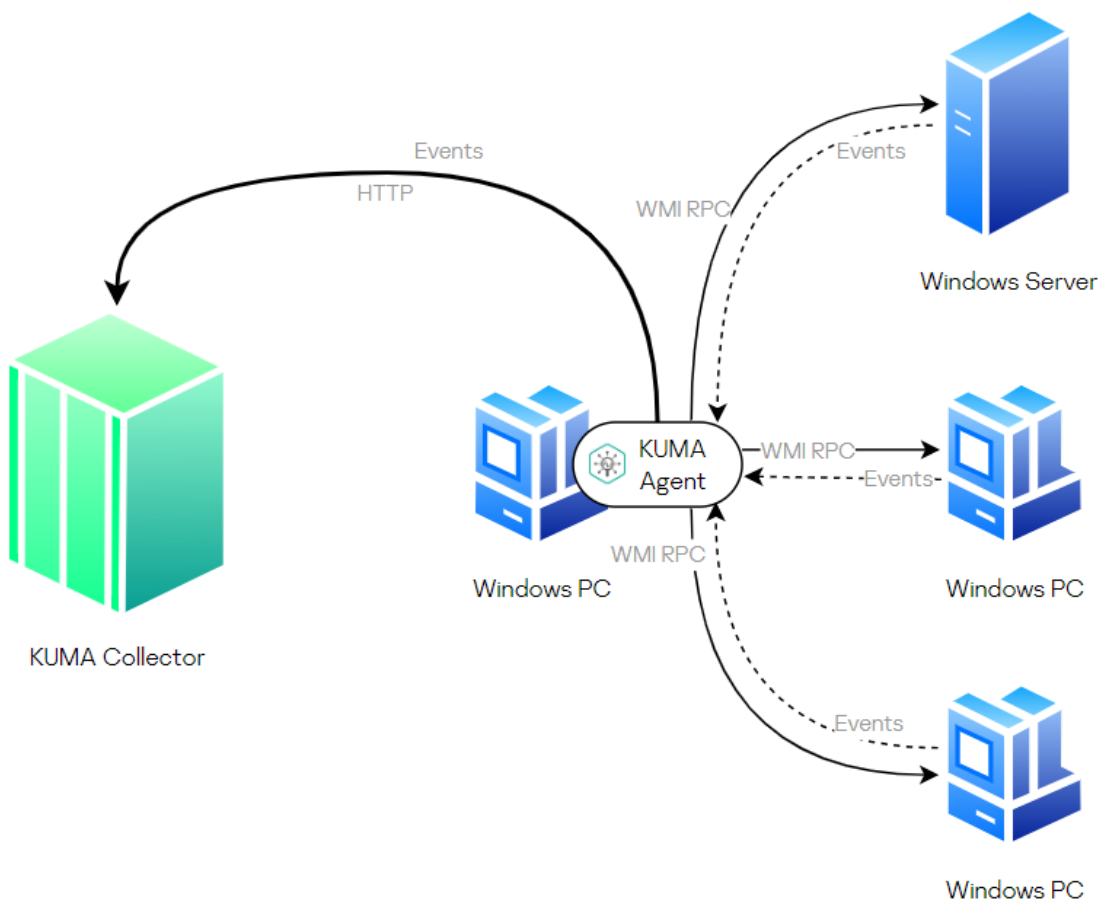


MS WMI

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

<https://www.youtube.com/embed/SxSDfGzCsO0?si=bKWWT0byXomL-OWv>

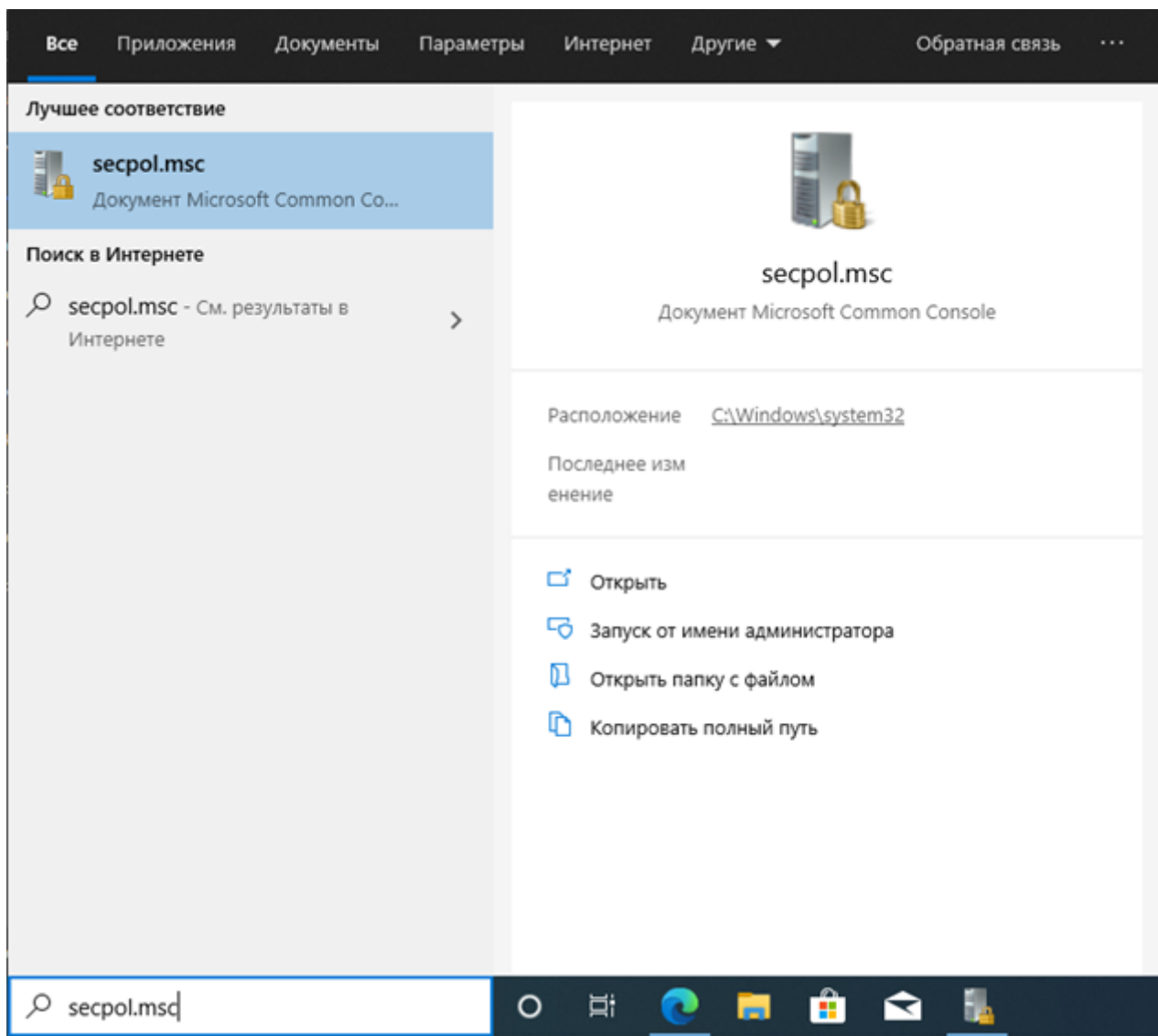
Схема работы сбора по WMI



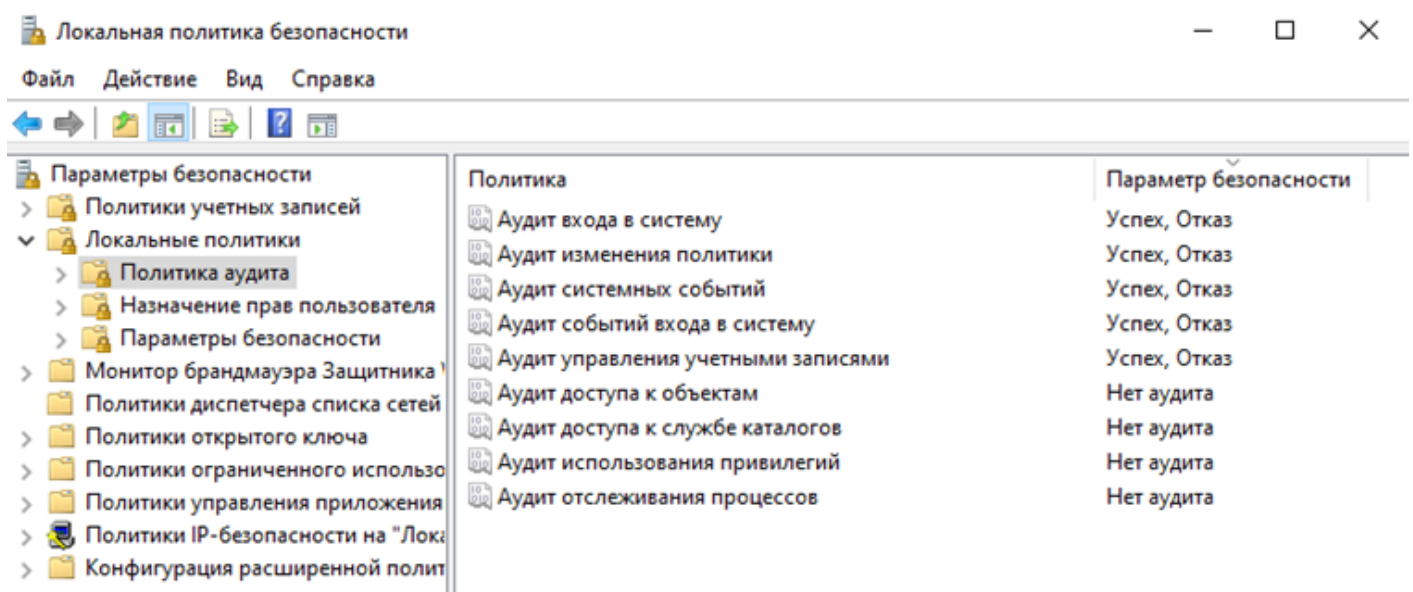
Настройка аудита отдельного сервера

Для настройки аудита на рядовом сервере/рабочей станции необходимо:

Запустить оснастку **Local Security Policy - secpol.msc**



Перейти в раздел Параметры безопасности/Локальные политики/Политика аудита и включить необходимые настройки аудита успешных и не успешных попыток.



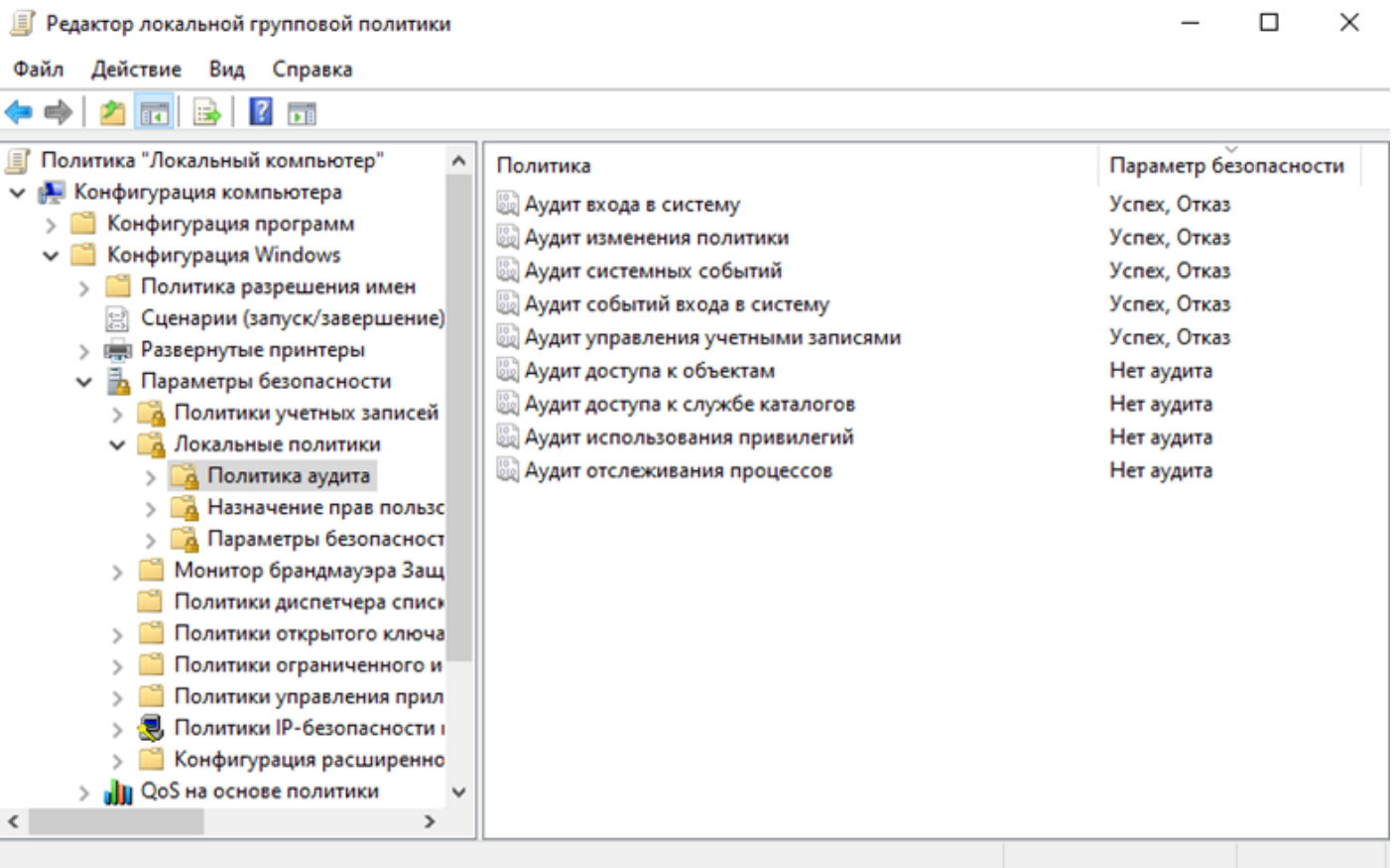
В общем случае, необходимо включить следующие параметры аудита

Аудит входа в систему	Успех, Отказ;
Аудит изменения политики	Успех, Отказ;
Аудит системных событий	Успех, Отказ;
Аудит событий схода в систему	Успех, Отказ;
Аудит управления учетными записями	Успех, Отказ;

Примеры рекомендованных политик можно найти [тут](#)

Настройка аудита при помощи групповой политики

Для централизованной настройки аудита при помощи групповых политик домена, необходимо запустить оснастку **Group Policy Management**, выбрать нужную политику и перейти к редактированию – запустится **Group Policy Management Editor**. На примере, представленном ниже, настройка аудита выполняется в рамках **Default Domain Policy**:



В случае, если предполагается сбор журналов Windows с большого количества серверов, или если установка агентов на контроллеры домена не допускается, рекомендуется

использовать перенаправление журналов на отдельные серверы с настроенной службой Windows Event Collector.

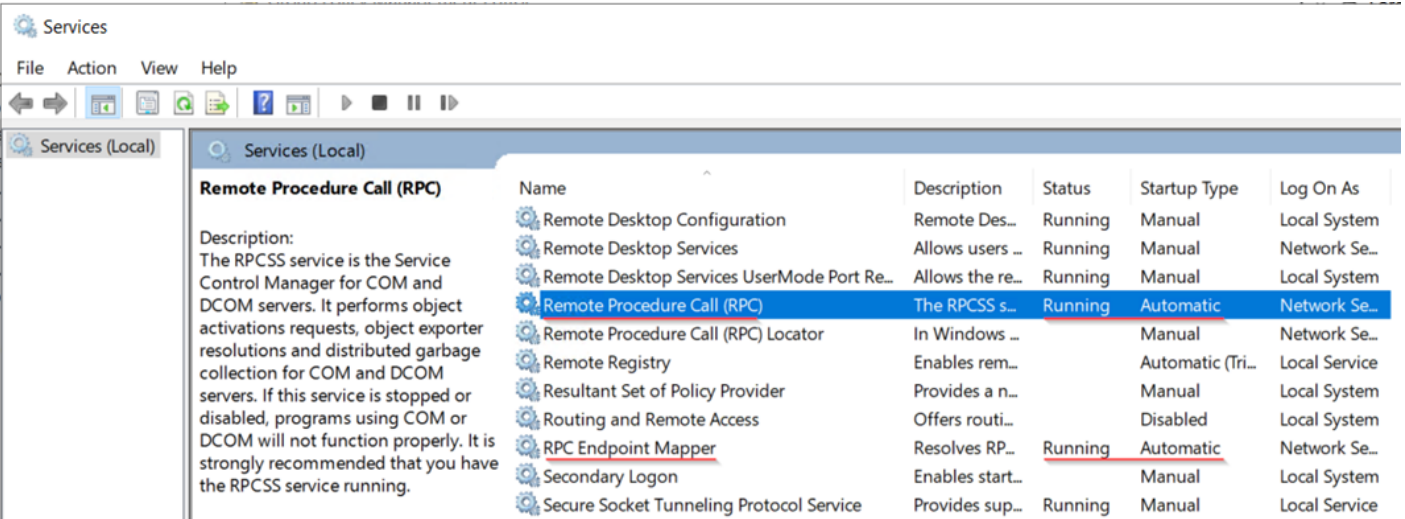
Примеры рекомендованных политик можно найти [тут](#)

Настройка сервера - источника событий

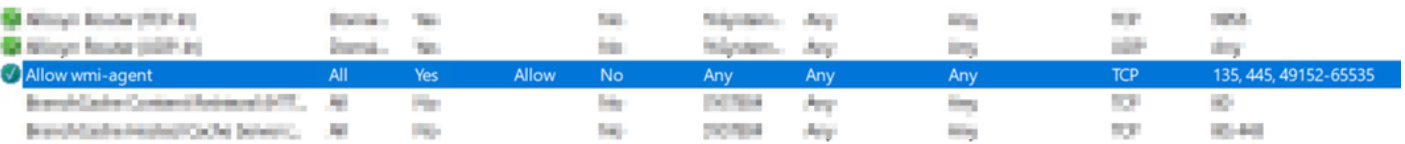
На сервере - источнике событий должны быть запущены следующие сервисы:

- Remote Procedure Call (RPC);
- RPC Endpoint Mapper.

Обозначенные выше сервисы могут быть запущены из оснастки **Службы** в Windows.



Также на сервере источнике событий должны быть открыты порты TCP: 135, 445, 5985, 49152-65535. Открыть данные порты для входящих подключений можно с помощью оснастки **Брандмауэра защитника Windows в режиме повышенной безопасности**.



Для проверки доступности целевых серверов - источников событий с компьютера, на котором планируется установка wmi-агента можно выполнить следующую команду из PowerShell:

```
Get-WmiObject -Namespace "root\cimv2" -Class Win32_Process -Impersonation 3 -ComputerName <hostname целевой машины>
```

Проверка работы выполнения удаленных WMI запросов на источнике

Выполните с хоста, где планируется к установке KUMA Agent следующую команду в PowerShell для проверки работы WinRM на удаленной машине:

```
Test-WSMan -ComputerName <Имя компьютера или IP>
```

При успешной проверке получим следующий результат:

```
PS C:\Users\boriso> Test-WSMan -ComputerName 10.68.85.2

wsmid           : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
ProtocolVersion : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
ProductVendor   : Microsoft Corporation
ProductVersion  : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

Для проверки доступа к журналам по WMI, можно выполнить следующую команду (не обязательно дожидаться конца выполнения запроса, если будет ошибка она сразу появится):

```
$strComputer = "dc-01.sales.lab"

$colLogFiles = Get-WmiObject -Class Win32_NTEventLogFile -ComputerName $strComputer | Where-Object
{$_ .LogFileName -eq 'security'}

foreach ($objLogFile in $colLogFiles)
{
    "Record Number: " + $objLogFile.NumberOfRecords
    "Maximum Size: " + $objLogFile.MaxFileSize
}
```

Создание коллектора KUMA

Для создания коллектора в веб-интерфейсе KUMA перейдите на вкладку **Ресурсы - Коллекторы** и нажмите на кнопку **Добавить коллектор**. Также можно на вкладке **Ресурсы** нажать на кнопку **Подключить источник событий**.

После выполнения указанных действий откроется соответствующий мастер. На первом шаге необходимо выбрать **Имя** коллектора и **Тенант**, к которому он будет принадлежать.

- 1 Connect event sources
- 2 Transport
- 3 Event parsing
- 4 Event filtering
- 5 Event aggregation
- 6 Event enrichment
- 7 Routing
- 8 Setup validation

Connect event sources

Collector is used to get events from event source and convert them into KUMA format for further processing. It can also filter out useless events, merge multiple events into one, and enrich events with additional data. Complete the wizard to create collector. For details see [Online Help](#).

*Collector name	<input type="text" value="Windows WMI Collector"/>
*Tenant	<input type="text" value="Main"/>
Workers	<input type="text" value="0"/>
Debug	<input type="text" value="Disable"/>
Description	<div>Description</div>

На втором шаге мастера необходимо выбрать транспорт. В данном случае рекомендуется использовать **http**. В поле URL необходимо указать порт, на котором коллектор будет ожидать соединение от агента. В качестве разделителя необходимо указать **\0**.

- 1 Connect event sources
- 2 Transport
- 3 Event parsing
- 4 Event filtering
- 5 Event aggregation
- 6 Event enrichment
- 7 Routing
- 8 Setup validation

Transport

Add a source from which you want to receive events. For details see [Online Help](#).

Basic settings Advanced settings

*Connector	<input type="text" value="Create new"/>	?
*Kind	<input type="text" value="http"/>	?
*URL	<input type="text" value=":5544"/>	?
Delimiter value	<input type="text" value="\0"/>	

На вкладке **Дополнительные параметры** для шифрованной передачи данных между агентом и коллектором необходимо выбрать **Режим TLS - С верификацией**.

1 Connect event sources

2 **Transport**

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Transport

Add a source from which you want to receive events. For details see [Online Help](#).

Basic settingsAdvanced settings

Buffer size

0

?

Character encoding

?

TLS mode

With verification

Compression

Disabled

Debug

Disabled

На третьем шаге мастера необходимо указать нормализатор. В данном случае рекомендуется использовать предустановленный расширенный нормализатор для событий Windows **[OOTB] Windows Extended v.0.3**.

1 Connect event sources

2 Transport

3 **Event parsing**

4 Event filtering

5 Event aggregation

Event parsing

Normalization schemeEnrichment

*Normalizer

[OOTB] Windows Extended v.0.3

Шаги мастера настройки с четвертого по шестой можно пропустить и вернуться к их настройке позднее.

На седьмом шаге мастера необходимо указать точки назначения. Для хранения событий необходимо добавить точку назначения типа **Хранилище**. В случае если предполагается также корреляция по событиям необходимо добавить точку назначения типа **Коррелятор**.

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Routing

Specify where processed events should be routed to. It is recommended to send events to at least two destinations: to a correlator for analysis and to a storage for retention. For details see [Online Help](#).

Storages

[Example] Storage	storage	test-kuma.sales.lab:7230
-------------------	---------	--------------------------

Correlators

[Example] Correlator	correlator	test-kuma.sales.lab:7249
----------------------	------------	--------------------------

Add destination ▾

На завершающем шаге мастера необходимо нажать на кнопку **Сохранить и создать сервис**. После чего появится строка установки сервиса, которую необходимо скопировать для дальнейшей установки.

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Setup validation

Configuring collector is complete and service is created in KUMA. For details see [Online Help](#).

To start receiving events, you must install this service on the server, dedicated for the collector (see example of the install command below). Make sure network access and ports were properly configured. For details see [Online Help](#).

Services using this collector

Kind	Name
collector	Windows WMI Collector

Save and restart services Save and reload services

Recommended command for collector installation

```
/opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 568a8ea8-7517-4097-bb71-cf673bfc3464 --api.port 7284 --install
```

Copy

Также после выполнения указанных действий на вкладке **Ресурсы - Активные сервисы** появится созданный сервис коллектора.

[Resources and services](#) >

Services

Add service Refresh

Reload Restart Copy ID Go to events Go to active lists Go to partitions Reset certificate Remove

<input type="checkbox"/>	Status	Kind ↑	Service	Version	Tenant	FQDN	IP Address	API port	Uptime
<input type="checkbox"/>	●	Collector	Windows WMI Collector		Main				

Установка коллектора KUMA

Для установки сервиса коллектора необходимо из командной строки выполнить команду, скопированную на прошлом шаге.


```
[root@test-kuma ~]# /opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 568a8ea8-7517-4097-bb71-cf673bfc3464 --api.port 7284 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-568a8ea8-7517-4097-bb71-cf673bfc3464.service → /usr/lib/systemd/system/kuma-collector-568a8ea8-7517-4097-bb71-cf673bfc3464.service.
[root@test-kuma ~]#
```

Также необходимо добавить порт коллектора в исключения фаервола и обновить параметры службы

```
firewall-cmd --add-port=5544/tcp --permanent
```

```
firewall-cmd --reload
```

После успешной установки сервиса его в статус в веб-консоли KUMA изменится на **зеленый**.

[Resources and services](#) >
Services

Add serviceRefresh

ReloadRestartCopy IDGo to eventsGo to active listsGo to partitionsReset certificateRemove

<input type="checkbox"/>	Status	Kind ↑	Service	Version	Tenant	FQDN	IP Address	API port	Uptime
<input type="checkbox"/>	●	Collector	Windows WMI Collector	2.0.0.306	Main	test-kuma.sales.lab	10.68.85.125	7284	30 seconds

Создание агента KUMA

Для создания агента в веб-интерфейсе KUMA перейдите на вкладку **Ресурсы - Агенты** и нажмите на кнопку **Добавить агент**.

В открывшейся вкладке **Общие параметры** необходимо выбрать **Имя** агента и **Тенант**, к которому он будет принадлежать.

Base settings

Config #1

+

*Agent name

Windows WMI Agent

*Tenant

Main

▼

☐ Debug

Description

На вкладке **Подключение 1** в параметрах коннектора необходимо задать тип **wmi**. Для пункта Удаленные хосты необходимо задать параметры подключения к удаленным хостам со следующими ограничениями:

- имя хоста должно содержать полный **FQDN** хоста или **ip-адрес**;
- домен хоста должен содержать **домен** хоста или, в случае отсутствия домена **FQDN** или **ip-адрес** хоста;
- тип журналов задается в соответствии с требованиями к логированию;
- в поле секрет необходимо выбрать или создать новый секрет типа **credentials** с указанием **логина и пароля**, при этом логин необходимо задавать **без доменной части (user - правильно, domain\user - неправильно, user@domain - неправильно)**. Учетная запись заданная в параметрах доступа к хосту должна быть членом группы читателей журнала событий (подробнее см. **Приложение А**).

Указывать и использовать для настройки подключения к хостам **учетную запись по умолчанию (Default credentials)** не рекомендуется.

Connector:

Basic settings

Advanced settings

Create new

*Name

Windows WMI Connector

*Kind

wmi

Default credentials

*Remote hosts:

Host	Domain	Log type	Secret
winser19.sales.lab	sales.lab	Security	winserv19
<div>+ Add new element</div>			

Указываем IP в полях Хост и Домен в случае, если используется локальная УЗ на системе для сбора логов, иначе имя хоста и его домен. В параметрах Секрет НЕ указывайте домен, достаточно использовать логин и пароль.

В общих параметрах точки назначения необходимо указать тип **http** (должен совпадать с настройками коллектора). URL нужно указать в формате **fqdn:port** (FQDN коллектора и порт, должны совпадать с настройками коллектора).

Destinations:

Basic settings

Advanced settings

Create new

*Name

Windows WMI Collector

Disabled

*Kind

http

*URL

test-kuma.sales.lab:5544

+ URL

?

*Authorization

disabled

Для версии 3.0+ параметр State (Состояние) должен быть включен:

Destinations

[Basic settings](#) [Advanced settings](#)

Destination

Create new

Name*

Windows WMI Collector

State

☒

Kind*

http

URL* ⓘ

test-kuma.sales.lab:5544

+ Add

Authorization*

Disabled

В дополнительных параметрах необходимо указать **Режим TLS С верификацией**, если требуется шифровать соединение между коллектором и агентом (настройка должна совпадать с соответствующей на стороне коллектора). Разделитель необходимо указать **\0** (должен совпадать с настройками коллектора). Также на изображении ниже приведены дополнительные параметры и их рекомендуемые значения.

Destinations:

Basic settings

Advanced settings

Compression

Disabled

Proxy

Buffer size

1073741824

?

Timeout

Timeout

?

Disk buffer size limit

1073741824

?

TLS mode

With verification

URL selection policy

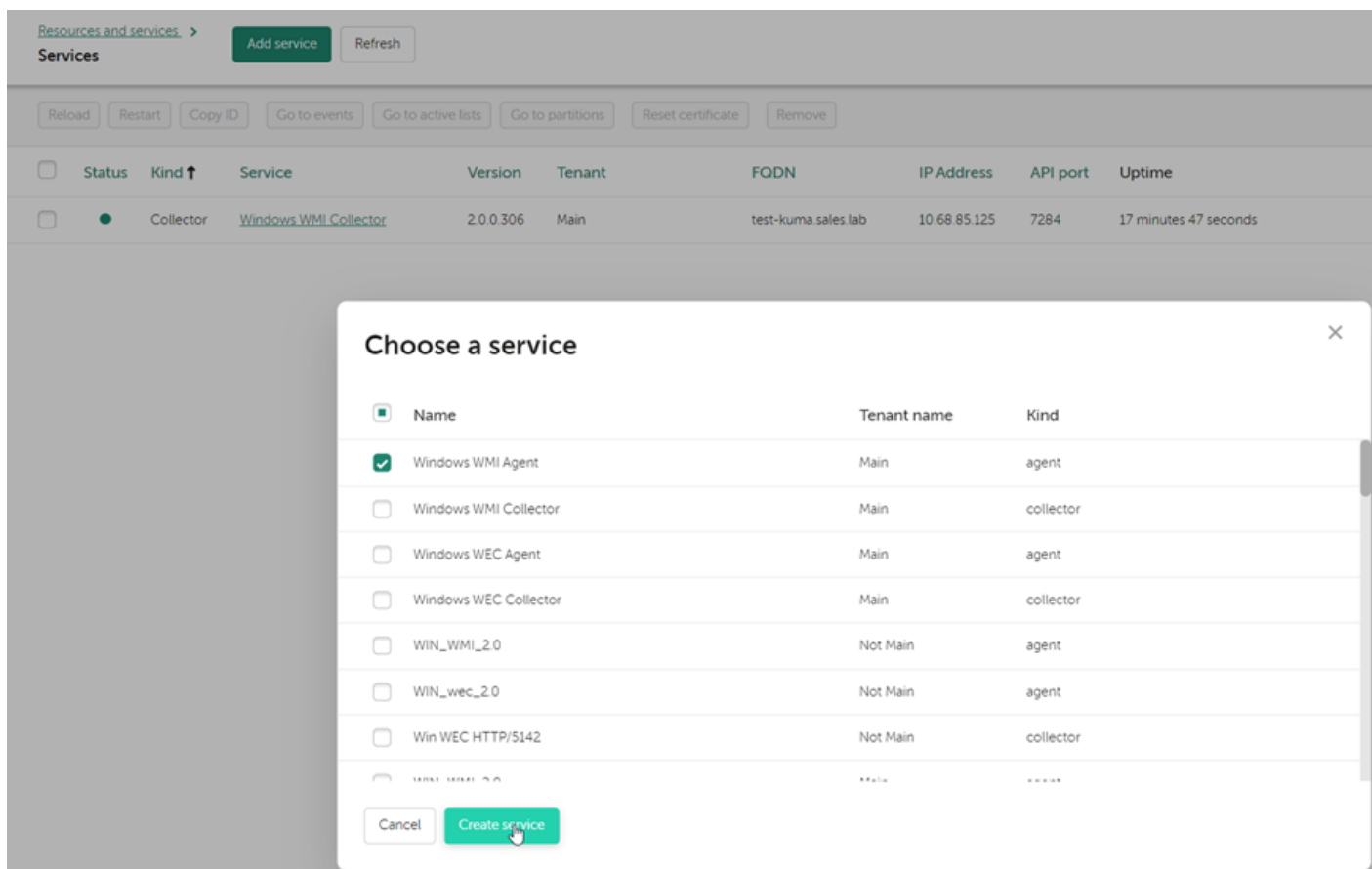
Delimiter

\0

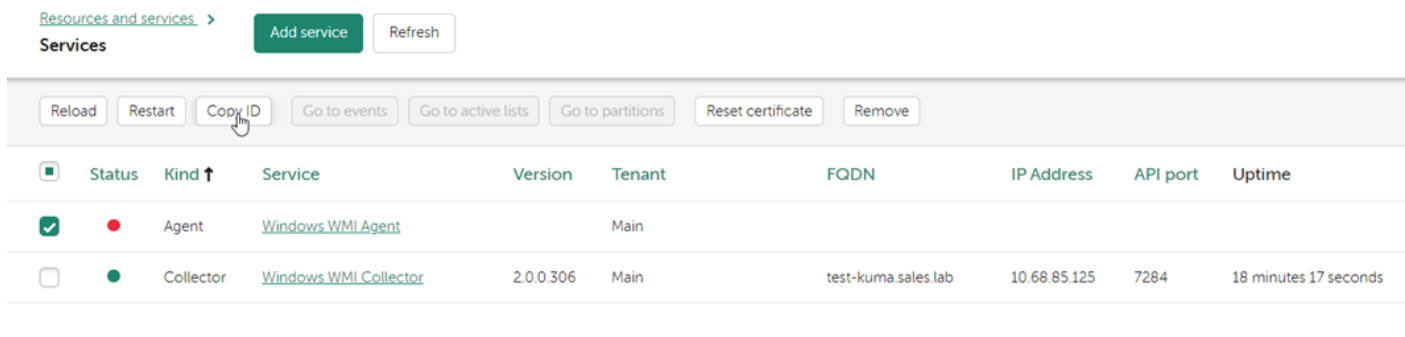
После указания всех параметров необходимо сохранить созданный ресурс агента.

Публикация агента KUMA

В разделе **Ресурсы - Активные сервисы** необходимо опубликовать созданную конфигурацию KUMA Windows Agent.



После публикации сервиса необходимо скопировать id данного сервиса для последующей установки на компьютере под управлением Windows.
















Установка агента KUMA

Выполняется на сервере Windows, журналы которого необходимо направить в KUMA. Предварительно FQDN KUMA должен быть добавлен в файл **hosts** на целевой машине, либо добавлен в DNS-зону организации.

- в файловой системе сервера рекомендуется создать папку `C:\Users\<имя пользователя>\Desktop\KUMA`
- скопировать в нее бинарный файл kuma.exe

Файл **kuma.exe** находится в архиве пакетов установки KUMA

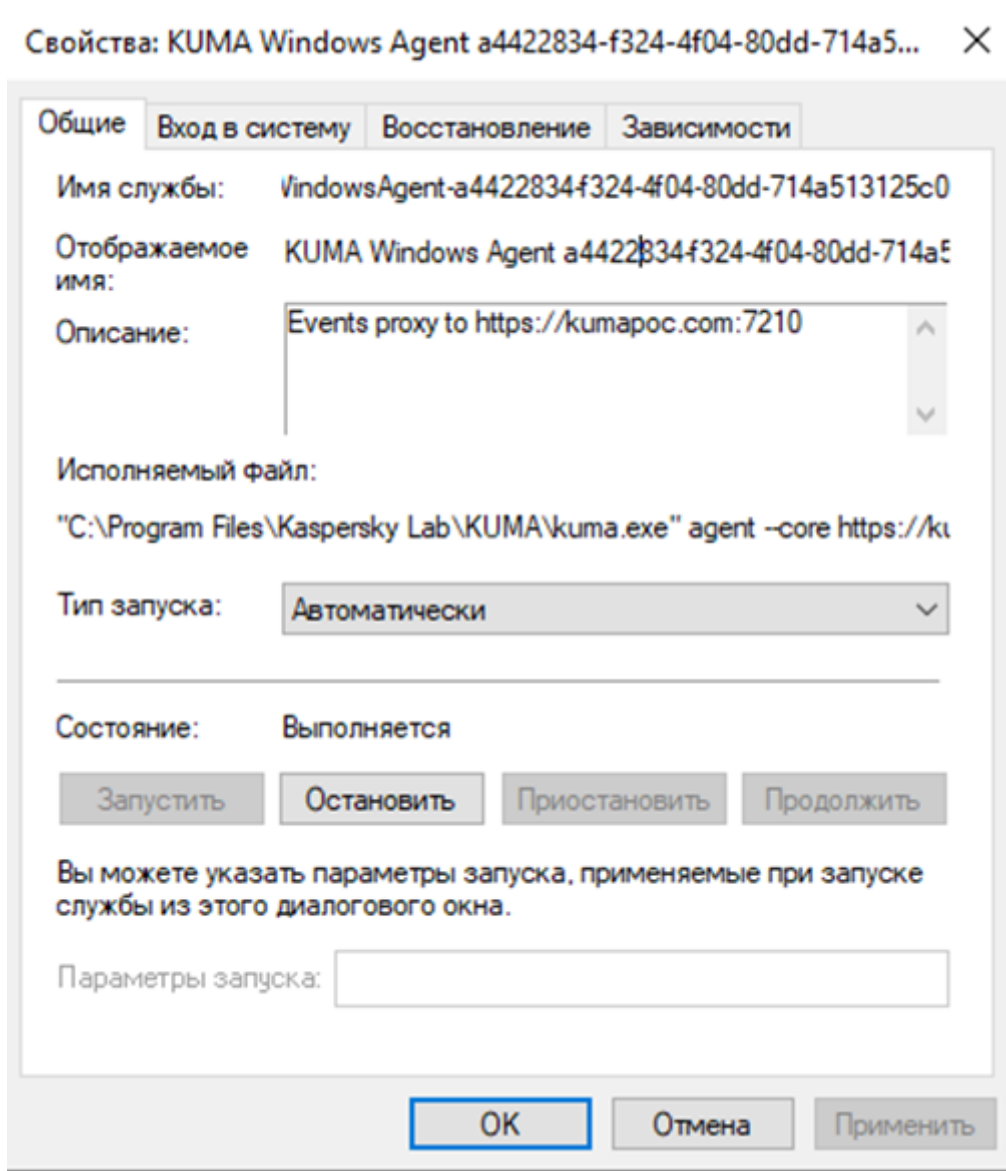
/root/KUMA/kuma-ansible-installer/roles/kuma/files/		
Name	Size	Changed
		13.09.2021 19:52:10
 clickhouse.tar.gz	94 868 KB	13.09.2021 19:52:36
 console.tar.gz	4 339 KB	13.09.2021 19:52:14
 example-content	1 806 KB	13.09.2021 19:52:10
 grafana.tar.gz	33 937 KB	13.09.2021 19:52:32
 kuma	56 291 KB	13.09.2021 19:52:37
 kuma.exe 	19 843 KB	13.09.2021 19:52:37
 LEGAL_NOTICES	187 KB	13.09.2021 19:52:10
 LICENSE	41 KB	13.09.2021 19:52:10
 license.key	4 KB	08.10.2021 10:39:28
 mongodb.tar.gz	61 866 KB	13.09.2021 19:52:25
 victoria-metrics.tar.gz	8 713 KB	13.09.2021 19:52:27

- запустить командную строку с правами администратора
- примите лицензионное соглашение: `C:\Users\<имя пользователя>\Desktop\KUMA\kuma.exe license`
- перейти в папку `C:\Users\<имя пользователя>\Desktop\KUMA`
- назначить учетной записи пользователя, от имени которой будет запускаться агент права входа в качестве службы (см. **Приложение Б**) и права на чтение журнала событий (см. **Приложение А**).
- запустить установку агента командой:

```
C:\Users\<имя пользователя>\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --id <Windows Agent ID> --user <Windows User> --install
```

```
C:\kuma>kuma.exe agent --core https://kumapoc.com:7210 --id a4422834-f324-4f04-80dd-714a513125c0 --install --user DESKTOP-68TNI3C\Gustko_I
User password:
Service KUMAWindowsAgent-a4422834-f324-4f04-80dd-714a513125c0 was installed successfully!
C:\kuma>_
```

В результате, в ОС установится сервис **KUMA Windows Agent <Windows Agent ID>**



Если статус агента веб-интерфейсе KUMA отображается как **red**, необходимо удостовериться в доступности портов 7210 и порта коллектора Windows по направлению от агента к KUMA Collector.

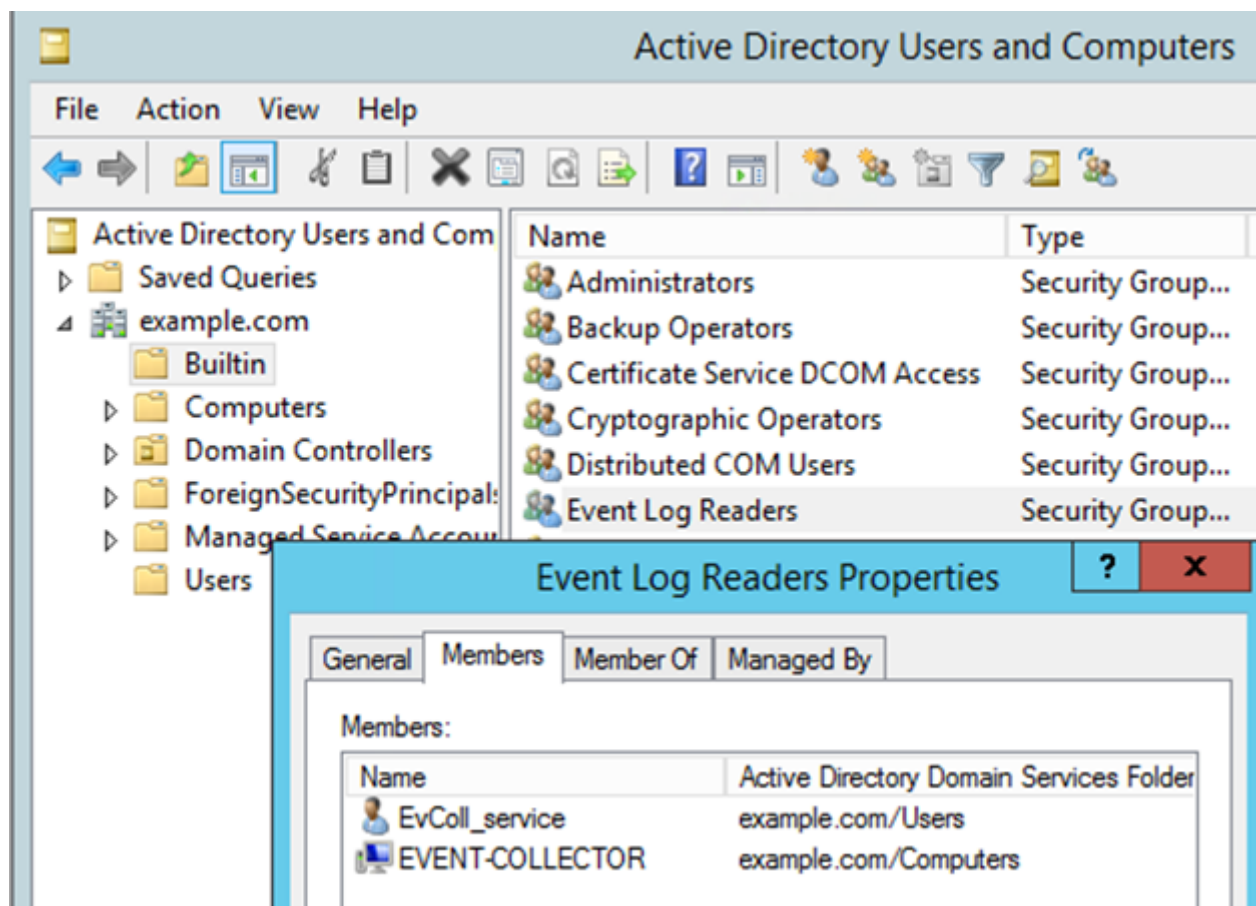
Для удаления сервиса агента по окончании тестирования продукта из ОС можно посредством следующей команды:

```
C:\Users\<имя пользователя>\Desktop\KUMA>kuma.exe agent --id <Windows Agent ID> --uninstall
```

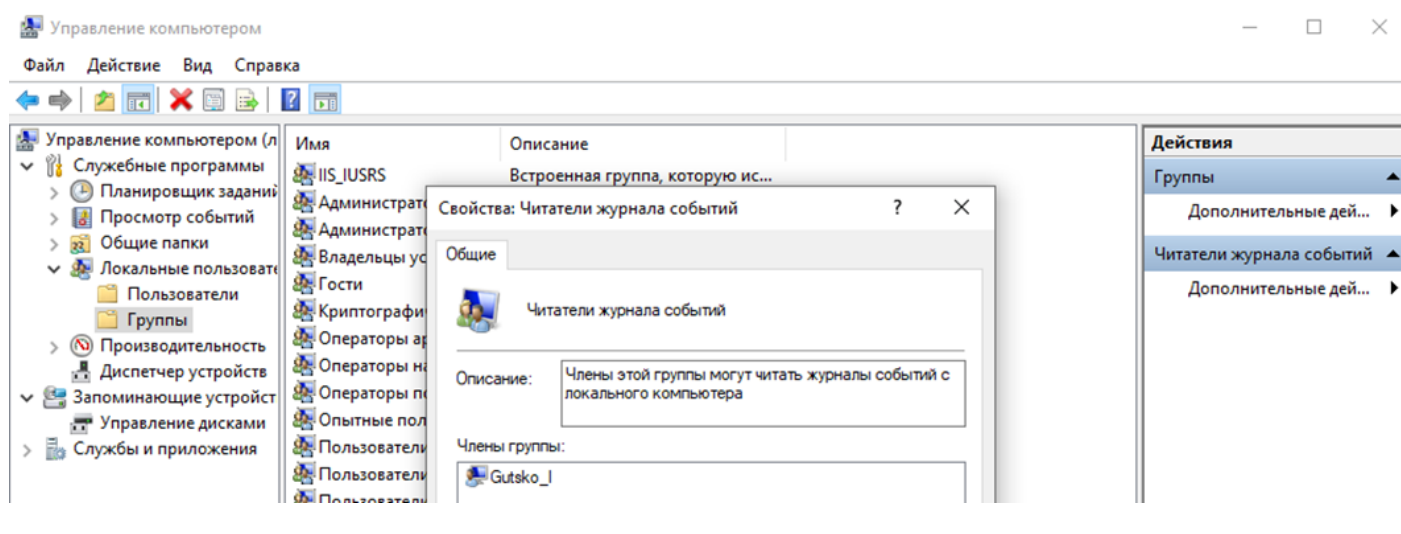
Приложение А. Назначение прав читателя журнала событий

Предоставить права читателя журнала событий в рамках домена можно при помощи оснастки **Active Directory Users and Computers** домена, добавив соответствующую

учетную запись пользователя или компьютера в встроенную группу **Event Log Readers**:



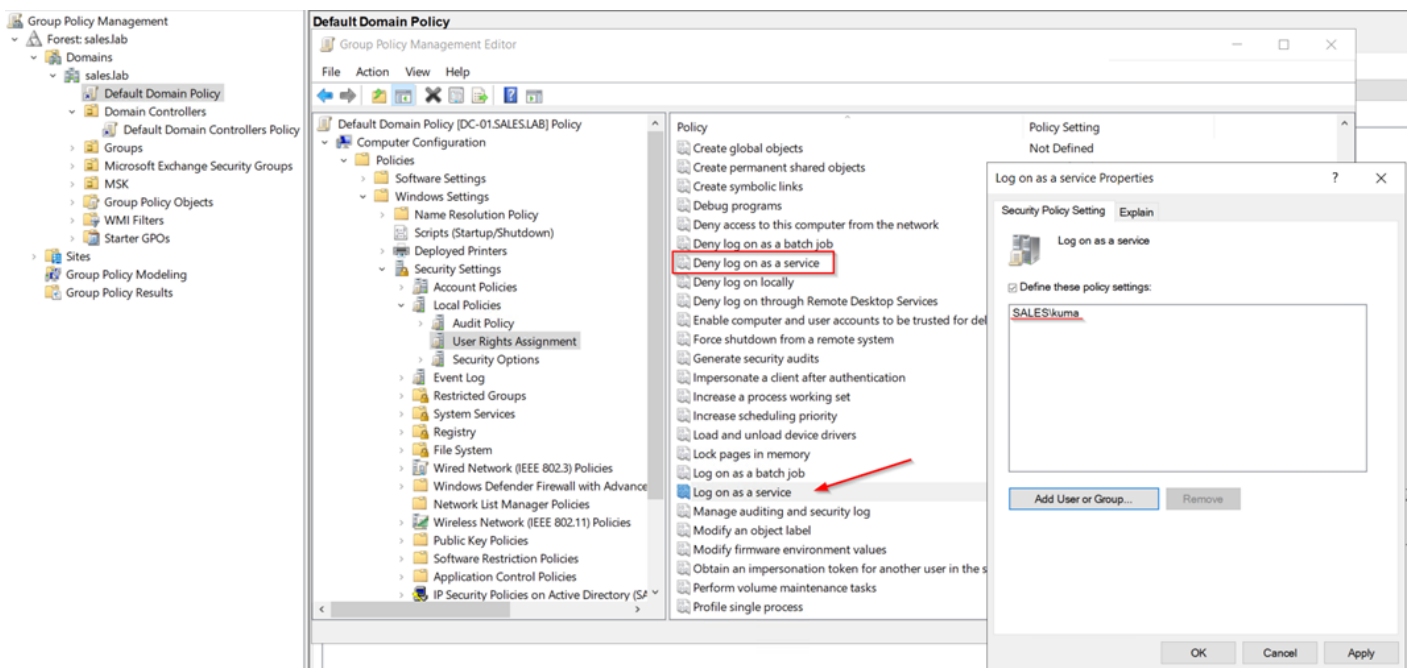
Для отдельного компьютера необходимо перейти в оснастку **Управление компьютером**, выбрать пункт **Локальные пользователи и группы**, перейти на вкладку **Группы**, выбрать группу **Event Log Readers** и добавить в нее соответствующую учетную запись пользователя или компьютера:



Приложение Б. Назначение прав входа в качестве службы

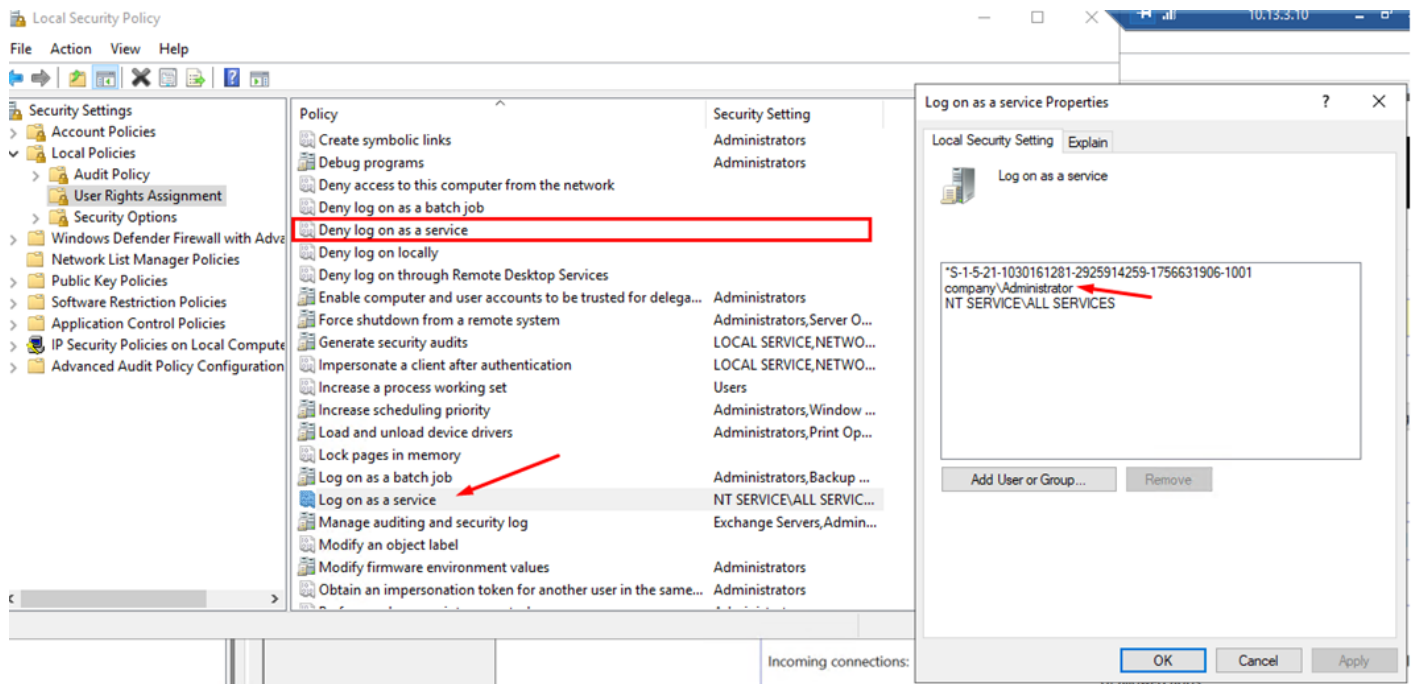
Для назначения прав входа в качестве службы для компьютеров домена необходимо открыть оснастку Group Policy Management, выбрать необходимую политику (в данном примере это Default Domain Policy) и нажать на кнопку редактирования политики.

В открывшемся окне необходимо перейти по пути **Computer Configuration - Windows Settings - Security Settings - Local Policies - User Rights Assignment** и в свойства **Log on as service** добавить соответствующую учетную запись пользователя. Дополнительно, необходимо убедиться, что соответствующая учетная запись отсутствует в свойствах **Deny log on as service**.



После сохранения настроек для их применения на целевом компьютере необходимо из командной строки, запущенной от имени администратора выполнить команду: `gpupdate /Force`

Права входа в качестве службы можно настроить локально для отдельного компьютера с помощью оснастки **Local Security Policy**. Для этого необходимо выбрать пункт **Local Policies**, перейти на вкладку **User Rights Assignment** и в свойства **Log on as service** добавить соответствующую учетную запись пользователя. Дополнительно, необходимо убедиться, что соответствующая учетная запись отсутствует в свойствах **Deny log on as service**.



Revision #20

Created 11 August 2023 12:31:59 by Boris RZR

Updated 24 January 2025 10:31:38 by Koala