Identity Console

Руководство по установке

Май 2021 г.

Уведомление

Дополнительную юридическую информацию, сведения о товарных знаках, заявлениях об отказах, гарантиях, экспортных ограничениях и ограничениях на использование, правах правительства США, политиках в отношении патентов и соответствии требованиям FIPS (Федеральный стандарт обработки информации) см. на веб-странице https://www.netiq.com/company/legal/.

Об этой книге и библиотеке

В документе *Руководство по установке* содержится информация по установке продукта NetIQ Identity Console (Identity Console). В этом руководстве определена терминология и рассмотрены сценарии внедрения.

Самая актуальная версия документа *NetIQ Identity Console Administration Guide (Руководство по администрированию NetIQ Identity Console)* доступна на английском языке на веб-сайте электронной документации по NetIQ Identity Console.

Целевая аудитория

Это руководство ориентировано на сетевых администраторов.

Другая информация в библиотеке

В данной библиотеке представлены перечисленные ниже информационные ресурсы.

Руководство по установке

В этом документе описана процедура установки и обновления Identity Console. Руководство предназначено для администраторов сети.

О NetIQ Corporation

Мы глобальная компания, которая разрабатывает корпоративное программное обеспечение, уделяя основное внимание трем постоянным проблемам в вашей среде: изменениям, сложности и риску. Мы работаем над тем, чтобы помочь вам контролировать их.

Наша точка зрения

Адаптация к изменениям и управление сложностью и риском — ничего нового

Из всех проблем, с которыми вы сталкиваетесь, указанные три проблемы, вероятно, являются самыми существенными препятствиями к тому, чтобы получить необходимый вам контроль для безопасного измерения, наблюдения и управления в отношении физических сред, виртуальных сред и сред облачных вычислений.

Обеспечение работы критически важных бизнес-сервисов: лучше и быстрее

Мы считаем, что единственный способ обеспечить своевременное и экономичное предоставление сервисов — предоставить ИТ-организациям максимально возможный контроль. По мере того как организации меняются и технологии, необходимые для управления этими изменениями, становятся все более сложными, постоянные проблемы будут только углубляться.

Наша философия

Продавать интеллектуальные решения, а не просто программное обеспечение

Чтобы обеспечить надежный контроль, сначала мы должны понять реальные сценарии, в которых изо дня в день работают ИТ-организации, наподобие вашей. Для нас это единственная возможность разрабатывать практичные, интеллектуальные ИТ-решения, которые обеспечат доказанные и измеримые результаты. И это гораздо более оправдано с точки зрения удовлетворенности результатами работы, чем просто продавать программное обеспечение.

Мы стремимся помочь вам быть более успешными

В своей работе мы ставим ваш успех на первое место. На всех этапах создания продукта — от начала разработки до развертывания — мы понимаем, что вам нужны хорошо работающие ИТ-решения, которые могут беспрепятственно интегрироваться с имеющимися ресурсами, постоянная поддержка и обучение после развертывания, а также люди, с которыми по-настоящему легко работать. Все это ради изменений. И наконец, ваш успех означает наш общий успех.

Наши решения

- Определение подлинности и управление доступом
- Управление доступом
- Управление безопасностью

- Управление системами и приложениями
- Управление рабочей нагрузкой
- Управление сервисами

Контактная информация службы поддержки продаж

С вопросами о продуктах, ценах и возможностях обращайтесь к местному партнеру. Если вам не удается связаться с партнером, обратитесь в службу поддержки продаж.

Интернациональный (Worldwide):	www.netiq.com/about_netiq/officelocations.asp
США и Канада:	1-888-323-6768
Электронная почта:	info@netiq.com
Веб-сайт:	www.netiq.com

Контактная информация службы технической поддержки

С особыми вопросами о продукте обращайтесь в нашу службу технической поддержки.

Интернациональный (Worldwide):	www.netiq.com/support/contactinfo.asp
Северная и Южная Америка:	1-713-418-5555
Европа, Ближний Восток, Африка:	+353 (0) 91-782 677
Электронная почта:	support@netiq.com
Веб-сайт:	www.netiq.com/support

Контактная информация службы документации

Наша цель — предоставить документацию, которая соответствует вашим потребностям. Если вы хотите поделиться своими предложениями по улучшению, перейдите по ссылке **Добавить комментарий** в нижней части любой HTML-страницы документации www.netiq.com/documentation. Также можно связаться с нами по электронной почте Documentation-Feedback@netiq.com. Мы высоко ценим ваше мнение. Ваши отзывы всегда желанны для нас.

Информация для доступа к интернет-сообществу пользователей

Qmunity — интерактивное сообщество NetIQ — сеть совместной работы, которая позволяет связаться с вашими коллегами и экспертами по NetIQ. В сообществе Qmunity вы можете получить информацию из первых рук, найти полезные ссылки и ресурсы, пообщаться с

экспертами по NetIQ. Таким образом, у вас есть возможность овладеть знаниями, необходимыми для реализации полного потенциала инвестиций в ИТ, на которые вы полагаетесь. Дополнительную информацию см. на веб-сайте http://community.netiq.com.

1 Планирование установки Identity Console

В этом разделе описаны требования к системе и предварительные условия для установки Identity Console. Поскольку Identity Console может выполняться как контейнер Docker или как автономное приложение, требования к системе и предварительные условия для обоих типов установки см. в соответствующих разделах.

ПРИМЕЧАНИЕ. Identity Console 1.3 поддерживает eDirectory 9.2.4 HF2 и Identity Manager Engine 4.8.3 HF2. Перед использованием этой версии Identity Console необходимо обновить экземпляры eDirectory и Identity Manager Engine.

Требования к системе и предварительные условия для установки Docker

В этом разделе описаны требования к системе и предварительные условия для установки Identity Console в качестве контейнера Docker.

Требования к системе

Поскольку Identity Console может выполняться как контейнер Docker, дополнительную информацию о требованиях к системе и поддерживаемых платформах для установки Identity Console см. в документации к Docker.

Необходимые условия

- ❒ Установите Docker 19.03.1 или более позднюю версию. Дополнительную информацию об установке Docker см. в документации к Docker.
- ❒ Необходимо получить сертификат сервера в формате `.pfx` с закрытым ключом для шифрования/дешифрования обмена данных между клиентом и сервером Identity Console. Можно использовать сертификаты сервера, сформированные какой-либо внешней сертифицирующей организацией (CA) или iManager. Например, можно сформировать сертификат сервера `keys.pfx`, используя iManager. Дополнительную информацию см. в документе Creating Server Certificate Objects (Создание объектов сертификата сервера).

Сертификат сервера `.pfx` должен содержать альтернативное имя субъекта с IP-адресом и именем DNS сервера. После создания объекта «Сертификат» сервера необходимо экспортировать его в формат `.pfx`.

- ❒ Необходимо получить сертификат сертифицирующей организации (CA) в формате `.pem` для проверки подписи сертифицирующей организации (CA) для сертификатов сервера, полученных в предыдущем действии. Этот корневой сертификат сертифицирующей организации (CA) также обеспечивает установку защищенного обмена данными LDAP между клиентом и сервером Identity Console. Например, можно получить сертификат сертифицирующей организации (CA) eDirectory (`SSCert.pem`) в расположении `/var/opt/novell/eDirectory/data/SSCert.pem`.
- ❒ (Необязательно) Используя One SSO Provider (OSP), можно включить аутентификацию с использованием единого входа для пользователей портала Identity Console. Перед установкой Identity Console необходимо установить OSP. Чтобы настроить OSP для Identity Console, выполняйте требования запросов на экране и укажите требуемые значения для параметров конфигурации. Дополнительные сведения см. в "Развертывание контейнера OSP" на стр. 20. Чтобы зарегистрировать Identity Console в имеющемся сервере OSP, необходимо вручную добавить следующие строки в файл `ism-configuration.properties` в папке `/opt/netiq/idm/apps/tomcat/conf/`:

  ```
  com.netiq.edirapi.clientID = identityconsole
  com.netiq.edirapi.redirect.url = https://<Identity Console Server IP>:<Identity Console Listener Port>/eDirAPI/v1/<eDirectory Tree Name>/authcoderedirect
  com.netiq.edirapi.logout.url = https://<Identity Console Server IP>:<Identity Console Listener Port>/eDirAPI/v1/<eDirectory Tree Name>/logoutredirect
  com.netiq.edirapi.logout.return-param-name = logoutURL
  com.netiq.edirapi.response-types = code,token
  com.netiq.edirapi.clientPass._attr_obscurity = NONE
  com.netiq.edirapi.clientPass = novell
  ```

  ПРИМЕЧАНИЕ

  - При первой установке OSP укажите `y` для параметра **Configure OSP with eDir API (Настроить OSP с использованием API eDir)** и отвечайте на запросы на экране для регистрации Identity Console с OSP.
  - При настройке Identity Console имя дерева eDirectory должно быть указано строчными буквами. В противном случае вход на сервер Identity Console может завершиться сбоем.

- ❒ Для хост-компьютера в файле `/etc/hosts` должно быть указано правильное полное доменное имя хоста.
- ❒ Чтобы использовать Identity Console в браузере Edge, необходимо загрузить Edge Chromium (v80) для обеспечения полной функциональности.

ПРИМЕЧАНИЕ. Если Identity Console используется в Mozilla Firefox, операция может завершиться сбоем с возвратом ошибки `Несоответствие источника`. Выполните следующие действия по поиску и устранению проблем:

1. Обновите Firefox до последней версии.
2. Укажите `about:config` в поле "URL-адрес Firefox" и нажмите клавишу Enter.
3. Выполните поиск по критерию "Origin".
4. Дважды щелкните `network.http.SendOriginHeader` и измените его значение на 1.

Настройка среды

Возможно, необходимо создать конфигурационный файл с определенными параметрами. Чтобы настроить Identity Console с OSP, необходимо указать параметры OSP в конфигурационном файле. Например, создайте ниже файл `identityconsole.conf` с параметрами OSP:

ПРИМЕЧАНИЕ. Необходимо указать имя своего дерева eDirectory в поле `osp-redirect-url`.

```
listen = ":9000"
ldapserver = "192.168.1.1:636"
ldapuser = "cn=admin,ou=sa,o=system"
ldappassword = "novell"
pfxpassword = "novell"
ospmode = "true"
osp-token-endpoint = "https://10.10.10.10:8543/osp/a/idm/auth/oauth2/
getattributes"
osp-authorize-url = "https://10.10.10.10:8543/osp/a/idm/auth/oauth2/grant"
osp-logout-url = "https://10.10.10.10:8543/osp/a/idm/auth/app/logout"
osp-redirect-url = "https://10.10.10.10:9000/eDirAPI/v1/edirtree/authcoderedirect"
osp-client-id = "identityconsole"
ospclientpass = "novell"
ospcert = "/etc/opt/novell/eDirAPI/conf/ssl/trustedcert/SSCert.pem"
bcert = "/etc/opt/novell/eDirAPI/conf/ssl/trustedcert/SSCert.pem"
loglevel = "error"
check-origin = "true"
origin = "https://10.10.10.10:9000,https://192.168.1.1:8543"
```

Если нужно настроить Identity Console без OSP, создайте конфигурационный файл без параметров OSP, как показано ниже:

```
listen = ":9000"
ldapserver = "192.168.1.1:636"
ldapuser = "cn=username,o=novell"
ldappassword = "novell"
pfxpassword = "novell"
ospmode = "false"
bcert = "/etc/opt/novell/eDirAPI/cert/SSCert.pem"
```

Если используется анонимная привязка, нет необходимости указывать учетные данные входа LDAP. В этом сценарии параметры `ldapuser` и `ldappassword` можно удалить из конфигурационного файла. Дополнительную информацию см. в разделе Connecting As a [Public] User (Подключение как пользователь услуг общедоступного поставщика) документа *NetIQ eDirectory Administration Guide* (Руководство по администрированию NetIQ eDirectory).

Таблица 1-1 *Описание параметров конфигурации в конфигурационном файле*

Параметры конфигурации	Описание
listen	Для порта сервера Identity Console в контейнере укажите 9000.
ldapserver	Укажите IP-адрес хост-сервера eDirectory.
ldapuser	Укажите имя пользователя eDirectory.
pfxpassword	Укажите пароль для файла сертификата .pfx.

Параметры конфигурации	Описание
ldappassword	Укажите пароль сервера LDAP.
ospmode	Укажите `true`, чтобы интегрировать OSP с Identity Console. Если задать значение `false`, Identity Console будет использовать вход LDAP.
osp-token-endpoint	Этот URL-адрес используется для получения определенных атрибутов с сервера OSP для проверки действительности маркера аутентификации.
osp-authorize-url	По этому URL-адресу пользователь указывает учетные данные для получения маркера аутентификации.
osp-logout-url	Этот URL-адрес используется для прерывания сеанса между пользователем и сервером OSP.
osp-redirect-url	Сервер OSP после предоставления маркера аутентификации перенаправляет пользователя по этому URL-адресу. **ПРИМЕЧАНИЕ.** При настройке Identity Console имя дерева eDirectory должно быть указано строчными буквами. В противном случае вход на сервер Identity Console может завершиться сбоем.
osp-client-id	Укажите ИД клиента OSP, который был указан при регистрации Identity Console в OSP.
ospclientpass	Укажите пароль клиента OSP, который был указан при регистрации Identity Console в OSP.
ospcert	Укажите расположение сертификата сертифицирующей организации (CA) сервера OSP.
bcert	Укажите расположение сертификата сертифицирующей организации (CA) Identity Console.
loglevel	Укажите только те уровни, которые нужно включить в файл журнала. Например, "Отладка", "Ошибка", "Паника" и т. д.
check-origin	Если задано значение "true", сервер Identity Console сравнивает исходное значение запросов. Доступные значения "true" или "false".
origin	Если для `check-origin` задано значение "true", Identity Console сравнивает исходное значение запросов со значениями, указанными в этом поле.
maxclients	Максимальное количество клиентов, которые могут одновременно получить доступ к `IDConsole`. Любые дополнительные клиенты сверх этого лимита должны ждать в очереди.

ПРИМЕЧАНИЕ

- Используйте параметр конфигурации `ospmode`, только если планируете интегрировать OSP с Identity Console.

- Если набор Identity Applications (Identity Apps) настроен в режиме кластера в установке Identity Manager, необходимо указать имя DNS для сервера балансировщика нагрузки в полях `osp-token-endpoint`, `osp-authorize-url` и `osp-logout-url` конфигурационного файла. В этом случае, если в этих полях указать данные сервера OSP, вход в Identity Console завершится сбоем.
- Если Identity Console настроена с тем же самым экземпляром OSP, что и Identity Apps и Identity Reporting, то при входе на портал Identity Console будет вызвана Single Sign-On (служба аутентификации).
- URL-адрес HTTPS для OSP должен быть заверен сертификатами с ключом длиной 2048 бит в Identity Console 1.1 или более ранней версии. Identity Console 1.2 поддерживает проверку сертификата с ключами длиной 4096 или 8192 бит.
- Чтобы ограничить доступ к порталу Identity Console с различных доменов, задайте параметру `samesitecookie` значение `strict`. Чтобы разрешить доступ к порталу Identity Console с различных доменов, задайте параметру `samesitecookie` значение `lax`. Если при настройке данный параметр не был указан, по умолчанию будут использоваться настройки браузера.

По окончании настройки конфигурационного файла продолжите развертывать контейнер. Дополнительную информацию см. в разделе "Развертывание Identity Console как контейнера Docker" на стр. 20.

Требования к системе и предварительные условия для автономной установки (не как контейнера Docker)

(Необязательно) Необходимые условия для конфигурации OSP

Используя One SSO Provider (OSP), можно включить аутентификацию с использованием единого входа для пользователей портала Identity Console. Перед установкой Identity Console необходимо установить OSP. Чтобы настроить OSP для Identity Console, выполняйте требования запросов на экране и укажите требуемые значения для параметров конфигурации. Дополнительные сведения см. в "Развертывание контейнера OSP" на стр. 20. Чтобы зарегистрировать Identity Console в имеющемся сервере OSP, необходимо вручную добавить следующие строки в файл `ism-configuration.properties` в папке `/opt/netiq/idm/apps/tomcat/conf/`:

```
com.netiq.edirapi.clientID = identityconsole
com.netiq.edirapi.redirect.url = https://<Identity Console Server IP>:<Identity Console Listener Port>/eDirAPI/v1/<eDirectory Tree Name>/authcoderedirect
com.netiq.edirapi.logout.url = https://<Identity Console Server IP>:<Identity Console Listener Port>/eDirAPI/v1/<eDirectory Tree Name>/logoutredirect
com.netiq.edirapi.logout.return-param-name = logoutURL
com.netiq.edirapi.response-types = code,token
com.netiq.edirapi.clientPass._attr_obscurity = NONE
com.netiq.edirapi.clientPass = novell
```

ПРИМЕЧАНИЕ

- При первой установке OSP укажите `y` для параметра **Configure OSP with eDir API (Настроить OSP с использованием API eDir)** и отвечайте на запросы на экране для регистрации Identity Console с OSP.
- При настройке Identity Console имя дерева eDirectory должно быть указано строчными буквами. В противном случае вход на сервер Identity Console может завершиться сбоем.

Требования к системе

В этом разделе описаны требования к системе и предварительные условия для установки Identity Console как автономного приложения.

Категория	Минимальные требования
Процессор	1,4 ГГц (64-разрядный)
Память	2 ГБ
Дисковое пространство	200 МБ в Linux
Поддерживаемый браузер	• Новейшая версия **Microsoft Edge** **ПРИМЕЧАНИЕ.** Чтобы использовать Identity Console в браузере Edge, необходимо загрузить Edge Chromium (v80) для обеспечения полной функциональности. • Новейшая версия **Google Chrome** • Новейшая версия **Mozilla Firefox** **ПРИМЕЧАНИЕ.** Если Identity Console используется в Mozilla Firefox, операция может завершиться сбоем с возвратом ошибки `Несоответствие источника`. Выполните следующие действия по поиску и устранению проблем: **1** Обновите Firefox до последней версии. **2** Укажите `about:config` в поле "URL-адрес Firefox" и нажмите клавишу Enter. **3** Выполните поиск по критерию "Origin". **4** Дважды щелкните `network.http.SendOriginHeader` и измените его значение на 1.

Категория	Минимальные требования
Поддерживаемая операционная система	◆ **Сертифицированные**: ◆ SUSE Linux Enterprise Server (SLES) 12 SP1, SP2, SP3, SP4 и SP5; ◆ SUSE Linux Enterprise Server (SLES) 15 SP1 и SP2; ◆ Red Hat Enterprise Linux (RHEL) 7.8, 7.9, 8.0, 8.1, 8.2 и 8.3; ◆ OpenSUSE 15.1 и 15.2. ◆ **Поддерживаемые**: поддерживаются в более поздних версиях пакетов поддержки вышеуказанных сертифицированных операционных систем.
Сертификаты	◆ Необходимо получить сертификат сервера в формате `.pfx` с закрытым ключом для шифрования/дешифрования обмена данных между клиентом и сервером Identity Console. Можно использовать сертификаты сервера, сформированные какой-либо внешней сертифицирующей организацией (CA) или iManager. Например, можно сформировать сертификат сервера `keys.pfx`, используя iManager. Дополнительную информацию см. в документе Creating Server Certificate Objects (Создание объектов сертификата сервера). Сертификат сервера `.pfx` должен содержать альтернативное имя субъекта с IP-адресом и именем DNS сервера. После создания объекта «Сертификат» сервера необходимо экспортировать его в формат `.pfx`. ◆ Необходимо получить сертификат сертифицирующей организации (CA) в формате `.pem` для проверки подписи сертифицирующей организации (CA) для сертификатов сервера, полученных в предыдущем действии. Этот корневой сертификат сертифицирующей организации (CA) также обеспечивает установку защищенного обмена данными LDAP между клиентом и сервером Identity Console. Например, можно получить сертификат сертифицирующей организации (CA) eDirectory (`SSCert.pem`) в расположении `/var/opt/novell/eDirectory/data/SSCert.pem`.

Когда будете готовы, приступайте к установке Identity Console. Дополнительную информацию см. в разделе "Развертывание автономной версии Identity Console (без среды Docker)" на стр. 23.

2 Развертывание Identity Console

В этом разделе описан процесс развертывания Identity Console вместе с рекомендациями по безопасности. Чтобы подготовиться к развертыванию, ознакомьтесь с предварительными условиями и требованиями к системе, приведенными в Глава 1 на стр. 11: "Планирование установки Identity Console".

ЗАМЕЧАНИЕ. Если Identity Console устанавливается в распределенной среде, необходимо должны установить по одному экземпляру Identity Console для каждого сервера eDirectory. Однако Identity Console следует настроить с теми серверами eDirectory, которые содержат все разделы.

Рекомендации по безопасности

- Контейнеры Docker не имеют никаких ограничений ресурсов по умолчанию. Это позволяет каждому контейнеру иметь доступ ко всем ресурсам ЦП и памяти, которые предоставляются ядром хоста. Кроме того, необходимо обеспечить, чтобы ни один выполняющийся контейнер не использовал излишние ресурсы за счет других контейнеров. Для этого нужно задать ограничения на объем ресурсов, которые может использовать один контейнер.
  - В контейнере Docker должно быть установлено жесткое ограничение для используемой им памяти. Для этого используется флаг `--memory` в команде запуска Docker.
  - В контейнере Docker должно быть ограничение на объем ЦП, используемый запущенным контейнером. Для этого используется флаг`cpuset-cpus` в команде запуска Docker.
- Для `--pids-limit` необходимо задать значение 300, чтобы ограничить количество потоков ядра, появляющихся в контейнере в каждый данный момент времени. Это необходимо для предотвращения атак DoS.
- Для политики перезапуска контейнера при сбое необходимо задать значение 5, используя флаг `--restart` в команде запуска Docker.
- После появления контейнера и отображения состояния **Healthy (Работоспособный)** необходимо использовать только контейнер. Чтобы проверить состояние работоспособности контейнера, выполните следующую команду:

  ```
  docker ps <container_name/ID>
  ```

- Контейнер Docker всегда будет запускаться от имени непривилегированного пользователя (`nds`). В качестве дополнительной меры безопасности в управляющей программе включите переназначение пространства имен пользователя для предотвращения атак с

повышением привилегий из данного контейнера. Дополнительную информацию о переназначении пространства имен пользователя см. в разделе Isolate containers with a user namespace (Изолирование контейнеров с пространством имен).

Развертывание Identity Console как контейнера Docker

В этом разделе описываются перечисленные ниже процедуры.

- "Развертывание контейнера OSP" на стр. 20
- "Развертывание Identity Console как контейнера Docker" на стр. 22

Развертывание контейнера OSP

Выполните следующие действия для развертывания контейнера OSP.

1. Загрузите файл `IdentityConsole_<версия>_Containers.tar.gz` с веб-сайта загрузок NetIQ.
2. Извлеките файл `IdentityConsole_<версия>_Containers.tar.gz`:

   ```
   tar -xvf IdentityConsole_<version>_Containers.tar.gz
   ```

3. Измените файл свойств установки без запросов в соответствии с вашими требованиями. Ниже показан образец файла свойств установки без запросов:

   ```
   # Silent file for osp with edirapi
   ## Static contents Do not edit - starts
   INSTALL_OSP=true
   DOCKER_CONTAINER=y
   EDIRAPI_PROMPT_NEEDED=y
   UA_PROMPT_NEEDED=n
   SSPR_PROMPT_NEEDED=n
   RPT_PROMPT_NEEDED=n
   CUSTOM_OSP_CERTIFICATE=y
   ## Static contents Do not edit - ends

   # OSP Details
   SSO_SERVER_HOST=osp.example.com
   SSO_SERVER_SSL_PORT=8543
   OSP_COMM_TOMCAT_KEYSTORE_FILE=/config/tomcat.ks
   OSP_COMM_TOMCAT_KEYSTORE_PWD=novell
   SSO_SERVICE_PWD=novell
   OSP_KEYSTORE_PWD=novell
   IDM_KEYSTORE_PWD=novell
   OSP_CUSTOM_NAME="Identity Console"
   USER_CONTAINER="o=novell"
   ADMIN_CONTAINER="o=novell"

   # IDConsole Details
   IDCONSOLE_HOST=192.168.1.1
   IDCONSOLE_PORT=9000
   EDIRAPI_TREENAME=ed913
   ```

```
#If ENABLE_CUSTOM_CONTAINER_CREATION is set to y
#ie., when you have user and admin container different from o=data
#and they need to be created in eDir
#then CUSTOM_CONTAINER_LDIF_PATH should be entered as well
ENABLE_CUSTOM_CONTAINER_CREATION=n
#ENABLE_CUSTOM_CONTAINER_CREATION=y
#CUSTOM_CONTAINER_LDIF_PATH=/config/custom-osp.ldif

# eDir Details
ID_VAULT_HOST=192.168.1.1
ID_VAULT_LDAPS_PORT=636
ID_VAULT_ADMIN_LDAP="cn=admin,o=novell"
ID_VAULT_PASSWORD=novell
```

4 Создайте сертификат сервера (`cert.der`) с помощью iManager и импортируйте его в хранилище ключей (`tomcat.ks`). Пример каталога: `/data`. Порядок создания сертификата сервера и его импорта в хранилище ключей

4a Запустите следующую команду, чтобы создать хранилище ключей (`tomcat.ks`). Сгенерируйте ключ, убедитесь, что полное имя или полное квалифицированное имя хоста машины является IP-адресом.

```
keytool -genkey -alias osp -keyalg RSA -storetype pkcs12 -keystore /opt/
certs/tomcat.ks -validity 3650 -keysize 1024 -dname "CN=blr-osp48-
demo.labs.blr.novell.com" -keypass novell -storepass novell
```

4b Выполните следующую команду, чтобы создать запрос на подпись сертификата (CSR). Пример: `cert.csr`.

```
keytool -certreq -v -alias osp -file /opt/certs/cert.csr -keypass novell -
keystore /opt/certs/tomcat.ks -storepass novell
```

4c Передайте этот запрос `cert.csr` в iManager и получите сертификат сервера `osp.der`. Убедитесь, что поле альтернативного имени субъекта сертификата содержит IP-адрес и имя хоста сервера OSP. Дополнительные сведения см. в разделе Создание объекта "Сертификат" сервера.

4d Запустите следующие команды, чтобы импортировать сертификат CA (`SSCert.der`) и сертификат сервера (`cert.der`) в хранилище ключей `tomcat.ks`.

```
keytool -import -trustcacerts -alias root -keystore /opt/certs/tomcat.ks -
file /opt/certs/SSCert.der -storepass novell -noprompt

keytool -import -alias osp -keystore /opt/certs/tomcat.ks -file /opt/certs/
cert.der -storepass novell -noprompt
```

5 Выполните следующую команду, чтобы загрузить образ:

```
docker load --input osp.tar.gz
```

6 Разверните контейнер с помощью следующей команды:

```
docker run -d --name OSP_Container --network=host -e SILENT_INSTALL_FILE=/
config/silent.properties -v /data:/config osp:<version>
```

Пример:

```
docker run -d --name OSP_Container --network=host -e SILENT_INSTALL_FILE=/
config/silent.properties -v /data:/config osp:6.3.9
```

Развертывание Identity Console как контейнера Docker

В этом разделе описана процедура развертывания Identity Console как контейнера Docker.

ПРИМЕЧАНИЕ. Параметры конфигурации, значения и примеры, используемые в описании этой процедуры, приведены только для справочных целей. Не используйте их непосредственно в вашей рабочей среде.

---

1 Загрузите файл `IdentityConsole_<версия>_Containers.tar.gz` с веб-сайта загрузок NetIQ.

2 Образ необходимо загрузить в локальный реестр Docker. Извлеките и загрузите файл `IdentityConsole_<версия>_Containers.tar.gz`, используя следующие команды:

```
tar -xvf IdentityConsole_<version>_Containers.tar.gz

docker load --input identityconsole.tar.gz
```

3 Создайте контейнер Docker для Identity Console, выполнив следующую команду:

```
docker create --name <identityconsole-container-name> --env ACCEPT_EULA=Y --
network=<network-type> --volume <volume-name>:/config/
identityconsole:<version>
```

Например,

```
docker create --name identityconsole-container --env ACCEPT_EULA=Y --
network=host --volume IDConsole-volume:/config/ identityconsole:1.3.0
```

ПРИМЕЧАНИЕ

- Чтобы принять условия лицензионного соглашения, задайте переменной среды `ACCEPT_EULA` значение `Y`. Кроме того, принять условия лицензионного соглашения можно в запросе, который появляется на экране при запуске контейнера с использованием параметра `-it` в команде создания Docker для интерактивного режима.
- Параметр `--volume` в вышеуказанной команде позволит создать том для хранения данных конфигурации и журнала. В этом случае в качестве образца создан том с именем `IDConsole-volume`.

---

4 Скопируйте файл сертификата сервера (`.pfx`) с локальной файловой системы в контейнер `/etc/opt/novell/eDirAPI/cert/keys.pfx`, выполнив указанную ниже команду. Дополнительную информацию о создании сертификата сервера см. в разделе "Необходимые условия" на стр. 11:

```
docker cp <absolute path of server certificate file> <identityconsole-
container-name>:/etc/opt/novell/eDirAPI/cert/keys.pfx
```

Пример:

```
docker cp /home/user/keys.pfx identityconsole-container:/etc/opt/novell/
eDirAPI/cert/keys.pfx
```

5 Скопируйте файл сертификата сертифицирующей организации (CA) (`.pem`) с локальной файловой системы в контейнер `/etc/opt/novell/eDirAPI/cert/SSCert.pem`, выполнив указанную ниже команду. Дополнительную информацию о получении сертификата сертифицирующей организации (CA) см. в разделе "Необходимые условия" на стр. 11:

```
docker cp <absolute path of CA certificate file> <identityconsole-container-name>:/etc/opt/novell/eDirAPI/cert/SSCert.pem
```

Пример:

```
docker cp /home/user/SSCert.pem identityconsole-container:/etc/opt/novell/eDirAPI/cert/SSCert.pem
```

6 Скопируйте конфигурационный файл (`identityconsole.conf`) с локальной файловой системы в контейнер `/etc/opt/novell/eDirAPI/conf/edirapi.conf`, выполнив указанную ниже команду:

```
docker cp <absolute path of identityconsole.conf> <identityconsole-container-name>:/etc/opt/novell/eDirAPI/conf/edirapi.conf
```

Например,

```
docker cp /home/user/identityconsole.conf identityconsole-container:/etc/opt/novell/eDirAPI/conf/edirapi.conf
```

7 Запустите контейнер Docker, выполнив следующую команду:

```
docker start <identityconsole-container-name>
```

Пример:

```
docker start identityconsole-container
```

ПРИМЕЧАНИЕ. В каталоге `/var/lib/docker/volumes/<volume_name>/_data/eDirAPI/var/log` находятся следующие файлы журналов:

- edirapi.log;
- edirapi_audit.log;
- container-startup.log.

Развертывание автономной версии Identity Console (без среды Docker)

В этом разделе описана процедура развертывания автономного приложения Identity Console:

1 Загрузите новейшую сборку Identity Console на веб-сайте загрузок.

2 Извлеките загруженный файл в настраиваемую папку, выполнив следующую команду:

```
tar -zxvf IdentityConsole_130_Linux.tar.gz
```

3 Откройте оболочку и перейдите к папке, в которую извлечена сборка Identity Console.

4 От имени суперпользователя или пользователя с эквивалентными правами выполните следующую команду:

```
./identityconsole_install
```

5 Ознакомьтесь с введением и нажмите клавишу **ENTER**.

6 Нажмите кнопку `Y`, чтобы принять условия лицензионного соглашения. После этого необходимые пакеты RPM будут установлены в системе.

7 Введите имя хоста сервера Identity Console (полное доменное имя в нижнем регистре) или IP-адрес. Это то же имя хоста или IP-адрес компьютера, на котором устанавливается Identity Console.

8 Введите данные порта, на котором Identity Console будет принимать входящие запросы. Если вы указываете настраиваемый порт, убедитесь, что он доступен для использования.

По умолчанию используется порт 9000.

9 Введите доменное имя/IP-адрес сервера eDirectory/Identity Vault с номером порта LDAPS.

Пример: `192.168.1.1:636`

10 Введите имя пользователя сервера eDirectory/Identity Vault.

Пример: `cn=admin,ou=sa,o=system`

11 Введите пароль пользователя сервера eDirectory/Identity Vault.

12 (Необязательно) Чтобы интегрировать Identity Console с OSP, введите `y`. Если вы не хотите интегрировать Identity Console с OSP, нажмите клавишу Enter и перейдите к п. Действ. 13. Если нужно настроить OSP, см. раздел "(Необязательно) Необходимые условия для конфигурации OSP" на стр. 15.

12a Введите доменное имя/IP-адрес сервера OSP с номером порта SSL сервера SSO.

12b Введите ИД клиента OSP, который был указан при регистрации Identity Console в OSP.

12c Введите пароль клиента OSP, который был указан при регистрации Identity Console в OSP.

12d Введите имя дерева eDirectory сточными буквами.

13 Укажите путь к доверенному корневому сертификату (`SSCert.pem`), включая имя файла.

Например, `/home/Identity_Console/SSCert.pem`.

14 Укажите путь к сертификату сервера (`keys.pfx`), включая имя файла.

Например, `/home/Identity_Console/keys.pfx`.

15 Введите пароль сертификата сервера. Дождитесь окончания установки.

ПРИМЕЧАНИЕ. В каталоге `/var/opt/novell/eDirAPI/log` находятся следующие файлы журналов:

- edirapi.log;
- edirapi_audit.log;
- identityconsole_install.log.

Журналы процесса **Запуск и остановка процесса Identity Console** находятся в каталоге `/var/log/messages`.

Остановка и перезапуск Identity Console

Остановка и перезапуск консоли Identity Console как контейнера Docker

Чтобы остановить Identity Console, запустите следующую команду:

```
docker stop <identityconsole-container-name>
```

Чтобы перезапустить Identity Console, выполните следующую команду:

```
docker restart <identityconsole-container-name>
```

Остановка и перезапуск автономного экземпляра Identity Console

Чтобы остановить Identity Console, запустите следующую команду:

```
/usr/bin/identityconsole stop
```

Чтобы запустить Identity Console, запустите следующую команду:

```
/usr/bin/identityconsole start
```

Управление сохранностью данных

Наряду с контейнерами Identity Console создаются тома для сохранности данных. Чтобы использовать параметры конфигурации старого контейнера с томами, выполните следующие действия:

1. Остановите текущий контейнер Docker, выполнив следующую команду:

   ```
   docker stop identityconsole-container
   ```

2. Создайте второй контейнер, используя данные приложения старого контейнера, сохраненные в томе Docker (`edirapi-volume-1`):

   ```
   docker create --name identityconsole-container-2 --network=host --volume
   edirapi-volume-1:/config/ identityconsole:1.0.0
   ```

3. Запустите второй контейнер, выполнив следующую команду:

   ```
   docker start identityconsole-container-2
   ```

4. (Необязательно) После этого первый контейнер можно удалить, выполнив следующую команду:

   ```
   docker rm identityconsole-container
   ```

3 Обновление Identity Console

В этом разделе описан процесс обновления Identity Console до новейших версий. Чтобы подготовиться к обновлению, ознакомьтесь с предварительными условиями и требованиями к системе, приведенными в разделе Глава 1 на стр. 11: "Планирование установки Identity Console".

Процедура обновления

При появлении новой версии образа Identity Console администратор может выполнить процедуру обновления, чтобы развернуть контейнер с новейшей версией Identity Console. Прежде чем приступать к обновлению, убедитесь, что все необходимые данные, относящиеся к приложению, постоянно хранятся в томах Docker. Порядок обновления Identity Console с использованием контейнера Docker

1. Загрузите новейшую версию образа Docker на веб-сайте загрузок NetIQ и выполните действия по установке новейшей версии Identity Console, как указано в разделе "Развертывание Identity Console" на стр. 19.
2. После загрузки новейшего образа Docker, остановите текущий контейнер, выполнив следующую команду:

   ```
   docker stop identityconsole-container
   ```

3. Создайте резервную копию общего тома.
4. Удалите существующий контейнер Identity Console, запустив следующую команду:

   ```
   docker rm <container name>
   ```

   Пример:

   ```
   docker rm identityconsole-container
   ```

5. (Необязательно) Удалите старый образ Docker Identity Console, запустив следующую команду:

   ```
   docker rmi <image ID>
   ```

6. Создайте новый контейнер, используя новый образ Identity Console Docker и данные приложения старого контейнера, сохраненные в томе Docker) (`IDConsole-volume`):

   ```
   docker create --name identityconsole-container --network=host --volume
   IDConsole-volume:/config/ identityconsole:<version>
   ```

   Пример:

   ```
   docker create --name identityconsole-container --network=host --volume
   IDConsole-volume:/config/ identityconsole:1.3.0
   ```

7. Скопируйте файл сертификата сервера (`.pfx`) с локальной файловой системы в новый созданный контейнер `/etc/opt/novell/eDirAPI/cert/keys.pfx`, выполнив следующую команду:

```
docker cp <absolute path of server certificate file> identityconsole-
container:/etc/opt/novell/eDirAPI/cert/keys.pfx
```

Пример:

```
docker cp /home/user/keys.pfx identityconsole-container:/etc/opt/novell/
eDirAPI/cert/keys.pfx
```

8 Скопируйте файл сертификата сертифицирующей организации (CA) (`.pem`) с локальной файловой системы в новый созданный контейнер `/etc/opt/novell/eDirAPI/cert/SSCert.pem`, выполнив следующую команду:

```
docker cp <absolute path of CA certificate file> identityconsole-container:/
etc/opt/novell/eDirAPI/cert/SScert.pem
```

Пример:

```
docker cp /home/user/SSCert.pem identityconsole-container:/etc/opt/novell/
eDirAPI/cert/SSCert.pem
```

9 Скопируйте конфигурационный файл (`identityconsole.conf`) с локальной файловой системы в новый созданный контейнер `/etc/opt/novell/eDirAPI/conf/identityconsole.conf`, выполнив следующую команду:

```
docker cp <absolute path of CA certificate file> identityconsole-container:/
etc/opt/novell/eDirAPI/conf/edirapi.conf
```

Пример:

```
docker cp /home/user/identityconsole.conf identityconsole-container:/etc/opt/
novell/eDirAPI/conf/edirapi.conf
```

10 Запустите второй контейнер, выполнив следующую команду:

```
docker start identityconsole-container
```

11 Чтобы проверить состояние работающего контейнера, запустите следующую команду:

```
docker ps -a
```

4 Удаление Identity Console

В этом разделе описывается процесс удаления Identity Console.

Процедура удаления для среды Docker

Чтобы удалить Docker-контейнер Identity Console, выполните следующие действия.

1. Остановите контейнер Identity Console.

   `docker stop <container-name>`

2. Запустите следующую команду, чтобы удалить Docker-контейнер Identity Console:

   `docker rm -f <container_name>`

3. Запустите следующую команду, чтобы удалить образ Docker:

   `docker rmi -f <docker_image_id>`

4. Удалите том Docker:

   `docker volume rm <docker-volume>`

ПРИМЕЧАНИЕ. Если вы удалите том, данные также будут удалены с вашего сервера.

Процедура удаления для автономного экземпляра Identity Console (без Docker)

Чтобы удалить автономный экземпляр Identity Console, выполните следующие действия.

1. Перейдите в каталог `/usr/bin` на компьютере, где установлен Identity Console.
2. Выполните следующую команду:

   `./identityconsoleUninstall`