ALD Pro

ИНСТРУКЦИИ

# МИГРАЦИЯ РОЛЕЙ

Версия 2.4.1

# Содержание

# Введение

При обновлении ALD Pro до версии 2.4.0 выполняется миграция ролей и привилегий обновляемой Системы.

Все события миграции регистрируются в журналах на контроллере домена по пути /opt/rbta/migration:

- в директории «migrate_user_roco_roles» хранятся журналы миграции ролей ALDPRO - IT Security Specialist, ALDPRO - IT Specialist и пользовательских ролей, созданных до обновления портала управления;
- в директории «migrate_roles_main_and_regional_administrator» хранятся журналы миграции роли ALD PRO - Main Administrator и создания роли ALD Pro - Regional Administrator
- в директории «create_preset_roles» хранятся журналы миграции, создающей пользовательские роли, поставляемые по умолчанию в версии 2.4.0.

Описанные выше директории появляются по пути /opt/rbta/migration только в том случае, если миграция запускалась хотя бы один раз.

# Миграция системных ролей

Все системные роли мигрируются полностью и в том же составе. В результате миграции:

- замена привилегий во время миграции в системных ролях не выполняется;
- в БД сохраняются системные роли, назначенные на пользователей (в интерфейсе портала управления системные роли, назначенные на пользователей, не отображаются и не выполняются).

# Миграция предустановленных ролей

## 3.1. Миграция Enrollment Administrator, helpdesk, Security Architect, User Administrator

Enrollment Administrator, helpdesk, Security Architect, User Administrator до версии 2.4.0 были предустановленными ролями. После обновления на версию 2.4.0:

- эти роли становятся системными (тип «Системная»), и меняется их поведение в портале управления (работать с ними теперь можно, как с системными ролями. См. раздел Системные роли)
- в БД сохраняются существующие до обновления назначения пользователей на роли Enrollment Administrator, helpdesk, Security Architect, User Administrator
- В БД сохраняются все существующие до обновления привязки привилегий и разрешений для данных ролей (см. Руководство Администратора раздел 2.2.6)

## 3.2. Миграция ALDPRO - Main Administrator

В результате миграции на версию 2.4.0 для роли ALD PRO - Main Administrator выполняется:

- тип роли остается «Предустановленная»;
- роль привязывается к корню домена с установленным признаком «Включая дочерние подразделения»;
- для всех привилегий, которые могут быть ограничены сайтом, устанавливается привязка ко всем сайтам;
- роль остается назначенной на всех пользователей и группы пользователей, на которых была назначена до обновления;
- по результатам миграции роль автоматически переводится Системой в состояние «Активна».

**Важно:** Для получения возможности после обновления до версии 2.4.0 делегировать роли средствами портала управления необходимо, чтобы до начала обновления на роль ALD PRO - Main Administrator был назначен хотя бы один пользователь.

## 3.3. Миграция ALDPRO - IT Security Specialist и ALDPRO - IT Specialist

В результате миграции на версию 2.4.0 для ролей ALDPRO - IT Security Specialist и ALDPRO - IT Specialist выполняется:

- тип ролей ALDPRO - IT Security Specialist и ALDPRO - IT Specialist становится «Пользовательская»;
- названия ролей не меняются
- роли привязываются к корню домена с установленным признаком «Включая дочерние подразделения»;
- для всех привилегий, которые могут быть ограничены сайтом, устанавливается привязка ко всем сайтам;
- роли остаются назначенными на всех пользователей и группы пользователей, на которых были назначены до обновления.

В связи с приобретением дополнительных привилегий для мигрированных ролей ALDPRO - IT Security Specialist и ALDPRO - IT Specialist добавляются следующие доступы к подразделам портала управления:

| Раз-дел/Подраздел | ALDPRO - IT Specialist до 2.4.0 | ALDPRO - IT Specialist в 2.4.0 после миграции | Привилегии в 2.4.0, которые предоставляют доступ к подразделам |
|---|---|---|---|
| Управление доменом/Доп. Параметры групповых политик | - | + | Поскольку роли ALDPRO - IT Specialist было доступно чтение групповых политик назначенных на подразделения, пользователей и компьютеры, в 2.4.0 требуются новые привилегии: • Computer Group Policy Additional Parameters - Read • User Group Policy Additional Parameters - Read |
| Управление доменом/ Пользователи и группы | - | + | • Users and Groups Settings - Read |
| Групповые политики/Групповые политики | - | + | Поскольку роли ALDPRO - IT Specialist было доступно чтение групповых политик назначенных на подразделения, пользователей и компьютеры, в 2.4.0 требуется новая привилегия: • Group Policies - Read |

| Раздел/ Подраздел | ALDPRO - IT Security Specialist до 2.4.0 | ALDPRO - IT Security Specialist в 2.4.0 после миграции | Привилегии в 2.4.0, которые предоставляют доступ к подразделам |
|---|---|---|---|
| Установка и обновление ПО/ Политики ПО | - | + | Поскольку ранее администратору ALDPRO - IT Security Specialist было доступно изменение конфигураций политик программного обеспечения, то в текущей парадигме прав доступа требуются следующие привилегии для управления политиками ПО: • Software Policies - Read • Software Policies - Modify • Software Policies Configurations - Manage • Software Policies Membership - Manage |
| Установка и обновление ПО/ Каталог ПО | - | + | Для корректной работы политик ПО, ALDPRO - IT Security Specialist необходимо чтение каталога ПО: • Software Catalog - Read |
| Роли и службы сайта/ Служба разрешения имен | - | + | Для корректной работы с подсистемами, ALDPRO - IT Security Specialist необходим доступ к чтению DNS: • DNS Zones - Read • DNS Forward Zones - Read |

### 3.3.1. Предоставляемые права для ALDPRO - IT Specialist

Права, предоставляемые роли «ALDPRO - IT Specialist» по умолчанию после миграции со старших версий. Доступы могут измениться после внесения изменений в состав привилегий.

| Раздел/ Подраздел | Предоставляемые права |
|---|---|
| **Автоматизация**/ Установка ОС по сети | 1.**Installation Server Computers - Manage** - Позволяет осуществлять полное управление компьютерами в рамках серверов установки 2. **Installation Server Profiles - Manage** - Дает возможность управлять профилями загрузки 3. **Installation Servers - Create** - Позволяет создавать серверы установки в системе 4. **Installation Servers - Drop** - Дает возможность удалять существующие серверы установки 5. **Installation Servers - Modify** - Позволяет изменять настройки и конфигурации существующих серверов установки 6. **Installation Servers - Read** - Предоставляет доступ для чтения к информации о серверах установки |
| **Автоматизация**/ Задания автоматизации | 1.**Automation Tasks Journal - Read** - Предоставляет возможность просматривать журнал заданий автоматизации 2. **Automation Tasks Membership - Manage** - Дает право управлять участниками заданий автоматизации |
| **Управление доменом**/ Пользователи и группы | **Users and Groups Settings - Read** - Предоставляет доступ для чтения к настройкам пользователей и групп |
| **Управление доменом**/ Доп. параметры групповых политик | 1.**User Group Policy Additional Parameters - Read** - Предоставляет возможность только для чтения для просмотра дополнительных параметров групповых политик для пользователей 2. **Computer Group Policy Additional Parameters - Read** - Предоставляет доступ для чтения к дополнительным параметрам групповых политик, применяемых к компьютерам |
| **Управление доменом**/ Сайты и службы | 1.**Replication Agreements - Add** - Позволяет добавлять новые соглашения о репликации 2. **Replication Agreements - Delete** - Дает возможность удалять существующие соглашения о репликации 3. **Replication Agreements - Modify** - Позволяет изменять параметры существующих соглашений о репликации 4. **Replication Agreements - Read** - Предоставляет доступ только для чтения к соглашениям о репликации 5. **Domain Controllers - Create** - Позволяет создавать новые контроллеры домена в системе. 6. **Domain Controllers - Drop** - Дает возможность удалять существующие контроллеры домена 7. **Domain Controllers - Modify** - Позволяет изменять параметры и настройки существующих контроллеров домена. 8. **Domain Controllers - Read** - Предоставляет доступ для чтения к информации о контроллерах домена9. **Site Parameters - Add** - Позволяет добавлять новые параметры конфигурации сайтов 10. **Site Parameters - Delete** - Дает возможность удалять существующие параметры сайтов 11. **Site Parameters - Modify** - Позволяет изменять существующие параметры сайта 12. **Site Parameters - Read** - Предоставляет доступ только для чтения к параметрам сайтов 13. **Site Domain Controllers - Add** - Позволяет назначить контроллер домена на сайт14. **Sites - Read** - Позволяет просматривать информацию о сайтах в системе |
| **Управление доменом**/ Общая информация | **Domain Info - Read** - Предоставляет возможность просматривать информацию о домене |
| **Управление доменом**/ Каталог заданий автоматизации | 1.**Automation Task Attributes - Manage** - Позволяет управлять атрибутами заданий автоматизации 2. **Automation Task Script - Manage** - Дает возможность управлять скриптами заданий автоматизации 3. **Automation Tasks - Manage** - Предоставляет полный контроль заданий автоматизации 4. **Automation Tasks - Read** - Предоставляет доступ для чтения к заданиям автоматизации 5. **Automation Tasks Folders - Manage** - Позволяет управлять папками в рамках заданий автоматизации |
| **Пользователи и компьютеры**/ Организационная структура | **Organization units - Read** - Предоставляет доступ для чтения к организационным единицам |

continues on next page

Таблица 3.1 – продолжение с предыдущей страницы

| Раздел/ Подраздел | Предоставляемые права |
|---|---|
| **Пользователи и компьютеры/** Группы компьютеров | 1.**Computer groups - Add** - Позволяет создавать новые группы компьютеров в системе. 2. **Computer groups - Delete** - Дает возможность удалять существующие группы компьютеров 3. **Computer groups - Modify** - Позволяет изменять параметры и состав существующих групп компьютеров 4. **Computer groups - Read** - Предоставляет доступ только для чтения к информации о группах компьютеров 5. **Computer groups - Set group membership** - Позволяет управлять членством компьютеров в определенных группах 6. **Computer groups - Set organization unit** - Позволяет назначать или изменять подразделение (OU) для групп компьютеров |
| **Пользователи и компьютеры/** Группы пользователей | **User groups - Read** - Предоставляет доступ для чтения к пользовательским группам |
| **Пользователи и компьютеры/** Пользователи | **Users - Read** - Предоставляет доступ только для чтения к пользовательским учетным записям |
| **Пользователи и компьютеры/** Компьютеры | 1.**Computers - Delete** - Позволяет удалять учетные записи компьютеров из системы 2. **Computers - Modify** - Дает возможность изменять свойства и настройки существующих учетных записей компьютеров 3. **Computers - Read** - Предоставляет доступ для чтения к информации о компьютерах в системе 4. **Computers - Remote access** - Позволяет осуществлять удаленный доступ к компьютерам 5. **Computers - Set organization unit** - Позволяет назначать или изменять подразделения (OU) для учетных записей компьютеров |
| **Групповые политики/** Групповые политики | **Group Policies - Read** - Предоставляет доступ только для чтения к существующим групповым политикам |
| **Роли и службы сайта/** Служба печати | 1.**Print Servers - Create** - Позволяет создавать новые серверы печати в системе 2. **Print Servers - Drop** - Дает возможность удалять существующие серверы печати из системы 3. **Print Servers - Modify** - Позволяет изменять настройки и конфигурации существующих серверов печати 4. **Print Servers - Read** - Предоставляет доступ для чтения к информации о серверах печати 5. **Printers - Manage** - Позволяет управлять принтерами, подключенными к серверам печати, включая добавление, удаление и изменение настроек |
| **Роли и службы сайта/** Служба динамической настройки узла | 1.**DHCP - Read** - Предоставляет доступ для чтения к DHCP 2. **DHCP Configuration - Modify** - Позволяет изменять конфигурации DHCP-сервера 3. **DHCP Servers - Create** - Дает возможность создавать новые DHCP-серверы 4. **DHCP Servers - Drop** - Позволяет удалять существующие DHCP-серверы 5. **DHCP Servers - Modify** - Позволяет вносить изменения в существующие DHCP-серверы |
| **Роли и службы сайта/** Служба разрешения имён | 1.**DNS Forward Zones - Add** - Позволяет добавлять новые перенаправления запросов**DNS** 2. **DNS Forward Zones - Delete** - Дает возможность удалять существующие перенаправления запросов **DNS** 3. **DNS Forward Zones - Delete** - Позволяет изменять конфигурацию существующих перенаправлений запросов **DNS** 4. **DNS Forward Zones - Read** - Предоставляет доступ для чтения к информации о перенаправлении запросов **DNS** 5. **DNS Global Configurations - Manage** - Позволяет управлять глобальными конфигурациями **DNS** 6. **DNS Zones - Manage** - Дает возможность управлять DNS-зонами, включая создание, изменение и удаление зон 7. **DNS Zones - Read** - Предоставляет доступ только для чтения к информации о DNS-зонах |
| **Роли и службы сайта/** Служба синхронизации времени | 1.**Root NTP Servers - Create** - Позволяет создавать новые корневые NTP-серверы 2. **Root NTP Servers - Drop** - Дает возможность удалять существующие корневые NTP-серверы из конфигурации системы 3. **NTP Servers - Read** - Предоставляет доступ для чтения к информации о NTP-серверах 4. **External NTP Servers - Create** - Позволяет добавлять новые внешние NTP-серверы 5. **External NTP Servers - Drop** - Дает возможность удалять внешние NTP-серверы из конфигурации системы |

continues on next page

Таблица 3.1 – продолжение с предыдущей страницы

| Раздел/ Подраздел | Предоставляемые права |
|---|---|
| **Установка и обновление ПО**/ Каталог ПО | 1.**Software Templates - Manage** - Позволяет управлять шаблонами программного обеспечения в системе 2. **Software - Manage** - Дает возможность управлять всем программным обеспечением в системе 3. **Software Catalog - Read** - Предоставляет доступ только для чтения к каталогу программного обеспечения 4. **Software Groups - Manage** - Позволяет управлять группами программного обеспечения 5. **Software Packages - Manage** - Дает возможность управлять программными пакетами в системе 6. **Software Parameters - Manage** - Позволяет управлять параметрами, связанными с программным обеспечением |
| **Установка и обновление ПО**/ Политики ПО | 1.**Software Policies - Add** - Позволяет добавлять новые политики программного обеспечения в системе 2. **Software Policies - Delete** - Дает возможность удалять существующие политики программного обеспечения 3. **Software Policies - Modify** - Позволяет изменять существующие политики программного обеспечения 4. **Software Policies - Read** - Обеспечивает доступ только для чтения к текущим политиками программного обеспечения 5. **Software Policies Configurations - Manage** - Позволяет управлять конфигурациями, связанными с политиками программного обеспечения 6. **Software Policies Membership - Manage** - Позволяет управлять членством в политиках программного обеспечения |
| **Установка и обновление ПО**/ Репозитории ПО | 1.**Repositories - Add** - Позволяет создавать новые репозитории в системе 2. **Repositories - Delete** - Дает возможность удалять существующие репозитории из системы 3. **Repositories - Modify** - Позволяет изменять параметры и содержимое существующих репозиториев 4. **Repositories - Read** - Предоставляет доступ для чтения к информации о репозиториях 5. **Repository Servers - Create** - Позволяет создавать новые сервера-репозитории в системе 6. **Repository Servers - Drop** - Дает возможность удалять существующие сервера-репозитории 7. **Repository Servers - Modify** - Позволяет изменять конфигурацию и параметры существующих серверов-репозиториев 8. **Repository Servers - Read** - Предоставляет доступ только для чтения к серверам-репозиториям 9. **Repository Versions - Manage** - Позволяет управлять версиями программных пакетов и репозиториев |
| **Установка и обновление ПО**/ Политики обновления ALD Pro | 1.**Update Policies - Add** - Позволяет добавлять новые политики обновления в системе 2. **Update Policies - Delete** - Дает возможность удалять существующие политики обновления 3. **Update Policies - Modify** - Позволяет изменять параметры существующих политик обновления 4. **Update Policies - Read** - Предоставляет доступ только для чтения к существующим политикам обновления 5. **Update Policies Computers - Manage** - Позволяет управлять применением политик обновления к конкретным компьютерам или группам компьютеров 6. **Update Policies Sources list - Manage** - Дает возможность управлять списком источников обновлений |
| **Доступ только через БД и API** | **IPA Servers - Read** - Предоставляет доступ для чтения к информации об IPA серверах |

### 3.3.2. Предоставляемые права для ALDPRO - IT Security Specialist

Права, предоставляемые роли «ALDPRO - IT Security Specialist» по умолчанию после миграции со старших версий. Доступы могут измениться после внесения изменений в состав привилегий.

| Раздел/ Подраздел | Предоставляемые права |
|---|---|
| **Автоматизация**/ Задания автоматизации | 1.**Automation Tasks Journal - Read** - Предоставляет возможность просматривать журнал заданий автоматизации 2. **Automation Tasks Membership - Manage** - Дает право управлять участниками заданий автоматизации |
| **Управление доменом**/ Сайты и службы | 1.**Site Parameters - Read** - Предоставляет возможность просматривать параметры конфигурации сайтов 2.**Sites - Read** - Даёт доступ для чтения к информации о сайтах в домене 3.**Domain Controllers - Read** - Позволяет просматривать информацию о контроллерах домена 4.**Replication Agreements - Read** - Обеспечивает доступ для чтения к соглашениям о репликации |
| **Управление доменом**/ Пользователи и группы | 1.**Users and Groups Settings - Manage** - Позволяет управлять настройками пользователей и групп в системе 2. **Users and Groups Settings - Read** - Предоставляет доступ для чтения к настройкам пользователей и групп |
| **Управление доменом**/ Роли и права доступа | 1.**Role Privileges - Add** - Позволяет добавлять новые привилегии к существующим ролям 2. **Role Privileges - Delete** - Дает возможность удалять привилегии из ролей 3. **Role Privileges - Modify** - Позволяет изменять существующие привилегии в ролях ролями 4. **Roles - Add** - Позволяет создавать новые роли в систем 5. **Roles - Delete** - Позволяет удалять существующие роли 6. **Roles - Modify** - Дает возможность изменять параметры существующих ролей 7. **Roles - Read** - Предоставляет доступ для чтения к существующим ролям 8. **Roles Membership - Manage** - Позволяет управлять членством в ролях, включая добавление или удаление пользователей или групп из определенных ролей |
| **Управление доменом**/ Общая информация | **Domain Info - Read** - Предоставляет возможность просматривать информацию о домене |
| **Управление доменом**/ Доп. параметры групповых политик | 1.**Computer Group Policy Additional Parameters - Manage** - Позволяет управлять дополнительными параметрами групповых политик для компьютеров 2. **Computer Group Policy Additional Parameters - Read** - Предоставляет возможность просматривать дополнительные параметры групповых политик для компьютеров 3. **User Group Policy Additional Parameters - Manage** - Позволяет управлять дополнительными параметрами групповых политик для пользователей 4. **User Group Policy Additional Parameters - Read** - Предоставляет возможность только для чтения дополнительных параметров групповых политик для пользователей |
| **Управление доменом**/ Службы и параметры Kerberos | 1.**Kerberos Configurations - Manage** - Позволяет управлять конфигурациями Kerberos в системе 2. **Kerberos Services - Add** - Дает возможность добавлять новые Kerberos службы в систему 3. **Kerberos Services - Delete** - Позволяет удалять существующие Kerberos службы 4. **Kerberos Services - Modify** - Предоставляет возможность изменять параметры существующих Kerberos служб 5. **Kerberos Services - Read** - Предоставляет доступ только для чтения к информации о Kerberos службах |
| **Управление доменом**/ Каталог заданий автоматизации | 1.**Automation Task Attributes - Manage** - Позволяет управлять атрибутами заданий автоматизации 2. **Automation Task Script - Manage** - Дает возможность управлять скриптами, связанными с заданиями автоматизации 3. **Automation Tasks - Manage** - Позволяет управлять заданиями автоматизации, включая их создание, изменение 4. **Automation Tasks - Read** - Предоставляет возможность только просматривать задания автоматизации 5. **Automation Tasks Folders - Manage** - Позволяет управлять папками, содержащими задания автоматизации |
| **Журнал событий**/ Серверы журнала событий | 1.**Event Log Servers - Create** - Позволяет создавать новые серверы журналов событий в системе 2. **Event Log Servers - Drop** - Дает возможность удалять существующие серверы журналов событий из системы 3. **Event Log Servers - Modify** - Позволяет изменять конфигурации и настройки существующих серверов журналов событий 4. **Event Log Servers - Read** - Предоставляет доступ для чтения к информации о серверах журналов событий |

continues on next page

Таблица 3.2 – продолжение с предыдущей страницы

| Раздел/ Подраздел | Предоставляемые права |
|---|---|
| **Журнал событий**/ Настройка сбора журналов событий | 1.**Event Registration Rules - Add** - Позволяет добавлять новые правила регистрации событий в системе 2. **Event Registration Rules - Delete** - Дает возможность удалять существующие правила регистрации событий. 3. **Event Registration Rules - Modify** - Позволяет изменять параметры и условия существующих правил регистрации событий 4. **Event Registration Rules - Read** - Предоставляет доступ только для чтения к правилам регистрации событий |
| **Роли и службы сайта**/ Общий доступ к файлам | 1.**File Server Folders - Manage** - Предоставляет возможность управлять папками на файловых серверах. 2. **File Servers - Create** - Позволяет создавать новые файловые серверы в системе 3. **File Servers - Drop** - Дает возможность удалять существующие файловые серверы из системы 4. **File Servers - Modify** - Позволяет изменять конфигурации и параметры существующих файловых серверов 5. **File Servers - Read** - Предоставляет доступ только для чтения к информации о файловых серверах |
| **Роли и службы сайта**/ Служба разрешения имён | 1.**DNS Forward Zones - Read** - Предоставляет доступ для чтения к информации о перенаправлении запросов **DNS** 2. **DNS Zones - Read** - Предоставляет доступ только для чтения к информации о DNS-зонах |
| **Групповые политики**/ Политики паролей | 1.**Password Policies - Add** - Позволяет добавлять новые политики паролей в систему 2. **Password Policies - Delete** - Дает возможность удалять существующие политики паролей 3. **Password Policies - Modify** - Позволяет изменять настройки существующих политик паролей 4. **Password Policies - Read** - Предоставляет доступ только для чтения к существующим политикам паролей |
| **Групповые политики**/ Политики повышения привилегий | 1.**SUDO - Read** - Предоставляет возможность просматривать текущие настройки и конфигурации SUDO 2. **SUDO Command Groups - Add** - Позволяет добавлять новые группы команд SUDO 3. **SUDO Command Groups - Delete** - Дает возможность удалять существующие группы команд SUDO 4. **SUDO Command Groups - Modify** - Позволяет изменять состав или параметры существующих групп команд SUDO 5. **SUDO Commands - Add** - Предоставляет возможность добавлять отдельные SUDO команды в группы или правила 6. **SUDO Commands - Delete** - Позволяет удалять отдельные SUDO команды из их групп или правил 7. **SUDO Commands - Modify** - Дает возможность изменять параметры существующих SUDO команд 8. **SUDO Parameters - Manage** - Позволяет управлять параметрами конфигурации SUDO 9. **SUDO Rules - Add** - Позволяет добавлять новые правила SUDO 10. **SUDO Rules - Delete** - Позволяет удалять существующие правила SUDO 11. **SUDO Rules - Modify** - Дает возможность изменять существующие правила SUDO |
| **Групповые политики**/ Групповые политики | 1.**Group Policies - Add** - Позволяет добавлять новые групповые политики в системе 2. **Group Policies - Delete** - Дает возможность удалять существующие групповые политики 3. **Group Policies - Modify** - Позволяет изменять настройки существующих групповых политик 4. **Group Policies - Read** - Предоставляет доступ только для чтения к существующим групповым политикам 5. **Group Policies Computer Parameters - Manage** - Позволяет управлять параметрами компьютеров в рамках групповых политик 6. **Group Policies User Parameters - Manage** - Предоставляет возможность управлять пользовательскими параметрами в рамках групповых политик 7. **Group Policies Membership - Manage** - Позволяет управлять членством в групповых политиках |

continues on next page

Таблица 3.2 – продолжение с предыдущей страницы

| Раздел/ Подраздел | Предоставляемые права |
|---|---|
| **Групповые политики**/ Политики доступа к узлу | 1.**HBAC - Read** - Предоставляет возможность просматривать настройки и правила контроля доступа на основе хоста (HBAC) 2. **HBAC Rules - Add** - Позволяет добавлять новые правила HBAC 3. **HBAC Rules - Delete** - Дает возможность удалять существующие правила HBAC 4. **HBAC Rules - Modify** - Позволяет изменять существующие правила HBAC 5. **HBAC Service Groups - Add** - Позволяет создавать новые группы служб в рамках HBAC 6. **HBAC Service Groups - Delete** - Дает возможность удалять существующие группы служб в рамках HBAC 7. **HBAC Service Groups - Modify** - Позволяет изменять состав или параметры существующих групп служб 8. **HBAC Services - Add** - Предоставляет возможность добавлять новые службы для контроля доступа в HBAC 9. **HBAC Services - Delete** - Позволяет удалять существующие службы из списка контролируемых доступа 10. **HBAC Services - Modify** - Дает возможность изменять параметры существующих служб |
| **Мониторинг**/ Витрины мониторинга домена | **Dashboards - Read** - Предоставляет доступ для чтения к дашбордам системы |
| **Мониторинг**/ Журнал событий мониторинга | 1.**Monitoring Event Logs - Read** - Предоставляет доступ только для чтения к журналам событий мониторинга 2. **Monitoring Servers - Create** - Позволяет создавать новые сервера для мониторинга в системе. 3. **Monitoring Servers - Drop** - Дает возможность удалять существующие сервера мониторинга из системы 4. **Monitoring Servers - Modify** - Позволяет изменять конфигурации и настройки существующих серверов мониторинга 5. **Monitoring Servers - Read** - Предоставляет доступ только для чтения к информации о серверах мониторинга |
| **Установка и обновление ПО**/ Каталог ПО | **Software Catalog - Read** - Предоставляет доступ для чтения к каталогу программного обеспечения |
| **Установка и обновление ПО**/ Политики ПО | 1.**Software Policies - Modify** - Позволяет изменять существующие политики программного обеспечения 2. **Software Policies - Read** - Предоставляет доступ для чтения к текущим политикам программного обеспечения 3. **Software Policies Configurations - Manage** - Позволяет управлять конфигурациями, связанными с политиками программного обеспечения |
| **Модуль синхронизации**/ Настройки | 1.**MS AD andALD Pro Controllers - Create** - Позволяет создавать новые контроллеры Microsoft Active Directory (AD) и ALD Pro 2. **MS AD and ALD Pro Controllers - Drop** - Дает возможность удалять существующие контроллеры Microsoft AD и ALD Pro из системы 3. **MS AD and ALD Pro Controllers - Modify** - Позволяет изменять настройки и конфигурации существующих контроллеров Microsoft AD и ALD Pro 4. **MS AD and ALD Pro Controllers - Read** - Предоставляет доступ для чтения к информации о контроллерах Microsoft AD и ALD Pro |
| **Модуль синхронизации**/ Сопоставление атрибутов | 1.**Attributes Mapping - Manage** - Позволяет управлять отображением атрибутов в системе 2. **Attributes Mapping - Read** - Предоставляет доступ только для чтения к отображению атрибутов |
| **Модуль синхронизации**/ Источники | 1.**Organizational Units Mapping - Manage** - Позволяет управлять сопоставлением подразделений (OU) 2. **Organizational Units Mapping - Read** - Предоставляет доступ для чтения к сопоставлению подразделений 3. **Synchronization Tree - Manage** - Позволяет управлять деревом синхронизации в системе 4. **Synchronization Tree - Read** - Предоставляет доступ для чтения к дереву синхронизации |

continues on next page

Таблица 3.2 – продолжение с предыдущей страницы

| Раздел/ Подраздел | Предоставляемые права |
|---|---|
| **Пользователи и компьютеры/** Группы компьютеров | 1.**Computer groups - Add** - Позволяет создавать новые группы компьютеров в системе 2. **Computer groups - Delete** - Дает возможность удалять существующие группы компьютеров 3. **Computer groups - Modify** - Позволяет изменять настройки и состав существующих групп компьютеров 4. **Computer groups - Read** - Предоставляет доступ только для чтения к информации о группах компьютеров 5. **Computer groups - Set group membership** - Позволяет управлять членством компьютеров в определенных группах 6. **Computer groups - Set organization unit** - Позволяет назначать или изменять подразделение (OU) |
| **Пользователи и компьютеры/** Компьютеры | 1.**Computers - Delete** - Позволяет удалять учетные записи компьютеров из системы 2. **Computers - Modify** - Дает возможность изменять свойства и настройки существующих учетных записей компьютеров 3. **Computers - Read** - Предоставляет доступ для чтения к информации о компьютерах в системе 4. **Computers - Remote access** - Позволяет осуществлять удаленный доступ к компьютерам 5. **Computers - Set organization unit** - Позволяет назначать или изменять подразделения (OU) для учетных записей компьютеров |
| **Пользователи и компьютеры/** Организационная структура | 1.**Organization Units - Add** - Позволяет создавать новые подразделения (OU) в системе 2. **Organization units - Delete** - Дает возможность удалять существующие подразделения 3. **Organization units - Modify** - Позволяет изменять параметры существующих подразделения 4. **Organization units - Read** - Предоставляет доступ для чтения к организационным единицам |
| **Пользователи и компьютеры/** Группы пользователей | 1.**User groups - Add** - Позволяет создавать новые пользовательские группы в системе 2. **User groups - Delete** - Дает возможность удалять существующие пользовательские группы 3. **User groups - Modify** - Позволяет изменять параметры существующих пользовательских групп 4. **User groups - Read** - Предоставляет доступ для чтения к пользовательским группам 5. **User groups - Set group membership** - Позволяет управлять членством пользователей в группах 6. **User groups - Set organization unit** - Позволяет назначать или изменять подразделение (OU) для пользовательских групп |
| **Пользователи и компьютеры/** Пользователи | 1.**Users - Add** - Позволяет добавлять новые пользовательские учетные записи в систему 2. **Users - Modify** - Позволяет изменять существующие пользовательские учетные записи 3. **Users - Read** - Предоставляет доступ только для чтения к пользовательским учетным записям 4. **Users - Set organization unit** - Позволяет назначать или изменять подразделение (OU) для учетных записей 5. **Users Password - Modify** - Дает возможность изменять пароли для учетных записей |
| **Пользователи и компьютеры/** Корзина | 1.**Users - Read trash** - Позволяет просматривать учетные записи, которые были перемещены в корзину 2. **Users - Delete from trash** - Дает возможность окончательно удалять пользовательские учетные записи из корзины 3. **Users - Return from trash** - Дает возможность восстанавливать из корзины пользовательские учетные записи, которые были ранее перемещены туда 4. **Users - Move to trash** - Дает возможность перемещать пользовательские учетные записи в корзину |
| **Доступ только через БД и API** | **IPA Servers - Read** - Предоставляет доступ для чтения к информации об IPA серверах |

# Миграция пользовательских ролей

## 4.1. Миграция пользовательских ролей, поставляемых по умолчанию в версии 2.4.0

После обновления до версии 2.4.0 появляются новые пользовательские роли, установленные в Системе по умолчанию:

- роли на операции в каждом подразделе портала управления;
- роль на чтение всего портала управления;
- роль регионального администратора.

Для этих ролей выполняются следующие условия:

- тип ролей «Пользовательская»;
- роли привязываются к корню домена с установленным признаком «Включая дочерние подразделения»;
- для всех привилегий, которые могут быть ограничены сайтом, устанавливается привязка ко всем сайтам;
- на эти роли не делегированы пользователи и группы пользователей.

## 4.2. Миграция пользовательских ролей, созданных до обновления портала управления

В версию 2.4.0 переносятся все роли, созданные пользователями до обновления.

С версии 2.4.0 привязка к подразделению указывается для роли. Привилегии в составе роли, которым требуется привязка к подразделению, наследуют эту настройку от роли.

Привилегии одной роли, привязанные к разным подразделениям, в результате миграции будут распределены по нескольким ролям с учетом общей привязки к подразделению и признака «Включая дочерние подразделения».

Правила миграции пользовательских ролей:

- тип ролей сохраняется: «Пользовательская»;
- создается набор ролей по количеству привязок привилегий с учетом признака «Включая дочерние подразделения» в мигрируемой роли:
  - если в результате миграции из одной роли создается несколько ролей, для новых ролей в наборе к старому названию добавляется порядковый номер;
  - если в результате миграции из одной роли создается несколько ролей, каждая новая роль в наборе содержит все привилегии старой роли, которые не могут быть ограничены подразделением;
- если мигрируемая роль была в статусе «Активна», то все соответствующие ей новые роли будут активированы:
  - будет выполнена попытка делегировать все новые роли всем пользователям и группам пользователей, на которых была назначена старая роль:
    - если некоторые пользователи выпадут из области действия привязки новой роли (т.е. подразделение новой роли и подразделение пользователя или хотя бы одного из пользователей в группе не совпадают с учетом признака «Включая дочерние подразделения» у новой роли), такой пользователь или группа не получат новую роль, в журнал миграции будет внесена запись об ошибке делегирования;
- если статус мигрируемой роли отличен от «Активна», то статус наследуется, и все пользователи и все группы переносятся во все новые роли:
  - при процедуре активации всех новых ролей будет происходить проверка возможности наличия перенесенных пользователей в каждой роли (с привязкой к конкретному подразделению);
  - привязку роли к подразделению можно сменить таким образом, чтобы подразделения всех пользователей, назначенных на роль, подпадали в область действия роли (обязательное условие успеха активации роли).