2.10-3.0

Подготовка

Изменения в требованиях

Wizard Linux-сервер

Для запуска Wizard требуется Linux-сервер, имеющий сетевую связность со всеми Linux-серверами по **SSH** и Windows-серверами по **WinRM** или **WinRM по HTTPS**. В качестве такого сервера можно использовать один из Linux-серверов с компонентами PAM.

Windows-серверы

- Отключите поддержку **IPv6** в сетевых адаптерах.
- Настройте **WinRM(5985)** или **WinRM по HTTPS(5986)** и разрешите подключения с Wizard Linux-сервера.
- Подготовьте доменную учётную запись, входящую в группу локальных администраторов, для установки через Wizard.

Сервера Indeed PAM

1. Выполните расшифровку конфигурационных файлов **Core**, **IdP**, **Gateway Service** и **LogServer** с использованием специальной утилиты (см. Приложение 1).

2. Создайте резервные копии файлов:

    - **На Windows-серверах управления:**
        - Core: `C:\inetpub\wwwroot\pam\core\appsettings.json`
        - IdP: `C:\inetpub\wwwroot\pam\idp\appsettings.json`
        - MC: `C:\inetpub\wwwroot\pam\mc\assets\config\config.prod.json`
        - UC: `C:\inetpub\wwwroot\pam\uc\assets\config\config.prod.json`
        - LogServer:
            - `C:\inetpub\wwwroot\ls\clientApps.config`

        - `C:\inetpub\wwwroot\ls\targetConfigs\*`
    - Выполните экспорт сертификатов PAM из хранилища сертификатов локальной машины в формате **.pfx**.
- **На Windows-серверах доступа:**
    - Фильтрация процессов:
      `C:\Program Files\Indeed\Indeed PAM\Gateway\ProcessCreateHook\processprotection.settings.json`
    - Защита уязвимых файлов:
      `C:\Program Files\Indeed\Indeed PAM\Gateway\Service\filesprotection.settings.json`
    - Gateway Service:
      `C:\Program Files\Indeed\Indeed PAM\Gateway\Pam.Gateway.Service\appsettings.json`
    - ProxyApp:
      `C:\Program Files\Indeed\Indeed PAM\Gateway\ProxyApp\appsettings.json`
    - Выполните экспорт сертификатов PAM из хранилища сертификатов локальной машины в формате **.pfx**.
- PowerShell команда для быстрого бэкапирования конфигурационных файлов PAM с сервера. Создаёт папку с именем сервера в месте запуска и копирует конфигурационные файлы в неё:

PowerShell

```
$serverName = $env:COMPUTERNAME
$basePath = Join-Path (Get-Location) $serverName
$folders = @("Core", "Idp", "MC", "UC", "LogServer\targetConfigs", "ProcessProtection",
"FileProtection", "GatewayService", "ProxyApp")
$filesToCopy = @{
"C:\inetpub\wwwroot\pam\core\appsettings.json" = "Core"
"C:\inetpub\wwwroot\pam\idp\appsettings.json" = "Idp"
"C:\inetpub\wwwroot\pam\mc\assets\config\config.prod.json" = "MC"
"C:\inetpub\wwwroot\pam\uc\assets\config\config.prod.json" = "UC"
"C:\inetpub\wwwroot\ls\clientApps.config" = "LogServer"
"C:\Program Files\Indeed\Indeed PAM\Gateway\ProcessCreateHook\processprotection.settings.
json" = "ProcessProtection"
"C:\Program Files\Indeed\Indeed PAM\Gateway\Service\filesprotection.settings.json" =
"FileProtection"
"C:\Program Files\Indeed\Indeed PAM\Gateway\Pam.Gateway.Service\appsettings.json" =
"GatewayService"
"C:\Program Files\Indeed\Indeed PAM\Gateway\ProxyApp\appsettings.json" = "ProxyApp"
}
$folders | ForEach-Object { New-Item -ItemType Directory -Path (Join-Path $basePath $_) -
Force | Out-Null }
$filesToCopy.GetEnumerator() | ForEach-Object {
if (Test-Path $_.Key) { Copy-Item $_.Key -Destination (Join-Path $basePath $_.Value) -
```

```
Force }
elseif ($_.Value -ne "LogServer" -and (Get-ChildItem -Path (Join-Path $basePath $_.
Value)).Count -eq 0) {
Remove-Item (Join-Path $basePath $_.Value) -Force
}
}
$sourceTargetConfigsPath = "C:\inetpub\wwwroot\ls\targetConfigs\*"
if (Test-Path $sourceTargetConfigsPath) { Copy-Item $sourceTargetConfigsPath -
Destination (Join-Path $basePath "LogServer\targetConfigs") -Recurse -Force }
```

- **На Linux-серверах управления:**
  - Core: `/etc/indeed/indeed-pam/core/appsettings.json`
  - IdP: `/etc/indeed/indeed-pam/idp/appsettings.json`
  - MC: `/etc/indeed/indeed-pam/mc/config.prod.json`
  - UC: `/etc/indeed/indeed-pam/uc/config.prod.json`
  - Nginx: `/etc/indeed/indeed-pam/nginx/*`
  - LogServer:
    - `/etc/indeed/indeed-pam/ls/clientApps.config`
    - `/etc/indeed/indeed-pam/ls/targets/*`
  - Сертификаты и ключи:
    - `/etc/indeed/indeed-pam/ca-certificates/*`
    - `/etc/indeed/indeed-pam/certs/*`
    - `/etc/indeed/indeed-pam/keys/*`
    - Выполните объединение **.crt** и **.key** в `/certs/` с указанием корневого **ca** из `/ca-certificates/` в **.pfx** с помощью команды: `openssl pkcs12 -export -out server-fqdn.pfx -inkey pam.key -in pam.crt -certfile ca.crt`
  - YML-файлы: `/etc/indeed/indeed-pam/*.yml`
- **На Linux-серверах доступа:**
  - RDP-Proxy: `/etc/indeed/indeed-pam/rdp-proxy/appsettings.json`
  - SSH-Proxy: `/etc/indeed/indeed-pam/ssh-proxy/appsettings.json`
  - Gateway Service: `/etc/indeed/indeed-pam/gateway-service/appsettings.json`
  - `.env`: `/etc/indeed/indeed-pam/.env`
  - Сертификаты и ключи:
    - `/etc/indeed/indeed-pam/ca-certificates/*`
    - `/etc/indeed/indeed-pam/certs/*`
    - `/etc/indeed/indeed-pam/keys/*`

- Выполните объединение **.crt** и **.key** в `/certs/` и `/keys/rdp-proxy/` с указанием корневого **ca** из `/ca-certificates/` в **.pfx** с помощью команды:
  `openssl pkcs12 -export -out server-fqdn.pfx -inkey pam.key -in pam.crt -certfile ca.crt`
- YML-файлы: `/etc/indeed/indeed-pam/*.yml`

- Bash команда для быстрого бэкапирования конфигурационных файлов и сертификатов PAM с сервера. Создаёт папку с именем сервера в месте запуска и копирует конфигурационные файлы и сертификаты в неё:

Bash

```
sudo bash -c '
serverName=$(hostname)
basePath="$(pwd)/$serverName"
folders=("Core" "IdP" "MC" "UC" "LogServer/targets" "ProcessProtection" "FileProtection"
"GatewayService" "Nginx" "RDPProxy" "SSHProxy" "Certificates/ca-certificates"
"Certificates/certs" "Certificates/keys" "Yml")
declare -A filesToCopy=(
["/etc/indeed/indeed-pam/core/appsettings.json"]="Core"
["/etc/indeed/indeed-pam/idp/appsettings.json"]="IdP"
["/etc/indeed/indeed-pam/mc/config.prod.json"]="MC"
["/etc/indeed/indeed-pam/uc/config.prod.json"]="UC"
["/etc/indeed/indeed-pam/nginx"]="Nginx"
["/etc/indeed/indeed-pam/rdp-proxy/appsettings.json"]="RDPProxy"
["/etc/indeed/indeed-pam/ssh-proxy/appsettings.json"]="SSHProxy"
["/etc/indeed/indeed-pam/gateway-service/appsettings.json"]="GatewayService"
["/etc/indeed/indeed-pam/.env"]=".env"
["/etc/indeed/indeed-pam/ls/clientApps.config"]="LogServer"
["/etc/indeed/indeed-pam/ls/targets"]="LogServer/targets"
["/etc/indeed/indeed-pam/ca-certificates"]="Certificates/ca-certificates"
["/etc/indeed/indeed-pam/certs"]="Certificates/certs"
["/etc/indeed/indeed-pam/keys"]="Certificates/keys"
["/etc/indeed/indeed-pam/*.yml"]="Yml"
)
for folder in "${folders[@]}"; do mkdir -p "$basePath/$folder"; done
for src in "${!filesToCopy[@]}"; do
dest="$basePath/${filesToCopy[$src]}"
if [[ "$src" == *"*"* ]]; then
cp -r $src "$dest" 2>/dev/null
else
[ -d "$src" ] && cp -r "$src"/* "$dest" 2>/dev/null
[ -e "$src" ] && [ ! -d "$src" ] && cp "$src" "$dest" 2>/dev/null
fi
done
for folder in "${folders[@]}"; do [ ! "$(ls -A "$basePath/$folder" 2>/dev/null)" ] &&
rmdir "$basePath/$folder" 2>/dev/null || true; done
'
```

3. Загрузите и распакуйте дистрибутив Indeed PAM 3.0 на подготовленный Linux-сервер.

Перед обновлением

1. Перед обновлением выполните бэкап виртуальных серверов Indeed PAM, включая серверы СУБД, используемые системой для хранения данных, и/или всех баз данных.
2. Убедитесь, что на время обновления в системе отсутствуют активные сессии пользователей и администраторов PAM.

Обновление

Запуск Wizard

1. Распакуйте дистрибутив и перейдите в директорию `IndeedPAM_3.0_RU\indeed-pam\` .

2. Если доступ к Windows-серверам осуществляется через **winrm по HTTPS**, убедитесь, что сертификат УЦ, добавляемый на **этапе 3** в разделе **Заполнение вкладок в Wizard**, доверяет сертификатам winrm на серверах.

3. Если доступ к каталогу пользователей осуществляется через **LDAPS** и требуется интерактивный выбор пользователя, которому будут выданы права администратора ролей, положите сертификат удостоверяющего центра в директорию `IndeedPAM_3.0_RU\indeed-pam\state\ca-certificates\` .

4. Если требуется использование сертификатов для Wizard, отличных от самоподписанных, выполните разделение **.pfx** сертификата на **.crt** и **.key** с помощью команд:

```bash
openssl pkcs12 -in web.pfx -clcerts -nokeys -nodes -out pam.crt
openssl pkcs12 -in web.pfx -nocerts -nodes -out pam.key
```

Поместите полученные файлы в директорию `IndeedPAM_3.0_RU\indeed-pam\state\certs-web-wizard\`.

5. Выполните команду:

```bash
sudo bash run-wizard.sh
```

6. После выполнения скрипта откройте URL, указанный в консоли.
7. Введите **AuthenticationCode**, отображённый в консоли, в поле **Код аутентификации**.
8. Выберите пункт **Новая конфигурация**.
9. Нажмите **Далее**.

Заполнение вкладок в Wizard

1. Во вкладке **Схема хостов**:
   - В поле **FQDN PAM** укажите общее имя PAM, по которому система была доступна.
   - В секции **Хосты** добавьте все серверы, на которых установлены компоненты Indeed PAM, укажите установленные на них компоненты и учётные записи для доступа к ним.
   - В секции **Балансировщики** выберите подходящий вариант:
     - **Не использовать**: для инсталляции без балансировки.
     - **HAProxy**: для балансировки с использованием встроенных балансировщиков Indeed PAM. Добавьте серверы с балансировщиками. Если добавлено два балансировщика, укажите способ связи между ними:
       - **keepalived PAM**: укажите виртуальный IP-адрес.
       - **Сторонняя служба**: оставьте отметку напротив **Использовать ProxyProtocol**.
     - **Сторонний**: для использования внешних балансировщиков.
   - Нажмите **Далее**.

2. Во вкладке **Порты** укажите значения, если они отличаются от сетевой архитектуры по умолчанию, по каким портам будут работать компоненты PAM. Если ранее был выбран пункт **HAProxy**, укажите порты, которые балансировщики будут прослушивать.
3. Во вкладке **Сертификаты** выполните следующие действия:
   - В поле **Сертификат УЦ без приватного ключа** укажите подготовленный сертификат удостоверяющего центра, который имеет доверие к веб-сертификатам, добавляемым в Wizard.
   - В поле **Тип сертификатов** выберите один из вариантов:
     - **Отдельный**: если для каждого сервера с компонентами PAM используется отдельный веб-сертификат.
     - **Wildcard**: если для серверов PAM используется единый Wildcard-сертификат.
   - Укажите один пароль для всех PFX-сертификатов.
   - Загрузите PFX-сертификаты в соответствующие поля:
     - Если выбран пункт **Отдельный**, укажите имя сервера и FQDN PAM для каждого сертификата.
     - Если выбран пункт **Wildcard**, загрузите только один сертификат.
   - Нажмите **Далее**.
4. Во вкладке **Базы данных** выполните следующие действия:
   - Откройте из бэкапов конфигурационные файлы **Core**, **Idp**, **LogServer**(Pam. DbTarget.config).
   - Укажите информацию о базе данных из расшифрованных конфигурационных файлов:
     - **Тип сервера**:
       - Если в `Core/appsettings.json:"Database":"Provider":"<значение>"` указано **pgsql**, выберите **PostgreSQL**.
       - В остальных случаях выберите **Microsoft SQL**.
     - **Адрес сервера**: значение параметра **Server** или **Data Source** в `Core/appsettings.json:"ConnectionStrings":"PamCore":" Server=<значение> или Data Source=<значение>"`.
       - Если в значении параметра **Data Source** присутствуют символы `\\`, то текст после них является наименованием инстанса **Microsoft SQL**

. Укажите это значение в поле **Имя инстанса MSSQL**, а в поле **Адрес сервера** оставьте всё до `\\`.

- **Безопасное подключение к СУБД**: если в строке подключения к БД есть параметр **TrustServerCertificate=true** в `Core/appsettings.json:"ConnectionStrings":"DefaultConnection":"TrustServerCertificate=true"`, уберите галочку, в противном случае оставьте галочку активной.
- **Пользователь и пароль**: значения параметров **User Id** и **Password** в `Core/appsettings.json:"ConnectionStrings":"PamCore":"User Id=<значение>;Password=<значение>"`.
- В поле **Ключи шифрования** выберите **Указать свой**:
  - В поле **Ключ для базы Core** укажите значение параметра **Key** в `Core/appsettings.json:"Encryption":"Primary":"Key":"<значение>"`.
  - В поле **Ключ для базы IDP** укажите значение параметра **Key** в `Idp/appsettings.json:"Encryption":"Primary":"Key":"<значение>"`.
- В секции **Базы данных** скорректируйте наименования баз данных PAM в СУБД:
  - **БД для привилегированных УЗ (Core)**: значение параметра **Database** в `Core/appsettings.json:"ConnectionStrings":"PamCore":"Database=<значение>"`.
  - **БД для задач по расписанию (CoreJobs)**: значение параметра **Database** в `Core/appsettings.json:"ConnectionStrings":"JobsQueue":"Database=<значение>"`.
  - **БД для аутентификаторов пользователей PAM (Idp)**: значение параметра **Database** в `Idp/appsettings.json:"ConnectionStrings":"DefaultConnection":"Database=<значение>"`.
  - **БД для задач по расписанию (IdpJobs)**: значение параметра **Database** в

`Idp/appsettings.json:"ConnectionStrings":"JobsQueue":"Database=<значение>"`

.

- **БД для событий PAM (ILS)**: значение параметра **Database** в `LogServer/Pam.DbTarget.config: <Settings><ConnectionString>Database=<значение>`

.

- Нажмите **Далее**.

5. Во вкладке **Хранилище данных**:

- Откройте из бэкапов конфигурационные файлы **Core** и **Gateway Service**:
  - В конфигурационных файлах `Core/appsettings.json:"Storage":"Type":"<значение>"` и `Gateway Service/appsettings.json:"Storage":"Type":"<значение>"` сравните значение параметров **Type**. Если значения не совпадают, потребуется дополнительное редактирование конфигурационных файлов после обновления.
  - Укажите значение параметра `Core/appsettings.json:"Storage":"Type":"<значение>"`:
    - **FileSystem**:
      - Выберите **Тип хранилища** — **Файловая система**.
      - Если серверы управления расположены на Windows, заполните поле **Корневая директория хранилища** значением параметра **Root** из `Core/appsettings.json:"Storage":"Root":"<значение>"`, убрав экранирование символов (например, `C:\\ProgramData\\Indeed\\Indeed PAM\\PamStorage` следует указать как `C:\ProgramData\Indeed\Indeed PAM\PamStorage`).
    - **SMB**:
      - Выберите **Тип хранилища** — **SMB**.
      - **Сетевой путь**: значение параметра **Root** из `Core/appsettings.json:"Storage":"Root":"<значение>"` без экранирования символов (например, `\\\\storage.indeed.local\\Share\\MediaData\\` следует указать как `\\storage.indeed.local\Share\MediaData\`).

    - **Домен**: значение параметра **Domain** из `Core/appsettings.json:"Storage":"Domain":"<значение>"`.
    - **Имя пользователя**: значение параметра **Login** из `Core/appsettings.json:"Storage":"Login":"<значение>"`.
    - **Пароль**: значение параметра **Password** из `Core/appsettings.json:"Storage":"Password":"<значение>"`.
- **rclone**:
    - Выберите **Тип хранилища** — **S3**.
    - **Сетевой адрес S3-сервера**: значение параметра **RCLONE_S3_ENDPOINT** из `Core/appsettings.json:"Storage":"Settings":"EnvironmentVariables":"RCLONE_S3_ENDPOINT":"<значение>"`.
    - **Путь до корневой директории хранилища на S3-сервере**: значение параметра **Root** из `Core/appsettings.json:"Storage":"Settings":"Root":"<значение>"`.
    - **Идентификатор ключа доступа (access key id)**: значение параметра **RCLONE_S3_ACCESS_KEY_ID** из `Core/appsettings.json:"Storage":"Settings":"EnvironmentVariables":"RCLONE_S3_ACCESS_KEY_ID":"<значение>"`.
    - **Секретный ключ доступа (secret access key)**: значение параметра **RCLONE_S3_SECRET_ACCESS_KEY** из `Core/appsettings.json:"Storage":"Settings":"EnvironmentVariables":"RCLONE_S3_SECRET_ACCESS_KEY":"<значение>"`.
    - **Регион**: значение параметра **RCLONE_S3_REGION** из `Core/appsettings.json:"Storage":"Settings":"EnvironmentVariables":"RCLONE_S3_REGION":"<значение>"`.

- **Ограничение локации**: значение параметра **RCLONE_S3_LOCATION_CONSTRAINT** из
  `Core/appsettings.json:"Storage":"Settings":"EnvironmentVariables":"RCLONE_S3_LOCATION_CONSTRAINT":"<значение>"`
  .
- Нажмите **Далее**.

6. Во вкладке **Каталоги пользователей**:
   - Откройте из бэкапов конфигурационный файл **Core**.
   - Для каждой секции с параметром **Id** в
     `Core/appsettings.json:"UserCatalog":"Providers":Ldap": [{"Id":"<значение>"}`
     нажмите **Добавить каталог** и выполните следующие действия:
     - В поле **Служба каталогов** выберите значение параметра **ConnectorType** из
       `Core/appsettings.json:"UserCatalog":"Providers":Ldap":[{"ConnectorType":"<значение>"}`
     - В поле **ID каталога** вставьте значение параметра **Id** из
       `Core/appsettings.json:"UserCatalog":"Providers":Ldap": [{"Id":"<значение>"}`
     - В поле **DNS-имя домена** вставьте значение параметра **Domain** из
       `Core/appsettings.json:"UserCatalog":"Providers":Ldap": [{"Domain":"<значение>"}`
     - В поле **DN контейнера пользователей** вставьте значение параметра **ContainerPath** из
       `Core/appsettings.json:"UserCatalog":"Providers":Ldap":[{"ContainerPath":"<значение>"}`
       - Если в секции
         `Core/appsettings.json:"UserCatalog":"Providers":Ldap":[{"CatalogFilter":`
         присутствует параметр **CatalogFilter**, перенесите его и его значение в конфигурационные файлы **Idp** и **Core** после обновления.
     - В поле **Пользователь для доступа** вставьте значение параметра **UserName** из
       `Core/appsettings.json:"UserCatalog":"Providers":Ldap":[{"UserName":"<значение>"}`

- В поле **Пароль** вставьте значение параметра **Password** из

  ```
  Core/appsettings.json:"UserCatalog":"Providers":Ldap":
  [{"Password":"<значение>"}
  ```

- В поле **Использовать LDAPS** поставьте галочку, если значения параметров **Port** и **SecureSocketLayer** равны **636** и **true** в

  ```
  Core/appsettings.json:"UserCatalog":"Providers":Ldap": [{"Port":636}
  ```

  и

  ```
  Core/appsettings.json:"UserCatalog":"Providers":Ldap":
  [{"SecureSocketLayer":true}
  ```

- Если в поле **Служба каталогов** выбраны **ALD PRO** или **FreeIPA**, дополнительно выберите **Формат идентификатора пользователей и групп**. Если значение параметра **Id** в

  ```
  Core/appsettings.json:"UserCatalog":"Providers":Ldap":
  [{"GroupMapRules":{"Attributes":{"Id":"<значение>"}}
  ```

  и

  ```
  Core/appsettings.json:"UserCatalog":"Providers":Ldap":
  [{"UserMapRules":{"Attributes":{"Id":"<значение>"}}
  ```

  равно **ipaNTSecurityIdentifier**, выберите **SID**, иначе **GUID**.

- Если в каталоге пользователей используются нестандартные атрибуты для пользователей и групп, настройте их в пунктах **Соответствие атрибутов пользователей** и **Соответствие атрибутов групп пользователей** из

  ```
  Core/appsettings.json:"UserCatalog":"Providers":Ldap":
  [{"GroupMapRules":{<параметры>}
  ```

  и

  ```
  Core/appsettings.json:"UserCatalog":"Providers":Ldap":
  [{"UserMapRules":{<параметры>}
  ```

- Нажмите **Сохранить**.

- Нажмите **Далее**.

7. Во вкладке **Администраторы ролей** выполните следующие действия:
   - Откройте из бэкапов конфигурационный файл **Idp**.
   - Выберите **Указать вручную**.
   - В поле **Каталог** выберите каталог пользователей, в котором находится учётная запись с правами администратора ролей.

- В поле **ID администратора ролей** вставьте значение параметра **AdminSids** из `Idp/appsettings.json:"IdentitySettings":"AdminSids"["<значение>"]`.
  - Если значений **AdminSids** больше одного, укажите только один SID. После обновления добавьте оставшиеся значения в конфигурационные файлы **idp**.
- Нажмите **Далее**.

8. Во вкладке **Аутентификация пользователей**:
   - Откройте из бэкапов конфигурационный файл **Idp**.
   - В поле **Механизм аутентификации** выберите значение параметра **DirectoryMechanism** из файла `Idp/appsettings.json:"IdentitySettings":"DirectoryMechanism":"<значение>"`.
   - Если выбран **RADIUS**:
     - В поле **Таймаут ответа сервера** вставьте значение из параметра **Timeout** в `Idp/appsettings.json:"Radius":"Timeout":<значение>`.
     - Для каждой секции в параметре **RemoteEndpoints** из `Idp/appsettings.json:"Radius":"RemoteEndpoints":{<значения>} {<значения>}`, нажмите **Добавить сервер RADIUS** и выполните следующие действия:
       - В поле **Схема аутентификации** выберите значение параметра **AuthenticationScheme** из `Idp/appsettings.json:"Radius":"RemoteEndpoints":{<значения>} {<значения>}`.
       - В поле **Адрес сервера** вставьте значение параметра **Address** из `Idp/appsettings.json:"Radius":"RemoteEndpoints":{"Address":"<значение>"...}`.
       - В поле **Порт** вставьте значение параметра **Port** из `Idp/appsettings.json:"Radius":"RemoteEndpoints":{"Port":"<значение>"...}`.

- В поле **Секрет** вставьте значение параметра **Secret** из `Idp/appsettings.json:"Radius":"RemoteEndpoints":{"Secret":"<значение>"...}`.
- В поле **Проверять атрибут Message-Authenticator** снимите галочку только в случае, если используемое программное обеспечение не поддерживает работу с этим атрибутом. В противном случае рекомендуется оставить галочку.
- В секции **Формат имени для аутентификации** выполните настройку в зависимости от значения переменной **AuthenticationUserName** в `Idp/appsettings.json:"Radius":"RemoteEndpoints":{"AuthenticationUserName":"<значение>"...}`:
  - Если **NameWithoutDomain**, выберите пункт **Имя без домена**.
  - Если **SamCompatibleName**, выберите пункт **Имя в формате SAM: COMPANY\pamadmin**.
  - Если **PrincipalName**, выберите пункт **Имя в формате UPN:** pamadmin@company.local .
  - Нажмите **Добавить**.

- Если выбран **Windows** или **LDAP**:
  - В пункте **Включить двухфакторную аутентификацию для всех пользователей по умолчанию**, если значение параметра **Enable2faByDefault** в `Idp/appsettings.json:"IdentitySettings":"Enable2faByDefault":<значение>` — **false**, снимите галочку. В противном случае оставьте её включённой.
  - В пункте **Тип второго фактора** выберите значение параметра **SecondFaType** из `Idp/appsettings.json:"IdentitySettings":"SecondFaType":"<значение>"`. Если некоторые значения отсутствуют в wizard, добавьте их вручную в конфигурационные файлы **Idp** после обновления.
  - Если выбран **Email**:
    - Поле **SMTP-сервер** заполните значением параметра **Address** из `Idp/appsettings.json:"Smtp":"Address":"<значение>"`.

- Поле **Адрес почты отправителя** заполните значением параметра **SenderAddress** из `Idp/appsettings.json:"Smtp":"SenderAddress":"<значение>"`.
- Поле **Порт** заполните значением параметра **Port** из `Idp/appsettings.json:"Smtp":"Port":<значение>`.
- Поле **Имя пользователя** заполните значением параметра **Username** из `Idp/appsettings.json:"Smtp":"Username":"<значение>"`.
- Поле **Пароль** заполните значением параметра **Password** из `Idp/appsettings.json:"Smtp":"Password":"<значение>"`.
- В секции **TLS-шифрование** выберите значения из переменной **AllowedSslProtocols** в `Idp/appsettings.json:"Smtp":"AllowedSslProtocols":"<значения>"`.
- Нажмите **Добавить**
- В пункте **Кеширование второго фактора** установите значения из параметра **Enable2FaCacheForClients**.
- В поле **Время кеширования** укажите значение параметра **SecondFaCacheLifetimeSeconds** из `Idp/appsettings.json:"IdentitySettings":"SecondFaCacheLifetimeSeconds":<значение>`.

- Нажмите **Далее**.

9. Во вкладке **Сервер доступа**:
   - В полях **Макс. время ответа агента** и **Интервал healthcheck агента** укажите другие значения при необходимости или оставьте значения по умолчанию.
   - Нажмите **Далее**.
10. Во вкладке **Логирование**:
    - В полях **Очищать логи компонентов сервера управления, если файлов больше чем** и **Очищать логи компонентов сервера доступа, если файлов больше чем** укажите другие значения при необходимости или оставьте значения по умолчанию.
    - Нажмите **Далее**.
11. Во вкладке **События**:

- Если в конфигурационном файле **LogServer** `LogServer/clientApps.config<Application><Targets><Target ... Type="syslog"` есть **Target** с **Type** равным "**syslog**", откройте соответствующие файлы в директориях `LogServer/targetConfigs/` или `LogServer/targets/`.
  - Для каждого файла добавьте Syslog-сервер:
    - В поле **Адрес сервера** вставьте значение переменной **HostName**.
    - В поле **Порт** укажите значение переменной **Port**.
    - В поле **Сетевой протокол** укажите значение переменной **Protocol**.
    - В поле **Формат событий** укажите значение переменной **Format**.
    - В поле **Версия Syslog** укажите значение переменной **SyslogVersion**.
    - Нажмите **Добавить**.
- Нажмите **Далее**.

12. Во вкладке **Резервная копия**:
    - Введите в поле **Пароль резервной копии** пароль для файла бэкапа.
    - Нажмите **Скачать резервную копию**.
    - **ВНИМАНИЕ: сохраните бэкап конфигурации PAM и запомните пароль, чтобы упростить последующие изменения конфигурации и обновления через wizard.**
    - Способ установки:
      - **Из мастера**:
        - Нажмите **Установить**.
        - Во вкладке **Установка PAM** будет выполняться процесс инсталляции из мастера.
        - После завершения установки нажмите **Завершить работу мастера**.
      - **Вручную**:
        - Скачайте архив с конфигурационными файлами, разархивируйте его и скопируйте папки с заменой на сервер wizard в директорию `IndeedPAM_3.0_RU/indeed-pam/state/`, а файл **inventory** — в `IndeedPAM_3.0_RU/indeed-pam/`.
        - Нажмите **Завершить работу мастера**.
        - Перейдите в директорию `IndeedPAM_3.0_RU/indeed-pam/`.
        - Запустите установку командой `sudo bash run-deploy.sh --bench-skip -vvv`.

- Введите логин и пароль учётной записи с правами sudo для сервера, на котором выполняется deploy.

Изменения адресации Windows-серверов управления

В версии 3.0 из путей PAM на Windows-серверах управления был убран `/pam/`. Если используются внешние балансировщики, обновите их конфигурационные файлы, учитывая изменения пути.

Пост-настройка

Windows-серверы доступа

- **processprotection.settings.json**: при наличии сессий к Desktop-приложениям проверьте и добавьте недостающие разрешения на запуск процессов в файл `C:\Program Files\Indeed PAM\Gateway\ProcessCreateHook\processprotection.settings.json`, используя данные из бэкапа `ProcessProtection/processprotection.settings.json`.
- **Наименование коллекции PAM**: проверьте, что наименование коллекции сеансов PAM совпадает на сервере и в MC.
- **Перенос значений параметров из бэкапов**: если в версии 2.10 были изменены параметры в конфигурационных файлах, которые нельзя задать через wizard, выполните перенос этих значений в новые конфигурационные файлы.

Проверка

Проверьте работоспособность основных сценариев через PAM.

Приложение 1

Расшифровка компонентов на Windows

- Перейдите в каталог с дистрибутивом PAM 2.10:

```
..\PAM_2.10.*\Indeed-pam-windows\MISC\ConfigurationProtector\
```

- Запустите PowerShell от имени администратора.
- Для снятия шифрования со всех файлов конфигурации в стандартных директориях выполните команду:

```
.\Pam.Tools.Configuration.Protector.exe unprotect
```

- Для снятия шифрования с файлов конфигурации отдельных компонентов выполните команду:

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component Имя_компонента
```

Пример:

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component core
```

- Для снятия шифрования с файла, находящегося вне стандартной директории, выполните команду:

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component Имя_компонента --file
путь_к_файлу
```

Пример:

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component core --file C:
\inetpub\wwwroot\pam\core\appsettings.json
```

Расшифровка компонентов на Linux

- Перейдите в директорию с файлом протектора:

bash

```
cd /etc/indeed/indeed-pam/tools
```

- Для снятия шифрования со всех файлов конфигурации в стандартных директориях выполните команду:

```bash
bash protector.sh unprotect
```

- Для снятия шифрования с файлов конфигурации отдельных компонентов выполните команду:

  ```bash
  bash protector.sh unprotect --component Имя_компонента
  ```

  Пример:

  ```bash
  bash protector.sh unprotect --component core
  ```