УСТАНОВКА И БАЗОВАЯ НАСТРОЙКА

RUSIEM

Всё под контролем

Что такое SIEM

SIEM (Security Information and Event Management) — решение для мониторинга и анализа любой активности, происходящей в организации

SIEM — это сложная комплексная система, позволяющая получать своевременную и всеобъемлющую информацию о состоянии ИТ-инфраструктуры предприятия.

SEM
(Security event management) — управление событиями безопасности

мониторинг в реальном времени, корреляция событий, извещения и отображение на конечных устройствах

+

SIM
(Security information management) — управление информационной безопасностью

долговременное хранение, анализ и отчетность по накопленным данным

=

SIEM

Зачем вообще SIEM

1

SIEM представляет собой улучшенную систему обнаружения вредоносной активности и различных системных аномалий.

2

Работа SIEM позволяет увидеть более полную картину активности сети и событий безопасности.

3

Когда обычные средства обнаружения по отдельности не видят атаки, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников.

Поэтому многие организации рассматривают использование SIEM-системы в качестве дополнительного и очень важного элемента защиты от целенаправленных атак.

Где может применяться SIEM

Везде, где из журналов событий можно извлечь полезную информацию.

Аудит доступа, контроль доступа к критичным ресурсам, оценка числа посетителей сайта, обнаружение malware, контроль физического доступа, оценка продаж, интересов потребителей, снижение числа ложных срабатываний, аудит финансовых показателей, анализ сетевой активности, контроль автоматизированных устройств (конвейерных лент).

Версии

Ограниченная по функциональным возможностям, бесплатно распространяемая версия системы RuSIEM. Фактически является LM (Log Management) системой с возможным расширением до RuSIEM

Коммерческая версия системы, имеющая расширенные возможности для работы. Система класса SIEM

Представляет собой модуль для коммерческой версии, который дополняет AI (искусственный интеллект), DL (обучение данных), управление активами и многие другие функции, чтобы повысить способность своевременно обнаруживать различные угрозы, решать многие задачи и визуализировать данные.

RvSIEM free

- 500 EPS
- Кластер баз данных на отдельных серверах
- Количество агентов: unlimited
- Техническая поддержка: limited
- Поддержка API
- Поиск по данным
- Симптоматика
- Отчеты

RuSIEM

- license EPS
- Кластер баз данных на отдельных серверах
- Количество агентов: unlimited
- Техническая поддержка: license, SLA
- Поддержка API
- Поиск по данным
- Симптоматика
- Отчеты
- Real-time корреляция
- Инцидент менеджмент
- Интеграция со СКУД

RuSIEM Analytics

- license EPS
- Кластер баз данных на отдельных серверах
- Количество агентов: unlimited
- Техническая поддержка: license, SLA
- Поддержка API
- Поиск по данным
- Симптоматика
- Отчеты
- Real-time корреляция
- Инцидент менеджмент
- Интеграция со СКУД

- Отслеживание аутентификации
- Vulnerability management
- Threat intelligence feeds
- Baseline
- Data learning
- Machine learning
- Compliance
- Asset management
- Аналитические отчеты

Минимальные аппаратные требования

Источник	Минимальный аудит, EPS	Полный аудит, EPS	Минимальный объем за сутки, Kb	Объем за сутки с полным аудитом, Kb
Рабочая станция Windows	10	50	320	22400
Файловый сервер	20	До 2700	640	86400
Контроллер домена	20	До 800	640	32000
Сетевое оборудование с передачей syslog	5	До 3000	160	96000
Прокси-сервер	100	До 8000	3200	256000

Минимальные аппаратные требования

Performance / Hardware Resources	Up to 2000 EPS	2 000 — 5 000 EPS	5 000 — 10 000	10 000 — 30 000	30 000 — 90 000
CPU, core count	4-8	4-6/per CPU	4-6	8-14	14+
CPU count	1	1	2+	2-4	4+
CPU, MHz	2+	2,4+	2+	2.4+	3.2+
RAM, GB	16	32	24-32	64-128	64-128+
HDD, speed	7200+	7200+	7200+	7200+	7200+
HDD, mode	Stand-alone, SAS/SATA	Stand-alone, SAS/SATA, dedicated for server	Stand-alone, SAS/SATA or raid mirror-mode. Dedicated.	Raid 5+, dedicated.	Raid 5+ performance, SSD for system disk
HDD, size for OS	100 GB	100+ GB	300 GB	500+ GB	700+ GB
HDD, size for data	300+ GB	300+ GB	600+ GB	1+ TB	3+ TB
MIPS	4700	8000	10000+	12000+	12000+

Совместимость процессора с SSE 4.2

Минимальные аппаратные требования

Основное отличие в потребляемой оперативной памяти

- RvSIEM free 16 GB
- RuSIEM 16 GB
- RuSIEM Analytics 16 GB*2 (Минимально 32 ГБ)

Мы запустили RvSIEM на 2 ГБ ОЗУ (DDR2), Intel Core 2 duo, HDD 500 GB (Sata1), но «умер» он на следующий день от своих логов. Следуйте рекомендациям.

Минимальные аппаратные требования

Расчет дискового пространства для хранения

Средний размер событий: 3 КБ
Размер детского пространства = (EPS * Время хранения * 3 * 86400)/ 1048576

Пример

10000 EPS необходимо обеспечить хранение в течении 3 месяцев
(10000 * 90 * 3 * 86400) / 1048576 = 222473

74 157 ГБ месяц при постоянном потоке событий в 10000 EPS

Минимальные аппаратные требования

При планировании ресурсов необходимо учитывать следующие факторы:

- Детализация аудита на источниках – важный фактор. Включать абсолютно весь имеющийся аудит на источниках ***бессмысленно***.
- Загруженность имеющихся гипервизоров. Большой поток событий не просто принимается и сохраняется в базы данных, но также осуществляется детальная обработка событий по множеству условий.
- Учитывайте, что вы планируете собирать, с каких источников, нужны ли все события сохранять (к примеру – нужно ли сохранить события о разрешенных соединениях и как долго требуется хранить).
- Учитывайте каналы связи между удаленными объектами. Возможно стоит поставить выделенный отдельный сервер или виртуальную машину для осуществления передачи событий.
- Учитывайте разрешенные зоны соединений. Возможно, если политикой запрещены соединения по сети – стоит пересмотреть расположение агентов/серверов или организовать выделенные vlan.

Минимальные аппаратные требования

Дата нода

CPU: 2-8
Mem: 8-64 GB
HDD: 16 — 24 ТБ

Минимальные аппаратные требования

- Ubuntu Server 14.04 x64 (обязательно x64!) http://releases.ubuntu.com/14.04/ubuntu-14.04.5-server-amd64.iso
- Ubuntu Server 18.04.4 http://releases.ubuntu.com/18.04.4/ubuntu-18.04.4-live-server-amd64.iso
- Hyperv
- ESX >= 5.5
- Доступ в интернет http/https

Архитектура

Rusiem

Одна нода:

- Пилот
- Малая организация

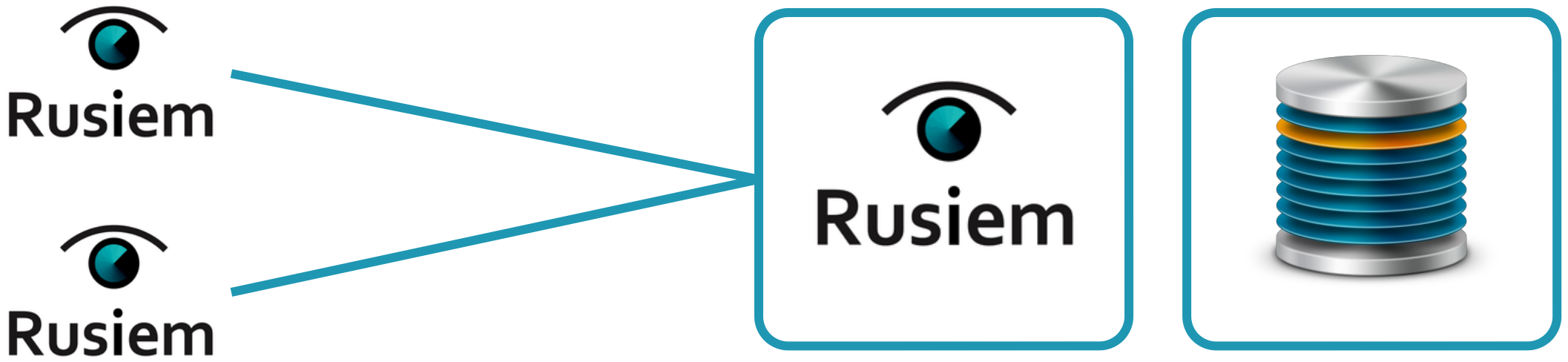
Архитектура

Rusiem

Нода + Дата нода:

- Средняя организация

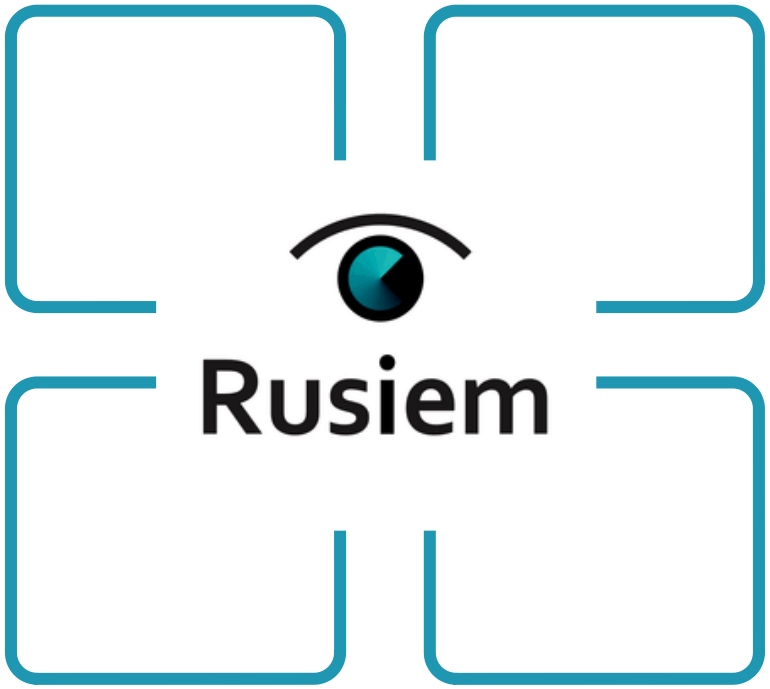
Архитектура



Нода + Дата нода + Удаленные ноды:

- Средняя организация
- Филиалы

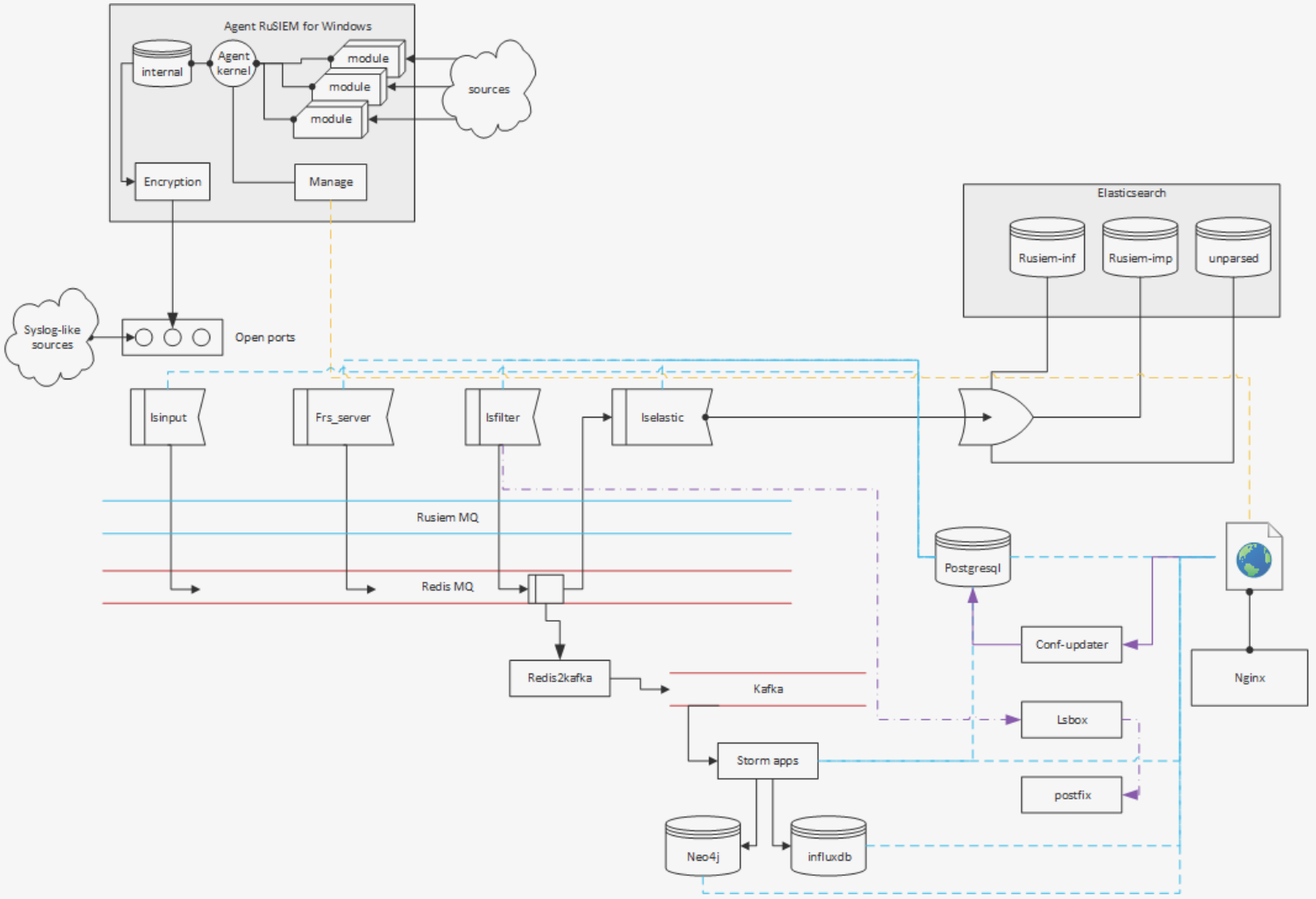
Архитектура



Нода (распределенная компонентно) + Дата нода:

- Крупная организация
- Крупный ЦОД
- Провайдер

Архитектура



Установка

```
nano /etc/hostname
nano /etc/hosts

nano /etc/network/interfaces

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 192.168.1.1 192.168.1.2
```

Установка

Получение UUID сервера

```
# dmidecode -s system-uuid |tr 'a-z' 'A-Z'
6C812441-1584-FCFA-F75B-DDEEE62A9383

# apt-get update;apt-get upgrade -y;apt-get dist-upgrade -y

# wget https://rusiem.com/install/install.sh; bash ./install.sh

# /opt/rusiem/update/bin/update-hourly.sh
```

Установка

```
Check OS (Ubuntu: trusty 14.04 or bionic 18.04 required)
PASSED: OS name is trusty
PASSED: You have 14.04 version
PASSED: running as bash ./install.sh
This utility will help you to install RuSIEM commercial version, RvSIEM free version or RuSIEM Analytics (also will be installed commercial version R
uSIEM)
More information you can find on the website:
https://rusiem.com/en (English version)
https://rusiem.com/ru (Russian version)
 ATTENTION!
 RuSIEM commercial version REQUIRES A LICENSE and previously accepted access to a private repository BEFORE install!
 RvSIEM free does not require any licenses and access, is distributed freely

At any time you can switch between versions.
For example, set RvSIEM free first. And then - for a commercial version of RuSIEM. And back.
Approximate installation time: ~20-30 min
Will be downloaded: ~200-400 Mb
Press 1 for install RvSIEM free (kernel + database)
Press 2 for install RuSIEM commercial version (kernel + database) (Subscription access required!)
Press 3 for install RuSIEM and RuSIEM analytics (kernel + database) (Subscription access required!)
Press 4 for install RuSIEM standalone database server (without any RuSIEM/RvSIEM kernel modules)

For all installations with a database on a single server - after installation, you can transfer the database to a separate server.
Select the version to install:
```

Установка

1. Бесплатная RvSIEM
2. RuSIEM+Database
3. RuSIEM Analitics + Database
4. Database

Установка Агента

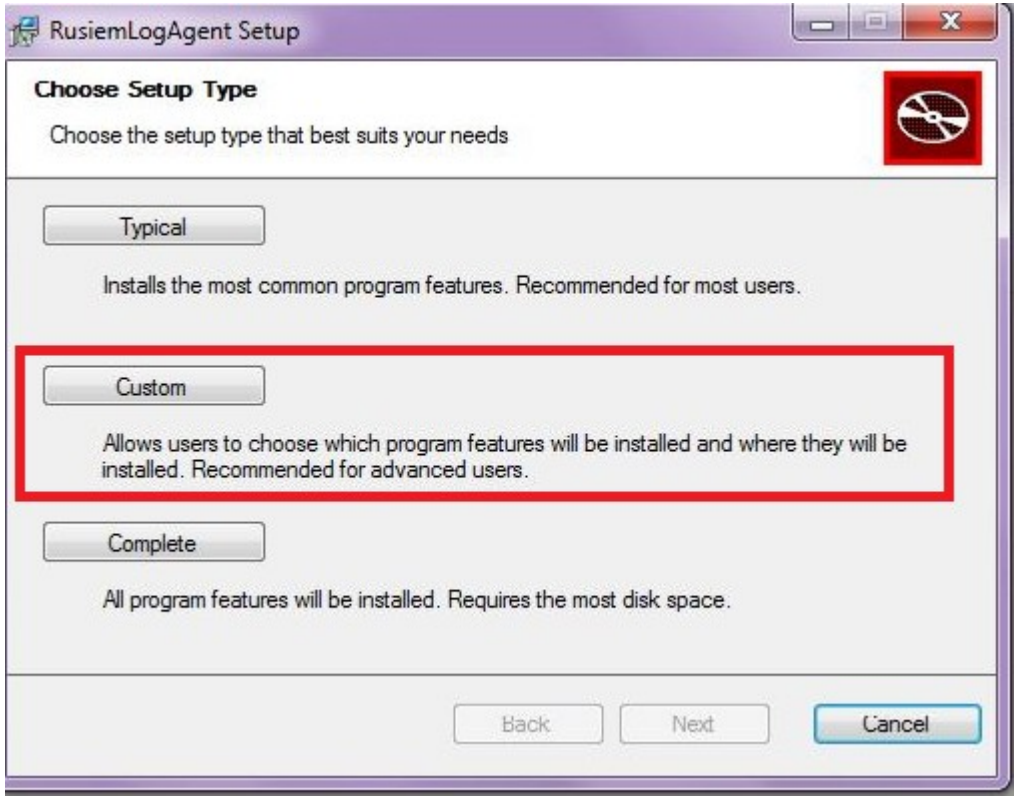
- MS Windows 7 +
- **Microsoft .NET Framework 4.5 +**

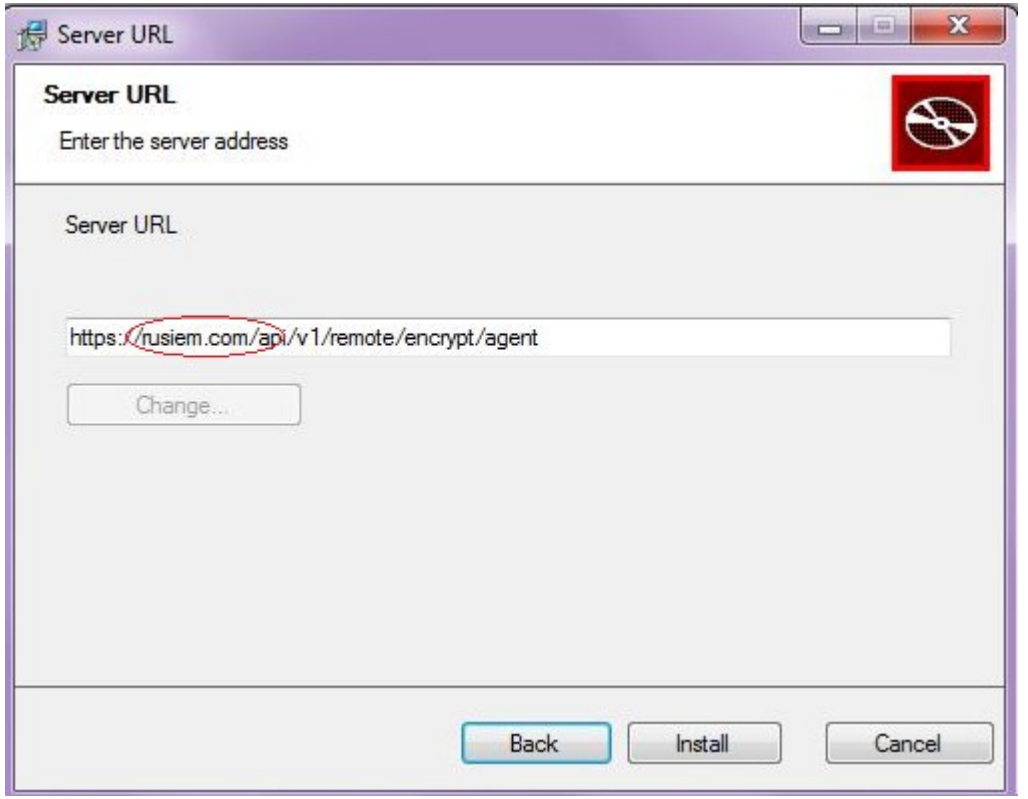
Ссылки на самую актуальную версию находятся на странице веб интерфейса в разделе "Источники" (скачивается с сервера, развернутого непосредственно у вас и обновляются вместе с обновление сервера через пакет rusiem-web).

https://x.x.x.x/files/agent/SetupRuAgent_x86.msi

https://x.x.x.x/files/agent/SetupRuAgent_x64.msi

Установка Агента





В процессе установке будет спрошен управлявший сервер - это будет ваш сервер Ru(v)SIEM. Замените адрес "rusiem.com" на адрес вашего управляющего сервера, не изменяя остальную часть URL.

Установка Агента

Управляющий сервер можно сменить в конфигурационном файле агента «C:\Program Files\Rusiem\LogAgent.config» в параметре необходимо менять лишь ip или fqdn вашего сервера

При установке агента необходимо корректно установить строку URL текущий параметры можно проверить в файле C:\Program Files\Rusiem\LogAgent.config

Строка должна иметь вид:
<add key="AdminUrl" value="https://*SIEM */api/v1/remote/encrypt/agent" />
Где *SIEM* - IP адрес SIEM

Установка Агента