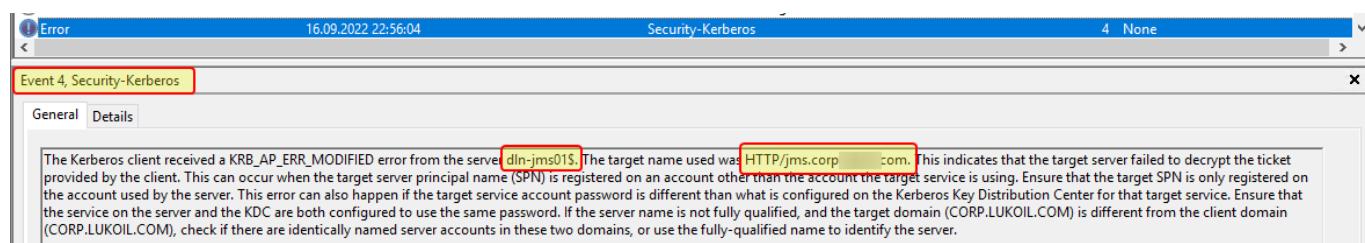


Настройка аутентификации Administration API JMS в кластерной конфигурации

Имеем кластер JMS в режиме балансировки нагрузки из двух нод, на каждой из которых установлены компоненты: JMS, JAS, JWM (Data Service+Admin Portal).

Службы JMS стартуют из под выделенной учетной записи, например corp\jms-service.

При попытке сконфигурировать компоненты JAS и JWM на подключение к кластеру JMS при попадании запроса на «свою» же ноду сталкиваемся с ошибкой аутентификации:



В логе Wireshark также видно, что получаем отлуп по Kerberos аутентификации.

19	07:12:58,432267	10.201.96.33	10.201.195.62	HTTP	199	HTTP/1.1 401 Unauthorized
20	07:12:58,433302	10.201.195.69	10.201.96.33	HTTP	199	HTTP/1.1 401 Unauthorized
21	07:12:58,433438	10.201.196.33	10.201.195.69	HTTP/X...	476	POST /EAPEngine/Default/IntegrationManager HTTP/1.1
22	07:12:58,433938	10.201.195.62	10.201.96.33	HTTP/X...	476	POST /EAPEngine/Default/IntegrationManager HTTP/1.1
23	07:12:58,453474	10.201.196.33	10.201.195.69	HTTP	385	POST /EAPEngine/Default/IntegrationManager HTTP/1.1 , NTLMSSP_NEGOTIATE
24	07:12:58,455628	10.201.195.62	10.201.96.33	HTTP	385	POST /EAPEngine/Default/IntegrationManager HTTP/1.1 , NTLMSSP_NEGOTIATE
25	07:12:58,457227	10.201.196.33	10.201.195.62	HTTP	500	HTTP/1.1 401 Unauthorized , NTLMSSP_CHALLENGE
26	07:12:58,458322	10.201.195.69	10.201.96.33	HTTP	500	HTTP/1.1 401 Unauthorized , NTLMSSP_CHALLENGE
29	07:12:58,462244	10.201.196.33	10.201.195.62	HTTP	199	HTTP/1.1 401 Unauthorized
30	07:12:58,463284	10.201.195.69	10.201.96.33	HTTP	199	HTTP/1.1 401 Unauthorized
31	07:12:58,463397	10.201.196.33	10.201.195.69	HTTP/X...	476	POST /EAPEngine/Default/IntegrationManager HTTP/1.1 , NTLMSSP_AUTH, User: corp..com\jms-service
32	07:12:58,463923	10.201.195.62	10.201.96.33	HTTP/X...	476	POST /EAPEngine/Default/IntegrationManager HTTP/1.1 , NTLMSSP_AUTH, User: corp..com\jms-service

Для исправления подобной ошибки достаточно прописать дополнительный SPN «HTTP» в служебную учетную запись:

```
setspn -A HTTP/fqdn.jms.loadbalancer corp\jms-service
```

, где fqdn.jms.loadbalancer - FQDN кластера, corp\jms-service - имя служебной УЗ.

Тюнинг аутентификации JWM (Auth и Data Service) при работе в режиме балансировки.

Аналогично, условием успеха является наличие у служебной записи SPN с префиксом HTTP/.

Дополнительно необходимо настроить аутентификацию в IIS, т.к. не получится выполнить аутентификацию по кластерному имени.

Открываем IIS Manager и для виртуальных папок Auth и Api заходим в раздел Configuration Editor.

1

2

Далее в параметре **useAppPoolCredentials** по пути
`system.webServer/security/authentication/windowsAuthentication` выставляем значение **true**.

Section: `system.webServer/security/authentication/windowsAuthentication` From: `ApplicationHost.config <location path='Default Web Site/JMS/`

authPersistNonNTLM	True
authPersistSingleRequest	False
enabled	True
extendedProtection	(Count=2)
providers	
useAppPoolCredentials	True
useKernelMode	True

Перезагружаем сервер.

From:
<https://wiki.virtlab.space/> -

Permanent link:
https://wiki.virtlab.space/russianway:jms_jas:jms_cluster_connection

Last update: **2024/12/21 19:00**

