в соответствии с требуемым сценарием аутентификации:

* для выполнения аутентификации устройство, используемое учетной записью пользователя, должно состоять в группе, указанной с помощью параметра --device-group;

В этом случае в качестве значения атрибут получает автоматически сформированную строку в формате SDDL с описанием правила аутентификации, содержащую условия принадлежности группе и идентификатор безопасности (SID) группы.

* для выполнения аутентификации устройство, используемое учетной записью пользователя, должно быть включено в силос, указанный с помощью параметра --device-silo.

В этом случае в качестве значения атрибут получает автоматически сформированную строку в формате SDDL с описанием правила аутентификации, содержащую условия принадлежности силосу и CN силоса.

**Параметры**

Параметры вызова:

* -H URL|--URL=URL — адрес сервера LDAP; может содержать указание на протокол, имя хоста и номер порта;
* --name=NAME (обязательный) — CN политики аутентификации, для которой требуется задать значение атрибута;
* --device-group — CN группы, в которой должно состоять устройство, используемое учетной записью пользователя, для выполнения аутентификации;
* --device-silo — CN силоса, в который должно быть включено устройство, используемое учетной записью пользователя, для выполнения аутентификации.

|  |  |
| --- | --- |
|  | Параметры --device-group и --device-silo являются взаимоисключающими. |

**Примеры**

Пример установки значения атрибута:

samba-tool domain auth policy user-allowed-to-authenticate-from set \

--name=AuthPolicy1 \

--device-silo=AuthSilo1

Updated authentication policy: AuthPolicy1

Updated SDDL: O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo == "AuthSilo1"))

**Установка атрибута user-allowed-to-authenticate-to для политики аутентификации**

Формат вызова:

samba-tool domain auth policy user-allowed-to-authenticate-to set [-H <URL>] [options]

Подкоманда устанавливает значение атрибута user-allowed-to-authenticate-to для политики аутентификации с указанным CN (--name) в соответствии с требуемым сценарием аутентификации:

* для аутентификации в сервисе, работающем под пользовательской учетной записью, пользователь должен состоять в группе, указанной с помощью параметра --by-group;

В этом случае в качестве значения атрибут получает автоматически сформированную строку в формате SDDL с описанием правила аутентификации, содержащую условия принадлежности группе и идентификатор безопасности (SID) группы.

* для аутентификации в сервисе, работающем под пользовательской учетной записью, пользователь должен быть включен в силос, указанный с помощью параметра --by-silo.

В этом случае в качестве значения атрибут получает автоматически сформированную строку в формате SDDL с описанием правила аутентификации, содержащую условия принадлежности силосу и CN силоса.

**Параметры**

Параметры вызова:

* -H URL|--URL=URL — адрес сервера LDAP; может содержать указание на протокол, имя хоста и номер порта;
* --name=NAME (обязательный) — CN политики аутентификации, для которой требуется задать значение атрибута;
* --by-group — CN группы, в которой должен состоять пользователь для выполнения аутентификации в сервисе, работающем под пользовательской учетной записью;
* --by-silo — CN силоса, в который должен быть включен пользователь для выполнения аутентификации в сервисе, работающем под пользовательской учетной записью.

|  |  |
| --- | --- |
|  | Параметры --by-group и --by-silo являются взаимоисключающими. |

**Примеры**

Пример установки значения атрибута:

samba-tool domain auth policy user-allowed-to-authenticate-to set \

--name=AuthPolicy1 \

--by-silo=AuthSilo1

Updated authentication policy: AuthPolicy1

Updated SDDL: O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo == "AuthSilo1"))