Astra
Infrastructure
Cloud

Серверы журнала событий

Минимальные требования к серверу журнала событий

Количество серверов — 1.

Количество CPU/ядер — 2.

Оперативная память — 2 Гб.

Свободное дисковое пространство — 30 Гб.

ОС — до Astra Linux 1.7.4 включительно.

Как развернуть сервер журнала событий

Перейти в раздел **Журнал событий — Серверы журнала событий — Развернуть сервер журнала событий**.

Будет выполнен переход на карточку нового сервера.

На карточке заполнить обязательные поля **Имя компьютера** и **Имя сайта**. Имя компьютера и Имя сайта выбираются из выпадающего списка.

Имя компьютера — какой компьютер будет использоваться в качестве сервера журналирования событий. В выпадающем списке предлагаются компьютеры, незанятые под серверы в других подсистемах и системе журнала событий ранее.

Для сохранения сервера нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов.

Разворачивание сервера может занять некоторое время, отследить выполнение можно 2 способами:

1. Через всплывающие окна в нижнем правом углу экрана. Появляются событийно.
2. В разделе **Автоматизация — Задания автоматизации — Журнал заданий** название задания **audit_install**.

При успешном выполнении задания на разворачивание сервера, он появится в списке серверов на странице **Журнал событий — Серверы журнала событий — Развернуть сервер журнала событий**.

ПКД позволяет разворачивать несколько серверов журнала событий. Ограничений на количество серверов в ПКД нет.

Ограничений на количество серверов журналов событий на одном сайте нет.

Что происходит при развертывании сервера

Агент Syslog-ng используется ОС Astra Linux и уже установлен на компьютерах.

Поэтому, при развертывании только формируется запись в LDAP о выборе хоста в качестве сервера для журнала событий.

```
cn={host}, cn=log,cn=services,cn=aldpro, cn=etc
```

где `host` — имя выбранного компьютера, `base_dn` — dn домена.

Управление сервером журнала событий

В разделе **Журнал событий — Серверы журнала событий — {Имя компьютера}**.

Управление сервером журнала событий выполняется на его карточке. Для открытия карточки необходимо в списке серверов журнала событий нажать на соответствующий сервер.

На карточке сервера доступны для редактирования поля **Имя сайта**.

Для сохранения изменений нажать на кнопку сохранения в правом верхнем углу.

Будет выполнен переход к списку серверов.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

Удаление сервера журнала событий

В разделе **Журнал событий — Серверы журнала событий — {Имя компьютера}**.

Удаление сервера журнала событий осуществляется из его карточки: открыть карточку, нажав в списке серверов на соответствующий сервер, затем на карточке нажать кнопку **Удалить сервер журнала событий**. После подтверждения удаления будет выполнен переход к списку серверов журнала событий.

Что происходит при удалении сервера

При удаление сервера в интерфейсе удаляется запись в LDAP:

```
cn=host, cn=service,cn=services,cn=aldpro, cn=etc,{base_dn}
```

Раз в сутки и при перезагрузке компьютеров на компьютерах домена актуализируется состояние правил. Правила, работающие с удаленном сервером, перестают работать.