Active Directory

При использовании авторизации Active Directory (AD), сервер использует NTLM v2 и LDAP протоколы, для авторизации пользователей находящихся в Active Directory. Процесс авторизации происходит за 5 шагов:

1. Архива авторизуется с Active Directory при помощи служебного аккаунта (далее будет инструкция по созданию такого аккаунта)
2. Архива ищет пользователя в Active Directory используя логин
3. Архива сопоставляет (авторизует) логин пользователя и предоставленный пароль
4. Архива назначает роль согласно логину и настроенным правам
5. Архива извлекает почтовый ящик пользователя из атрибута LDAP, заданных в поле для поиска

Если вы переходите с более ранней версии Архива, вы должны знать, что механизм авторизации был изменен с Kerberos на NTLM v2 авторизацию.

ПРИ ОБНОВЛЕНИИ: Если вы обновляетесь с ранних версий Архива, вы должны знать, что механизм авторизации Архива поменялся с Kerberos на NTLM v2 авторизацию. Для NTLM v2 авторизации необходимо, чтобы сервисный учетная запись была учетной записью компьютера, а не обычного пользователя. Поэтому, для установки/обновления, вам необходимо создать учетную запись типа компьютер в AD, установить пароль этой учетной запись с помощью предоставляемых скриптов, и измените учетную запись в Архива на service$@business.local. Знак $ в UPN обозначает, что это учетная запись типа компьютер (в противовес учетной записи типа пользователь в AD).

Поле	Описание	Пример
DNS Сервер IP адрес	IP вашего сервера DNS	192.168.0.1
Active Directory Сервер Адреса	Полное доменное имя сервера Active Directory	active.business.local
Bind DN	Отличительное имя расположения в AD, где Архива должны начать поиск	dc=company,dc=com
Логин на чтение LDAP	Полное доменное имя (FQDN) сервисной учетной запись компьютера в AD.	service$@business.local
Пароль	Пароль сервисной учетной запись компьютера	
Email Attribute	Атрибут где содержится данные о почтовом адресе пользователя	ProxyAddresses
Значение сообщения	Регулярное выражение с помощью которого извлекается почтовый адрес пользователя из Email Attribute.	SMTP:(*.)
Bind Attribute	Данный атрибут используется для поиска логина пользователя в AD LDAP. Оставьте данный атрибут без изменений, для использования адреса электронной почты в логине, или используйте любой другой нужный вам атрибут.	SAMAccountName
NTLM SSO (единый пароль на вход) авторизация	Когда NTLM авотризация включена, Архива использует единый вход (SSO) сессии пользователя.	Disabled

В целях авторизации в Active Directory, Архива требует, чтобы новая учетная запись компьютера была создана в Active Directory и пароль для учетной записи установлен. Хоть и возможно создать новый компьютер в Active Directory Users And Computers с помощью графического интерфейса, но к сожалению задать пароль данной учетной записи с помощью графического интерфейса невозможно. Для этого выполните скрипт VBS который называется ADSetupWizard.vbs входит в состав установочного пакета Архива. Сценарий необходимо выполнять с правами администратора домена, он автоматически создаст учетную запись компьютера в Active Directory и установить пароль на данную учетную запись. В завершении данный скрипт выведет все параметры конфигурации, которые вы сможете использовать в настройке Архива.

Процедура настройки авторизации Active Directory осуществляется следующим образом:

1. Залогинтесь на сервер контроллера домена
2. Запустите скрипт ADSetupWizard.vbs
3. Следуйте помощнику установки для создания сервисной учетной записи компьютера и установки пароля для этой учетной записи в AD
4. После завершения работы скрипта, скопируйте данные которые он выведет
5. Зайдите в консоль Архива - Настройка - Авторизация
6. Выберите авторизацию Active Directory и введите необходимые значения (пользователь и пароль может быть скопирован из результатов работы скрипта)
7. Нажмите "Назначить новую роль" и создайте связь между ролью в Архива и атрибутом в Active Directory

Если при выполнении скрипта ADSetupWizard.vbs появилась ошибка “AccessDenied 80070005”, необходимо временно выключить

Windows UAC на компьютере где выполняется данный скрипт.

Если возникают проблемы при выполнении скрипта ADSetupWizard.vbs, как альтернативное решение вы можете вручную создать новый компьютер средствами Active Directory Users and Computers. После этого, запустить скрипт SetComputerPassword.vbs для установки пароля на данную учетную запись.

Microsoft требует, чтобы пользователю которому назначены права имперсонализации не имел одновременно назначенных прав администратора.

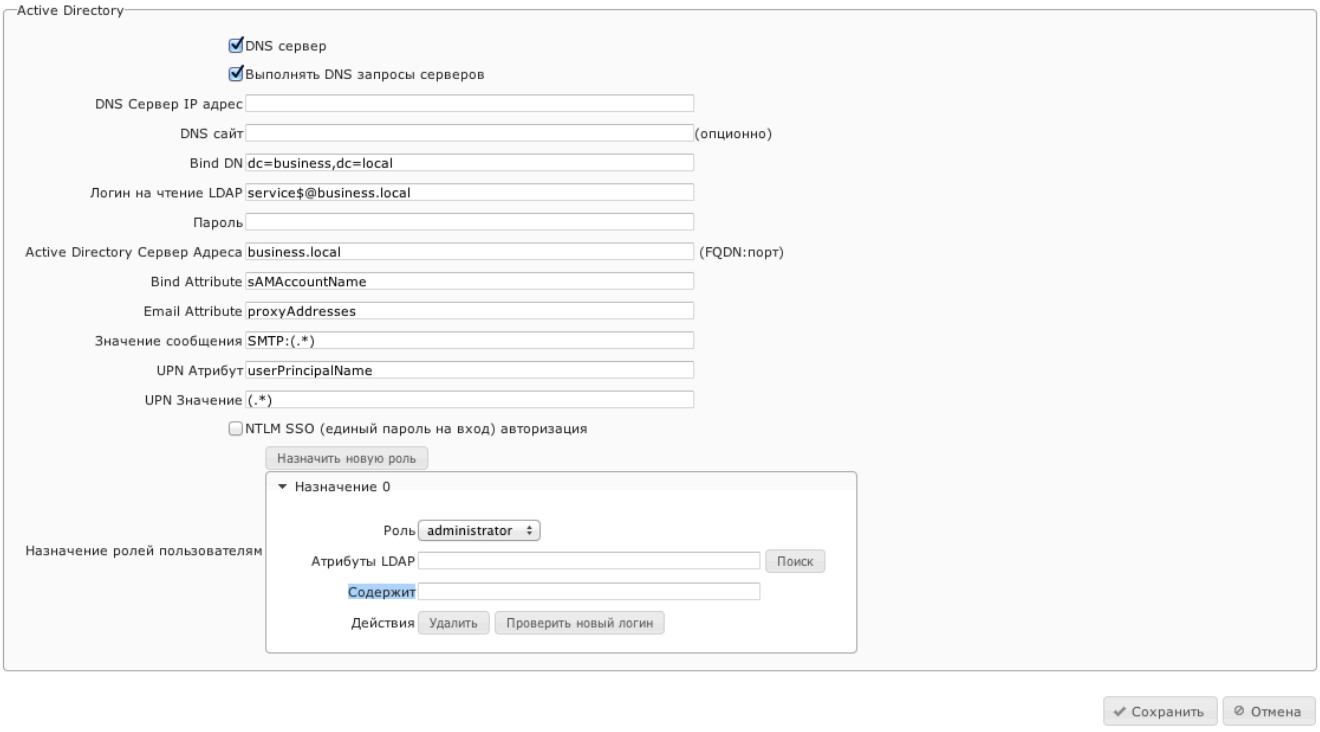
При назначении ролей пользователей Active Directory, необходимо выбрать роль, выбрать атрибут LDAP и задать критерий соответствия.

Поле	Описание
Роль	Роль которую требуется назначить
Атрибуты LDAP	Атрибут LDAP используемый для назначении роли
Содержит	Значение которое сравнивается с атрибутом LDAP в AD для авторизации

Для заполнения "Атрибуты LDAP" и "Содержит" будет полезно узнать как назначаются роли пользователям при авторизации в Архива. Пользователь в Active Directory имеет множество LDAP атрибутов ассоциированных с ним. Эти атрибуты как свойства пользователя (имя пользователя, группа, email и т.д.). Во время авторизации, после того как пользователь был идентифицирован, значение из "Атрибуты LDAP" извлекается из AD, данное значение сравнивается со значением в "Содержит". Если значения совпадают, то назначается роль и пользователь авторизуется в Архива.

Для назначения роли Windows пользователю, выберите “SAMAccountName” как "Атрибуты LDAP" и введите имя пользователя в поле "Содержит". Для назначения роли группе пользователей, выберите “memberOf” в "Атрибуты LDAP" и введите в "Содержит" назначаемое имя группы в Active Directory (например “CN=Enterprise Admins, CN=Users, DC=company, DC=com”).

Поле "Содержит" так-же понимает регулярные выражения для сложных требований к шаблону совпадения.



LDAP атрибут	Содержит
memberOf	группа в Active Directory CN=Enterprise Admins,CN=Users,DC=company,DC=com
userPrincipalName	jdoe@company.com

SAMaccountName	Jdoe
distinguishedName	CN=John Doe,CN=Users,DC=company,DC=com

Во время заполнения поля "Содержит", полезно посмотреть имена LDAP атрибутов и их значения для пользователя. Для этого нажмите "поиск" и в диалоговом окне введите логин и пароль пользователя, атрибуты и значения которого вы хотите посмотреть (например admin@company.com и пароль). Для простого назначения роли конкретному пользователю, просто выберите атрибут и значение из окна поиска, они будут автоматически скопированы в "Атрибут LDAP" и "содержит".

Диалог поиска атрибутов не будет работать если режим Internet Explorer Enhanced Security Configuration включен. Выключите Internet Explorer Enhanced Security Configuration или используйте брайзеры Chrome, Firefox для этих целей. Чтобы отключить Internet Explorer Enhanced Security Configuration Mode: В Windows Server 2003, удалите соответствующий компонент Windows в Add / Remove Programs. В Windows Server 2008, нажмите на корневую папку в Server Manager, перейдите к разделу информационной безопасности и нажмите кнопку "Configure IE ESC". Выключить IE ESC для администраторов.

Если поиск возвращает пустой результат, наверняка есть ошибка в конфигурации. После того, как все роли назначены выполните "тестовый логин" для проверки настроек. Если возникли проблемы, пожалуйста обратитесь к решению проблем авторизации.

Если вы не смогли настроить AD авторизацию в вашем окружении, возможно настроить авторизацию используя авторизацию LDAP основанную на паролях. Для этого выберите LDAP авторизацию, введите "proxyAddresses" в поле "Email Attribute" и "SAMAccountName" в "Bind Attribute". Так-же вам потребуется изменить имя логина. Обратитесь в раздел LDAP авторизация.

Мультидоменная авторизация: Если ваша организация имеет множество доменов, настройте Архива на подключение к глобальному серверу каталогов на порт 3268. Для этого, измените FQDN имя вашего сервера Active Directory эквивалентно company.com:3268. Удалите все значения в поле "Bind DN".

Требования и настройки Windows для единого входа (SSO)

Для обеспечения по-настоящему беспарольной работы, обеспечиваемой встроенным SSO в Windows, необходимо соблюсти следующие требования и настройки (в противном случае пользователю будет представлено диалоговое окно ввода сетевого пароля).:

1. Целевое имя хоста должно быть добавлено в зону безопасности "Локальная интрасеть". Целевое имя хоста - это часть URL-адреса с именем хоста в адресной строке браузера. Это описано далее в следующем разделе.
2. Пользователь должен войти на рабочую станцию, используя свои учетные данные AD DS.

   Примечание
   Конечно, это условие может быть выполнено только в том случае, если операционной системой является Windows. Если пользователь не вошел в домен или если операционная система - Mac или Linux, будет представлено диалоговое окно ввода пароля.
3. Браузер должен поддерживать встроенную в Windows аутентификацию SSO. Большинство браузеров, включая Edge, Chrome и Firefox, работающих под управлением ОС Windows, просто обращаются к Windows SSPI и, следовательно, полностью поддерживают встроенный в Windows SSO.
4. URL-адрес, используемый для посещения сайта, возможно, должен быть полным именем хоста DNS или именем NetBIOS. Специальное имя "localhost" или IP-адрес1 могут работать не так, как ожидалось.

Параметры Интернета и локальная зона интрасети

Чтобы клиенты Windows могли инициировать единый вход, имя хоста или префикс URL-адреса целевого сервера необходимо будет добавить в настройки зоны "Локальная интрасеть" всех клиентов. Найдите и запустите inetcpl.cpl или Internet Settings, чтобы запустить диалоговое окно "Свойства обозревателя". Выберите Безопасность > Локальная интрасеть > Сайты > Дополнительно. Добавьте целевой сайт (или регулярное выражение, соответствующее целевому сайту) в этот список. Вот некоторые примеры значений для этого списка: