

Интеграция с Active Directory в платформе виртуализации РУСТЭК

### Содержание

ВВЕДЕНИЕ	3
1 Настройка сервера AD	4
2 Настройка конфигуратора РУСТЭК	7
3 Управление пользователями AD в портале РУСТЭК	10
4 Варианты поломок и методы их устранения	11

#### ВВЕДЕНИЕ

В платформе РУСТЭК есть возможность использовать Active Directory (далее AD) как внешний сервер аутентификации. Пользователи, находящиеся в AD и помещенные в определенную группу, могут аутентифицироваться на платформе РУСТЭК для управления инфраструктурой.

#### 1 Настройка сервера AD

Для интеграции с AD сначала необходимо выполнить соответствующую настройку.

В первую очередь следует создать пользователя с правами вывода списка остальных пользователей РУСТЭК и установить для него пароль (рисунок 1).

▲ Данного пользователя, как и других пользователей для РУСТЭК, необходимо создавать только в контейнере, который создан по умолчанию AD – "Users".

Active Directory Users and Computers           File         Action         View         Help				×
🔶 🔿 🖄 🛅 🛣 📾	@ 📾   🛙 📷   🐍 📚 🖆 🍞 🧕 🍇			
Active Directory Users and Comput Saved Queries Saved Queries Saved Queries Saved Queries Sustaination Computers Solution Solution Solution Active Directory Users and Compute Solution	ters [dc.rust Name Type Description Administrator User Built-in account for Allowed RO Security Group Members in this gr Cert Publish Security Group Members of this gr Coneable D Security Group Members of this gr Coneable D Security Group Members of this gr DefaultAcco User A user account ma DefaultAcco User A user account ma DefaultAcco User DNS Administrator DnsAdmins Security Group DNS Administrator DNS Clients who ar Domain Ad Security Group DNS clients who ar Domain Co Security Group All workstations ar Domain Gue Security Group All domain control Domain Gue Security Group All domain guests Domain Users Security Group All domain users	or ad roup c roup t anage roup c rs Gro rs Gro re per istrato nd ser llers i		
> I NTD Find	IIIII Marchine Construction and the security Group Designated admini Construction and the security Group Members of this g	istrato roup		
TPM New All Tasks View Refresh Export List Properties Help Conductor point in terms	Computer       of this gr         Contact       count for         Group       of this gr         InetOrgPerson       pution Co         msDS-KeyCredential       of this gr         msDS-ResourcePropertyList       of this gr         msDS-ShadowPrincipalContainer       of this gr         msImaging-PSPs       MSMQ Queue Alias         Printer       Vser	roup or gue or gue roup roup up can roup istrato		
Create a new object	Shared Folder			

Рисунок 1. Создание нового пользователя

Затем необходимо создать группу, позволяющую добавлять (создавать) в неё других пользователей РУСТЭК (рисунок 2).

Active Directory Users and Computers				_	×	
<u>File</u> <u>Action</u> <u>V</u> iew <u>H</u> elp						
	51 % 🗽 🛅	7 🗾 🐍				
Active Directory Users and Computers [dc.rust >  Saved Queries	Name 🛃 Administrator	Type User	Descriptio Built-in ac	n :count for ad		
<ul> <li>Fig. Tustack local</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipals</li> <li>Keys</li> </ul>	Allowed RO Cert Publish Cloneable D DefaultAcco DefaultAcco	Security Group Security Group Security Group User Security Group	Members Members A user acc Members	in this group c of this group of this group t count manage in this group c		
<ul> <li>LostAndFound</li> <li>Managed Service Accounts</li> <li>Program Data</li> <li>Roles</li> <li>System</li> <li>Tenants</li> </ul>	DonsAdmins DnsUpdateP Domain Ad Domain Co Domain Con Domain Gue	Security Group Security Group Security Group Security Group Security Group Security Group	DNS Adm DNS client Designate All workst All domain All domain	inistrators Gro ts who are per d administrato ations and ser n controllers i n guests		
> Delegate Control > NTDS Find	Enterprise A	Security Group Security Group	Designate Members	d administrato of this group		
New >	Computer			of this group in this group c		
All Tasks >	Group	N		count for gue of this group		
Refresh Export List	InetOrgPerson <sup>VS</sup> ut msDS-KeyCredential of msDS-ResourcePropertyList :hi		ution Center of this group :his group can			
Properties	msDS-ShadowPrincipalContainer of this group		of this group			
Help	msImaging-PSPs MSMQ Queue Alias					
< >> Create a new object	Printer User Shared Folder	r				

Рисунок 2. Создание новой группы

👃 Все пользователи должны находиться в контейнере "Users".

Теперь можно создавать других пользователей, задавать им пароль, либо добавлять существующих из AD в созданную группу (рисунок 3).

File Action View Help				
← ⇒ 2 📷 ¼ 📋 🗙 🖾 @ 🕞 🛛 📷 % 🗞 🛅 🔻 🧕 🍇				
Active Directory Users and Computers [dc.rust Name Type Description				
Image: Security Principals       Image: Administrator U       Copy       br ad         Image: Security Principals       Image: Copy and Co				
Select Groups X Interview Construction Const				
Select this object type: Conups or Built-in security principals Object Types Object Types				
From this location:     Members of this group       rustack.local     Locations       Members of this group				
Enter the object names to select ( <u>examples</u> ):          ustack       Check Names       Servers in this group can         Members of this group       Designated administrato				
Advanced     OK Cancel				

Рисунок 3. Добавление в группу

После выполнения указанных выше действий настройка со стороны AD считается завершённой. Далее необходимо выполнить настройку в конфигураторе РУСТЭК.

### 2 Настройка конфигуратора РУСТЭК

Для настройки AD в конфигураторе РУСТЭК необходимо перейти в раздел «Интеграция с Active Directory», заполнить все необходимые поля и поставить флажок X в поле «Интеграция с AD» (рисунок 4).

РУС	СТЭК Конфигуратор	
>	Интеграция с Active Directory	
>	Интеграция с AD	[ <u>X</u> ]
>	Полное имя домена AD (FQDN)	rustack.local
	Короткое имя домена	rustack
>	IP-agpec AD	10.11.2.202
>	Полное СN сервисного пользователя	a cn=admin,cn=Users,dc=ru
>		stack,dc=local
	Пароль сервисного пользователя	*****
>	Фильтр пользователей в AD	(memberOf=cn=rustack,cn
		=Users,dc=rustack,dc=lo cal)
	CN контейнера с пользователями	cn=Users,dc=rustack,dc=
	•	local
	Логин администратора	admin
	Пароль администратора	*****
	< Применить >< 0	Этмена >

Рисунок 4. РУСТЭК Конфигуратор. Интеграция с AD

В таблице 1 представлено описание полей для заполнения.

Таблица 1. Поля для заполнения в окне **Интеграция с AD** в РУСТЭК Конфигураторе

Параметр	Описание
Полное имя домена AD (FQDN)	Полное имя домена, использующееся в AD, без точки в конце
Короткое имя домена	Имя, получаемое с сервера AD, указано в свойствах домена (рисунок 5)
IP-адрес AD	IP-адрес сервера AD
Полное CN сервисного пользователя	Имя пользователя в формате distinguishedName
Пароль сервисного пользователя	Пароль сервисного пользователя, который задавался при его создании в AD
Фильтр пользователей в AD	Фильтр, по которому будет происходит поиск пользователей, указанных в группе (создана ранее в AD)
CN контейнер с пользователями	Контейнер, в котором находятся пользователи для интеграции с РУСТЭК (только созданный по умолчанию - "Users")
Логин администратора	Пользователь (только admin), который будет создан в РУСТЭК для управления пользователями из AD (также пользователями из AD может управлять администратор РУСТЭК)
Пароль администратора	Пароль администратора, который будет создан в РУСТЭК

Active Directory Users and Computers	X
File Action View Help	rustack.local Properties ? X
🗢 🔿   🚈 💼   🗎   🗟 🗟 🗟   🖬 🛪 🐚 🔻	General Managed By Object Security Attribute Editor
Active Directory Users and Computers [dc.rust       Name         Saved Queries       Builtin         Builtin       Delegate Control         Compu       Find         Compu       Find         Foreign       Change Domain         Keys       Change Domain Controller         CostAnc       Raise domain functional level         Prograr       New         System       All Tasks         System       View         View       Yiew         NDD       Refresh         TPM De       Export List	Image by Object Security Public Editor       Image by Object Secure       Image by Object Security Public Pub
rich	OK Cancel Apply Help

Рисунок 5. Имя домена, получаемое с сервера AD

После полной настройки конфигуратора РУСТЭК (см. документы «Установка РУСТЭК. Быстрый старт» и «Описание конфигуратора РУСТЭК») и применения конфигурации РУСТЭК можно управлять пользователями AD в портале РУСТЭК.

#### 3 Управление пользователями AD в портале РУСТЭК

Для авторизации пользователя в портале необходимо ввести имя пользователя AD в формате: <имя@полное имя домена>.

При блокировке пользователя в AD он также блокируется в РУСТЭК.

При удалении пользователя из группы ему запрещена авторизация в РУСТЭК.

#### 4 Варианты поломок и методы их устранения

## 1. Выполнена настройка в AD и в конфигураторе, но пользователь не смог зайти в портал.

Возможные причины:

- Пользователь AD не добавлен в соответствующую группу;
- Пользователь не находится в контейнере по умолчанию «Users»;
- Неправильно выполнена настройка. Для этого можно проверить доступность AD и список пользователей командой на рисунке 6.

ldapsearch -b 'cn=Users,dc=rustack,dc=local' -H ldap://<IP> -w <PASSWORD> -D cn=admin,cn=Users,dc=rustack,dc=local '(&(memberOf=cn=rustack,cn=Us ers,dc=rustack,dc=local)(objectClass=person)(cn=\*))'

Рисунок 6. Команда для просмотра доступности AD и списка пользователей

Переменные указанные в команде на рисунке 6:

- b место, где происходит поиск;
- H URL AD;
- D указанное в binddn уникальное имя Distinguished Name при подсоединении к каталогу LDAP;
- memberOf... фильтр для поиска.

# 2. При работе в интерфейсе командной строки РУСТЭК некоторые команды Openstack выдают ошибку.

На рисунке 7 представлен вид ошибки.

You are not authorized to perform the requested action: identity:list\_users. (HTTP 403) (Request-ID: req-0c1178ee-8e11-4cd1-98c3-6dcddefc3641)

#### Рисунок 7. Вид ошибки

При работе в интерфейсе командной строки в командах Openstack необходимо указывать параметр *os-cloud*. В качестве примера команда представлена на рисунке 8.

openstack --os-cloud rustack\_system <команда>

Рисунок 8. Команда для параметра os-cloud