OpenWEC

An open source Windows event collector based on the WEF protocol

William BRUNEAU & Vincent RUELLO - SSTIC 2023

1. Collect Windows events

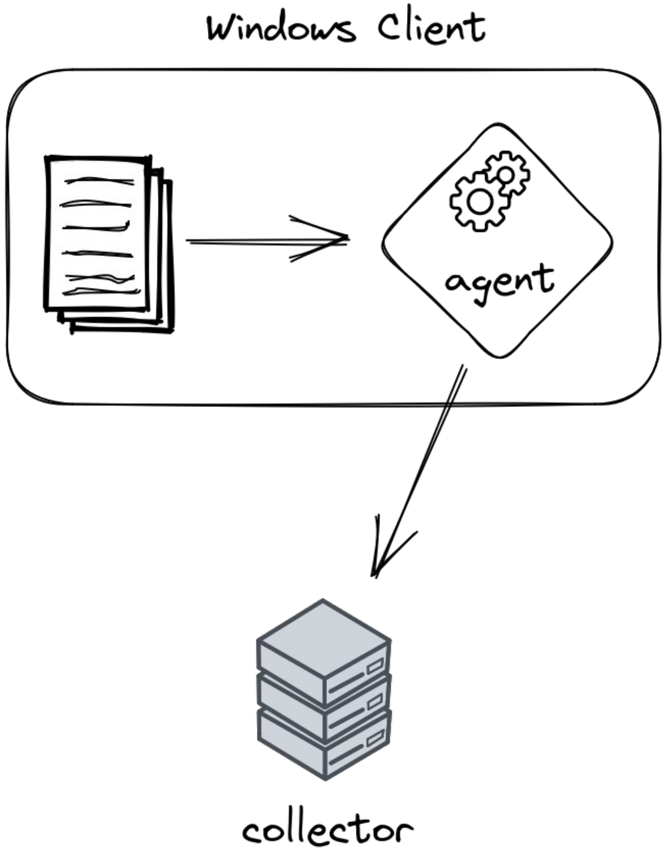
Short version

Collect Windows events

Using a third-party local agent

The agent retrieves local events and sends them using a protocol.

- Increase **attack surface**
- The agent may be privileged

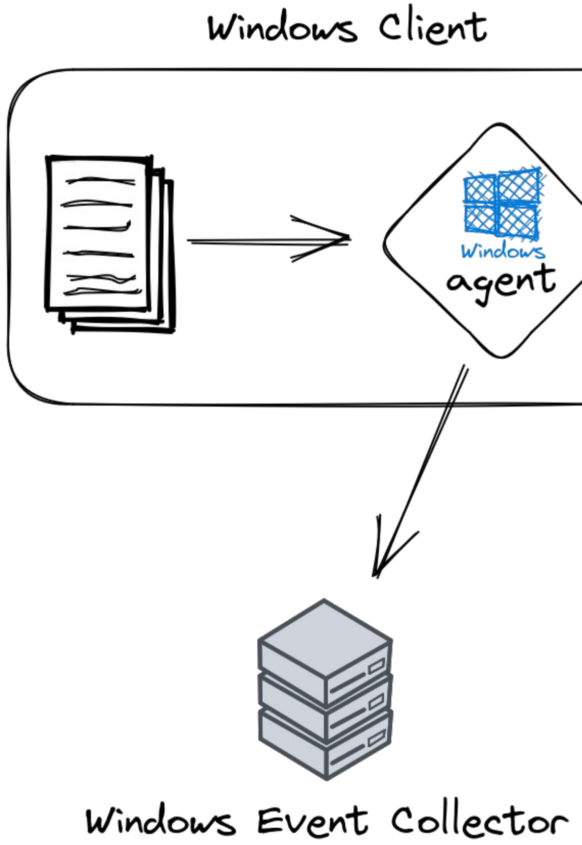


Collect Windows events

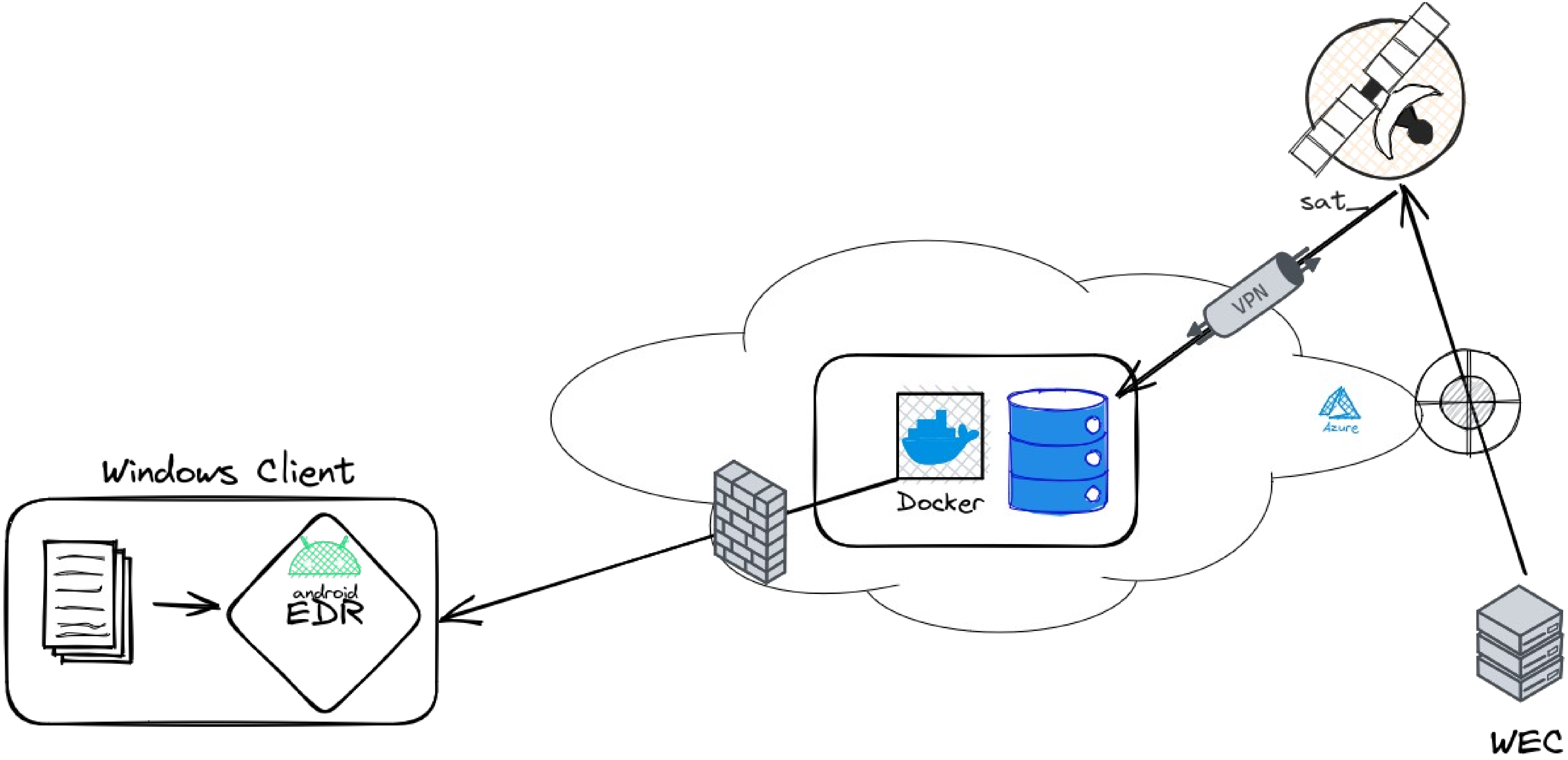
Using the built-in agent

We use the built-in Windows EventLog-Forwarder.

- **Does not increase attack surface (much)**
- **Windows Event Forwarding** protocol
- Execution with « Network Service » privileges



Collect Windows events



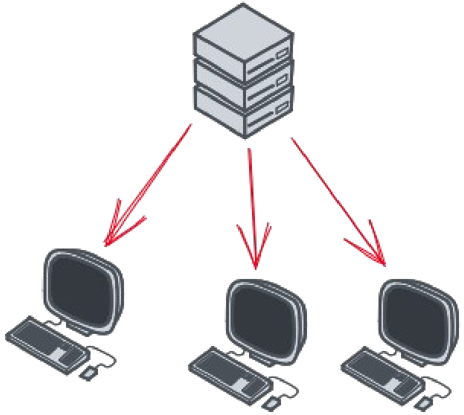
Windows Event Forwarding

- Based on Web Services for Management (*WS-Management*)
- Microsoft extension (MS-WSMV)
- HTTP/SOAP (**XML** 💔)
- **Authentication** and **encryption** (Kerberos or TLS)
- Events are **compressed** (SLDC)
- Many configurations : delivery mode, delay, …

Delivery modes

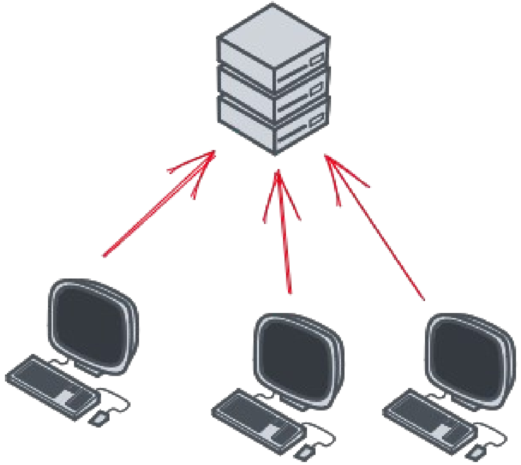
« Pull » or « Collector Initiated »

The collector connects to the clients to retrieve their events.



« Push » or « Source Initiated »

Clients connect to the collector to send their events.



WEF collector choice

Should we use the Windows Server built-in collector ?

- Windows Event Collector (WEC)

- No **redundancy**
- Some data are « missing »
  - Client IP address
  - Client identification (Kerberos principal)
- SIEM integration ?
- **Fully controlled ?**

WEF collector choice

Should we use commercial implementation running on Linux ?

- Limited features
- Some data are also missing
- Fully controlled ?

- Examples : NXLog, Cribl Edge

WEF collector choice

Should we invent the wheel again ?

- We would have **full control**
- We could **adapt it to our needs**
- We could make it available to the community
  - Even if a PoC already exists on Github: owinec

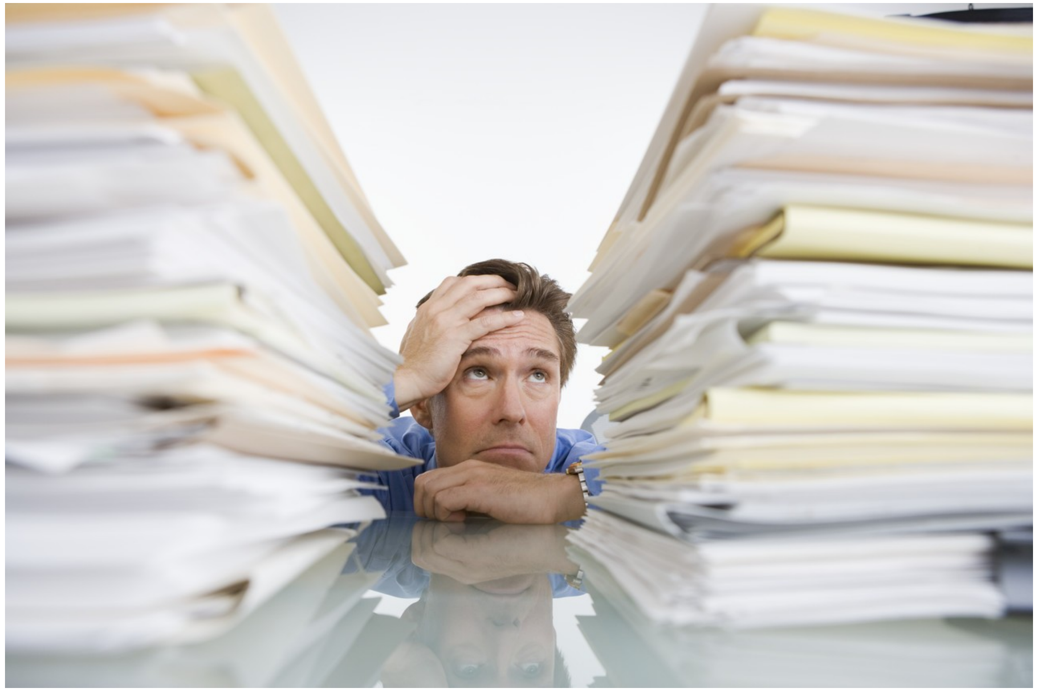
- But first, we need to understand how it works

2. Windows Event Forwarding protocol

At least, what we understood

Methodology

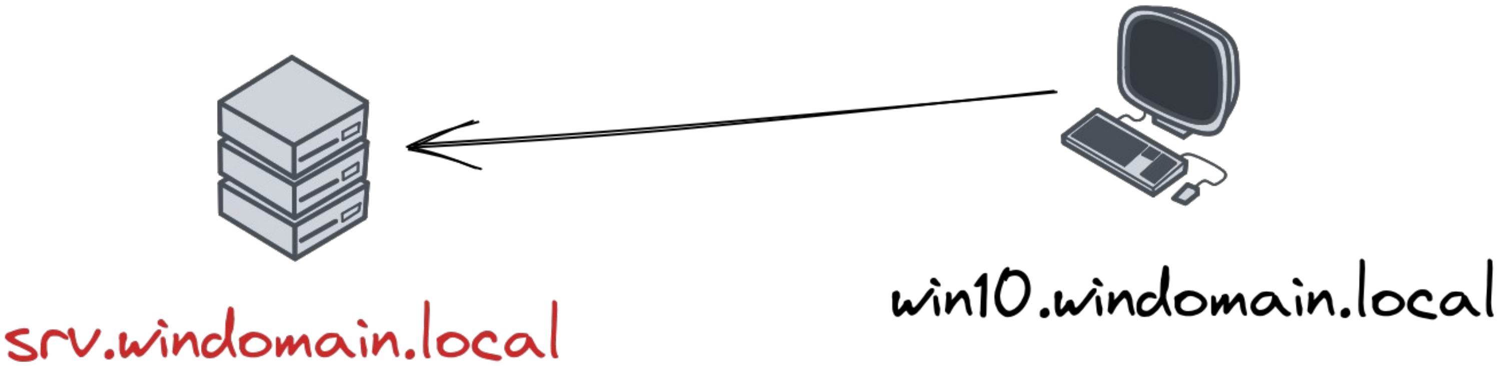
- Some **documentation**:
  - WS-Management: DSP0226_1.0.0
  - Microsoft extension: MS-WSMV
  - SLDC: ECMA-321
- **Network capture analysis**
- ~~Reverse~~



Elit lab

- Windows client configuration:

```
Server=http://srv.windomain.local:5985/wsman/SubscriptionManager/WEC,Refresh=30
```



The client authenticates to the collector

- The client authenticates to the collector using **Kerberos**:

```
POST /wsman/SubscriptionManager/WEC HTTP/1.1
Connection: Keep-Alive
Content-Type: application/soap+xml;charset=UTF-16
Authorization: Kerberos YIIH9AYJKoZIhvcSAQI...
User-Agent: Microsoft WinRM Client
Content-Length: 0
Host: srv.windomain.local:5985
```

The client sends encrypted data

- The client sends a **multipart** request containing data **encrypted** with a **Kerberos session key**.

```
    POST /wsman/SubscriptionManager/WEC HTTP/1.1
    Content-Type: multipart/encrypted;protocol="application/HTTP-Kerberos-session-encrypted";boundary="Encrypted Boundary"
    [...]

    --Encrypted Boundary
    Content-Type: application/HTTP-Kerberos-session-encrypted
    OriginalContent: type=application/soap+xml;charset=UTF-16;Length=3240
    --Encrypted Boundary
    Content-Type: application/octet-stream
    [blob de données chiffrées]
    --Encrypted Boundary--
```

Deciphering sent data

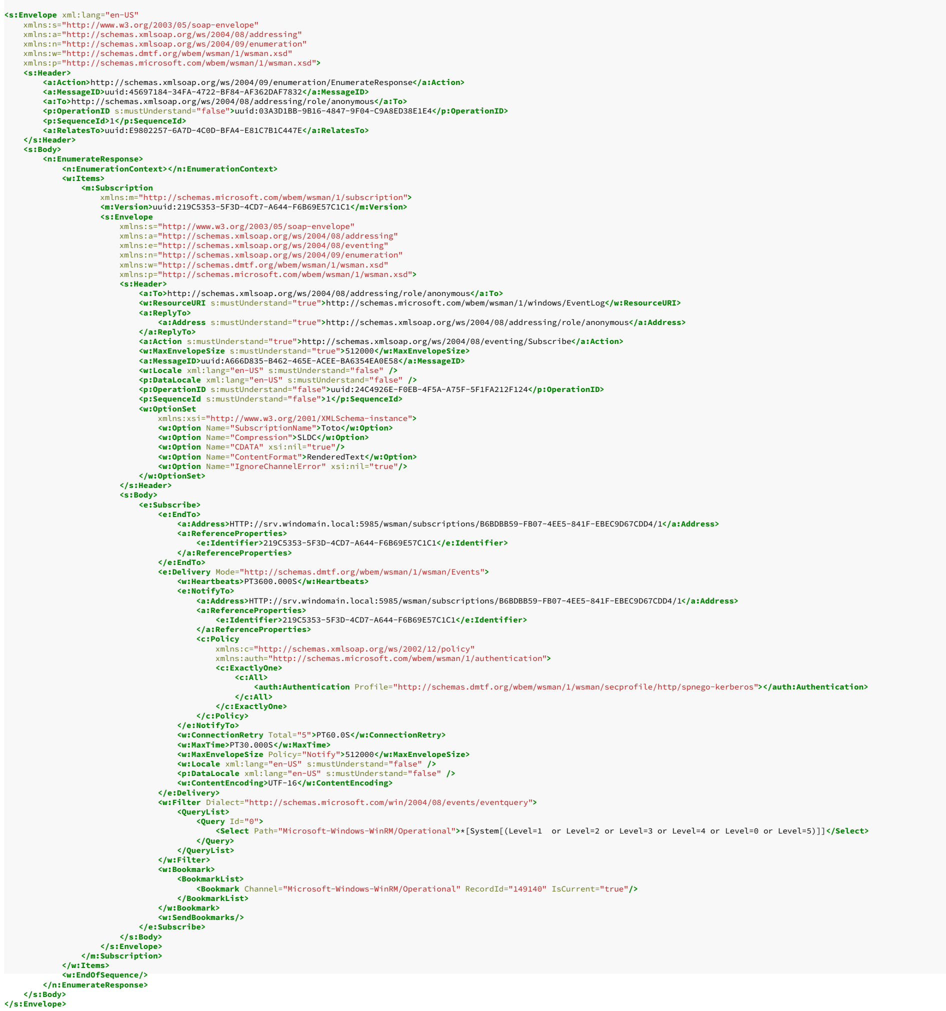
- Wireshark can:
  - Decipher encrypted parts of Kerberos tickets
  - Decipher data encrypted with a Kerberos session key
  - Just need to provide a keytab

- We generated a keytab containing srv.windomain.local secrets:
  - Retrieve keys with secretsdump.py (impacket 💚)
  - Generate a keytab using the keytab module of gmsad

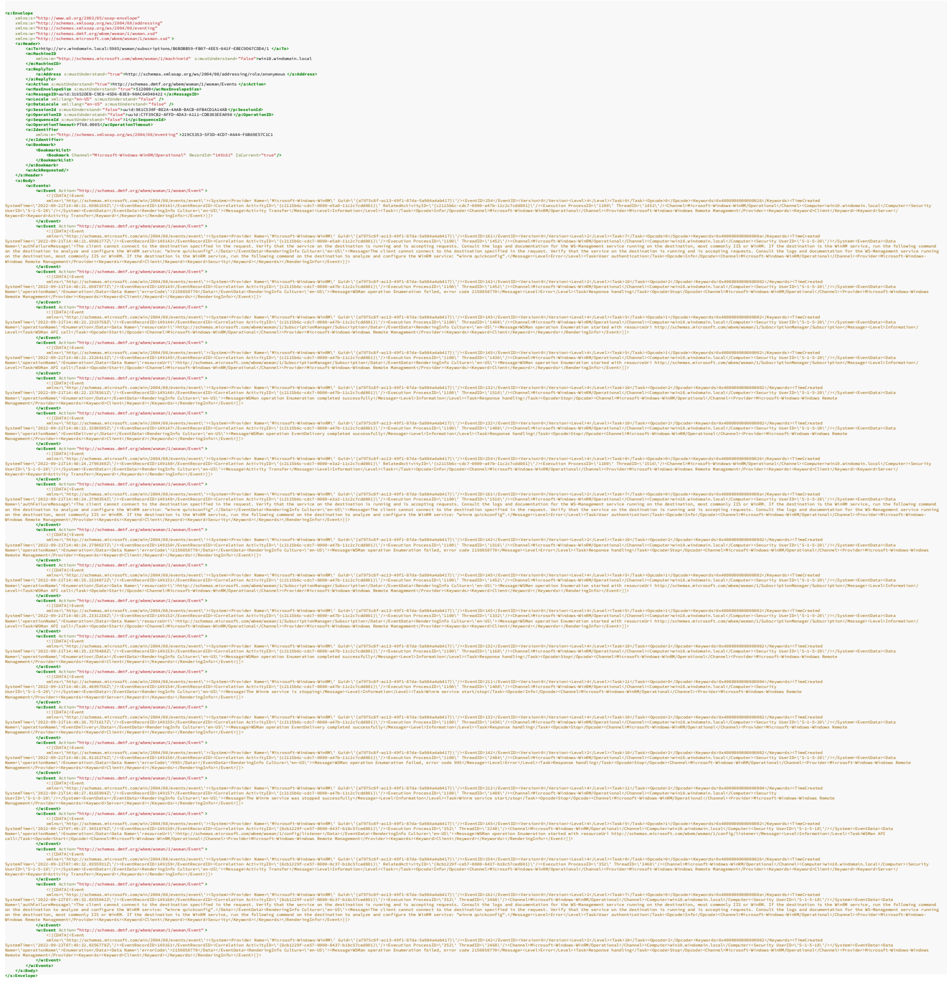
Message content

```
<s:Envelope>
    <s:Header>
        <a:To>http://srv.windomain.local:5985/wsman/SubscriptionManager/WEC</a:To>
        <m:MachineID>win10.windomain.local</m:MachineID>
        <a:Action>http://schemas.xmlsoap.org/ws/2004/09/enumeration/Enumerate</a:Action>
        [...]
    </s:Header>
    <s:Body>
        <n:Enumerate>
            <w:OptimizeEnumeration/>
            <w:MaxElements>32000</w:MaxElements>
        </n:Enumerate>
    </s:Body>
</s:Envelope>
```

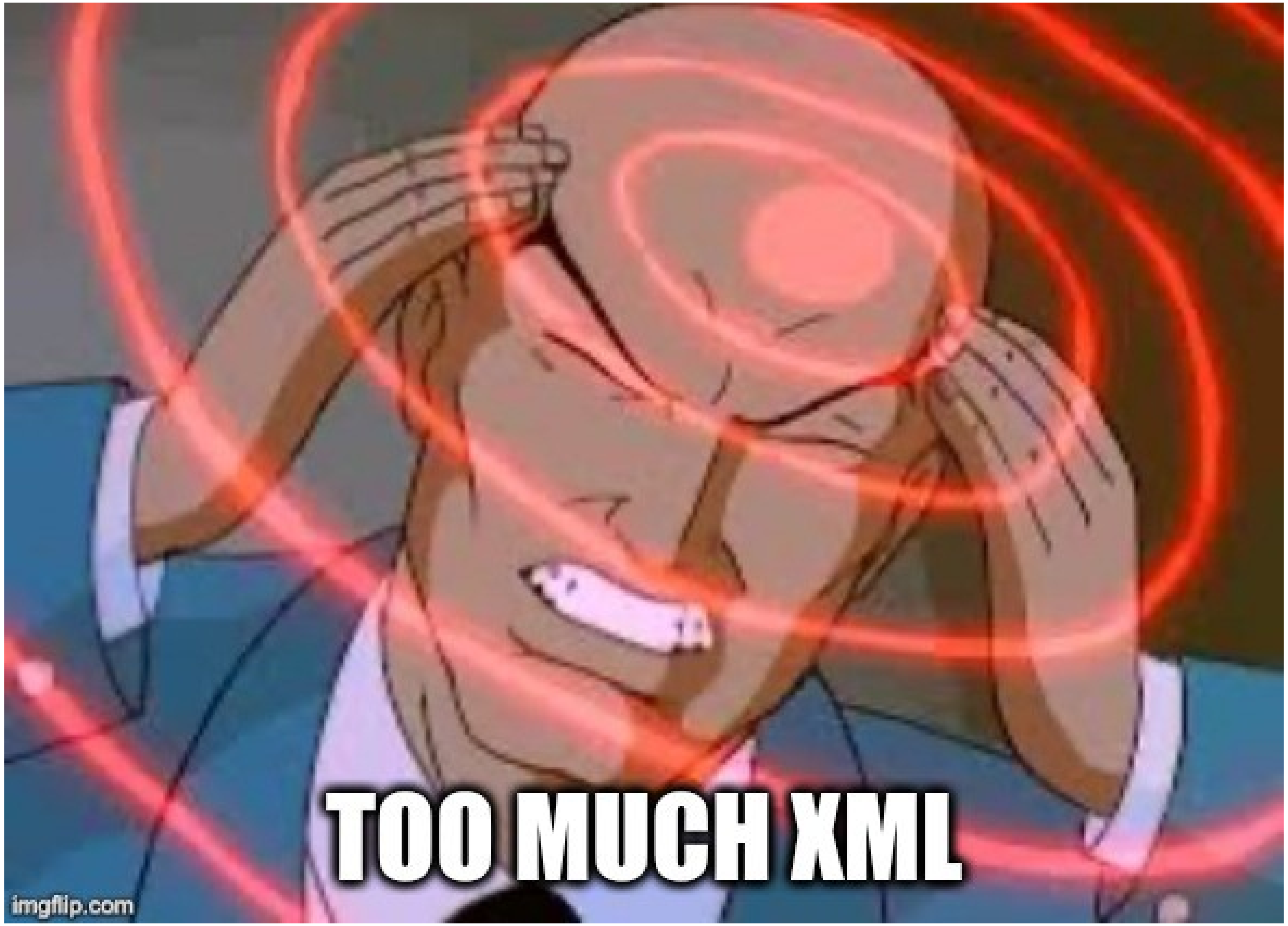
Some other message content



```xml
<s:Envelope xml:lang="en-US"
    xmlns:s="http://www.w3.org/2003/05/soap-envelope"
    xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
    xmlns:n="http://schemas.xmlsoap.org/ws/2004/09/enumeration"
    xmlns:w="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd"
    xmlns:p="http://schemas.microsoft.com/wbem/wsman/1/wsman.xsd">
    <s:Header>
        <a:Action>http://schemas.xmlsoap.org/ws/2004/09/enumeration/EnumerateResponse</a:Action>
        <a:MessageID>uuid:45697184-34FA-4722-BF84-AF362DAF7832</a:MessageID>
        <a:To>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</a:To>
        <p:OperationID s:mustUnderstand="false">uuid:03A3D1BB-9B16-4847-9F04-C9A8ED38E1E4</p:OperationID>
        <p:SequenceId>1</p:SequenceId>
        <a:RelatesTo>uuid:E9802257-6A7D-4C0D-BFA4-E81C7B1C447E</a:RelatesTo>
    </s:Header>
    <s:Body>
        <n:EnumerateResponse>
            <n:EnumerationContext></n:EnumerationContext>
            <w:Items>
                <m:Subscription
                    xmlns:m="http://schemas.microsoft.com/wbem/wsman/1/subscription">
                    <m:Version>uuid:219C5353-5F3D-4CD7-A644-F6B69E57C1C1</m:Version>
                    <s:Envelope
                        xmlns:s="http://www.w3.org/2003/05/soap-envelope"
                        xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
                        xmlns:e="http://schemas.xmlsoap.org/ws/2004/08/eventing"
                        xmlns:n="http://schemas.xmlsoap.org/ws/2004/09/enumeration"
                        xmlns:w="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd"
                        xmlns:p="http://schemas.microsoft.com/wbem/wsman/1/wsman.xsd">
                        <s:Header>
                            <a:To>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</a:To>
                            <w:ResourceURI s:mustUnderstand="true">http://schemas.microsoft.com/wbem/wsman/1/windows/EventLog</w:ResourceURI>
                            <a:ReplyTo>
                                <a:Address s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</a:Address>
                            </a:ReplyTo>
                            <a:Action s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/08/eventing/Subscribe</a:Action>
                            <w:MaxEnvelopeSize s:mustUnderstand="true">512000</w:MaxEnvelopeSize>
                            <a:MessageID>uuid:A666D835-B462-465E-ACEE-BA6354EA0E58</a:MessageID>
                            <w:Locale xml:lang="en-US" s:mustUnderstand="false" />
                            <p:DataLocale xml:lang="en-US" s:mustUnderstand="false" />
                            <p:OperationID s:mustUnderstand="false">uuid:24C4926E-F0EB-4F5A-A75F-5F1FA212F124</p:OperationID>
                            <p:SequenceId s:mustUnderstand="false">1</p:SequenceId>
                            <w:OptionSet
                                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                                <w:Option Name="SubscriptionName">Toto</w:Option>
                                <w:Option Name="Compression">SLDC</w:Option>
                                <w:Option Name="CDATA" xsi:nil="true"/>
                                <w:Option Name="ContentFormat">RenderedText</w:Option>
                                <w:Option Name="IgnoreChannelError" xsi:nil="true"/>
                            </w:OptionSet>
                        </s:Header>
                        <s:Body>
                            <e:Subscribe>
                                <e:EndTo>
                                    <a:Address>HTTP://srv.windomain.local:5985/wsman/subscriptions/B6BDBB59-FB07-4EE5-841F-EBEC9D67CDD4/1</a:Address>
                                    <a:ReferenceProperties>
                                        <e:Identifier>219C5353-5F3D-4CD7-A644-F6B69E57C1C1</e:Identifier>
                                    </a:ReferenceProperties>
                                </e:EndTo>
                                <e:Delivery Mode="http://schemas.dmtf.org/wbem/wsman/1/wsman/Events">
                                    <w:Heartbeats>PT3600.000S</w:Heartbeats>
                                    <e:NotifyTo>
                                        <a:Address>HTTP://srv.windomain.local:5985/wsman/subscriptions/B6BDBB59-FB07-4EE5-841F-EBEC9D67CDD4/1</a:Address>
                                        <a:ReferenceProperties>
                                            <e:Identifier>219C5353-5F3D-4CD7-A644-F6B69E57C1C1</e:Identifier>
                                        </a:ReferenceProperties>
                                        <c:Policy
                                            xmlns:c="http://schemas.xmlsoap.org/ws/2002/12/policy"
                                            xmlns:auth="http://schemas.microsoft.com/wbem/wsman/1/authentication">
                                            <c:ExactlyOne>
                                                <c:All>
                                                    <auth:Authentication Profile="http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/spnego-kerberos"></auth:Authentication>
                                                </c:All>
                                            </c:ExactlyOne>
                                        </c:Policy>
                                    </e:NotifyTo>
                                    <w:ConnectionRetry Total="5">PT60.0S</w:ConnectionRetry>
                                    <w:MaxTime>PT30.000S</w:MaxTime>
                                    <w:MaxEnvelopeSize Policy="Notify">512000</w:MaxEnvelopeSize>
                                    <w:Locale xml:lang="en-US" s:mustUnderstand="false" />
                                    <p:DataLocale xml:lang="en-US" s:mustUnderstand="false" />
                                    <w:ContentEncoding>UTF-16</w:ContentEncoding>
                                </e:Delivery>
                                <w:Filter Dialect="http://schemas.microsoft.com/win/2004/08/events/eventquery">
                                    <QueryList>
                                        <Query Id="0">
                                            <Select Path="Microsoft-Windows-WinRM/Operational">*[System[(Level=1  or Level=2 or Level=3 or Level=4 or Level=0 or Level=5)]]</Select>
                                        </Query>
                                    </QueryList>
                                </w:Filter>
                                <w:Bookmark>
                                    <BookmarkList>
                                        <Bookmark Channel="Microsoft-Windows-WinRM/Operational" RecordId="149140" IsCurrent="true"/>
                                    </BookmarkList>
                                </w:Bookmark>
                                <w:SendBookmarks/>
                            </e:Subscribe>
                        </s:Body>
                    </s:Envelope>
                </m:Subscription>
            </w:Items>
            <w:EndOfSequence/>
        </n:EnumerateResponse>
    </s:Body>
</s:Envelope>
```



```xml
<s:Envelope
    xmlns:s="http://www.w3.org/2003/05/soap-envelope"
    xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
    xmlns:e="http://schemas.xmlsoap.org/ws/2004/08/eventing"
    xmlns:w="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd"
    xmlns:p="http://schemas.microsoft.com/wbem/wsman/1/wsman.xsd" >
    <s:Header>
        <a:To>http://srv.windomain.local:5985/wsman/subscriptions/B6BDBB59-FB07-4EE5-841F-EBEC9D67CDD4/1 </a:To>
        <m:MachineID
            xmlns:m="http://schemas.microsoft.com/wbem/wsman/1/machineid"  s:mustUnderstand="false">win10.windomain.local
        </m:MachineID>
        <a:ReplyTo>
            <a:Address s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous </a:Address>
        </a:ReplyTo>
        <a:Action s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wsman/1/wsman/Events </a:Action>
        <w:MaxEnvelopeSize s:mustUnderstand="true">512000</w:MaxEnvelopeSize>
        <a:MessageID>uuid:31652DEB-C9E8-45D6-B3E8-90AC64D48422 </a:MessageID>
        <w:Locale xml:lang="en-US" s:mustUnderstand="false" />
        <p:DataLocale xml:lang="en-US" s:mustUnderstand="false" />
        <p:SessionId s:mustUnderstand="false">uuid:981C530F-BE2A-4AAB-BACB-6FB4CD1A14AB </p:SessionId>
        <p:OperationID s:mustUnderstand="false">uuid:C7F39CB2-8FFD-4DA3-A111-CDB303EEA098 </p:OperationID>
        <p:SequenceId s:mustUnderstand="false">1</p:SequenceId>
        <w:OperationTimeout>PT60.000S</w:OperationTimeout>
        <e:Identifier
            xmlns:e="http://schemas.xmlsoap.org/ws/2004/08/eventing" >219C5353-5F3D-4CD7-A644-F6B69E57C1C1
        </e:Identifier>
        <w:Bookmark>
            <BookmarkList>
                <Bookmark Channel="Microsoft-Windows-WinRM/Operational"  RecordId="149161"  IsCurrent="true"/>
            </BookmarkList>
        </w:Bookmark>
        <w:AckRequested/>
    </s:Header>
    <s:Body>
        <w:Events>
            [illegible]
        </w:Events>
    </s:Body>
</s:Envelope>
```


TOO MUCH XML
imgflip.com

Subscription

Event collection configuration:

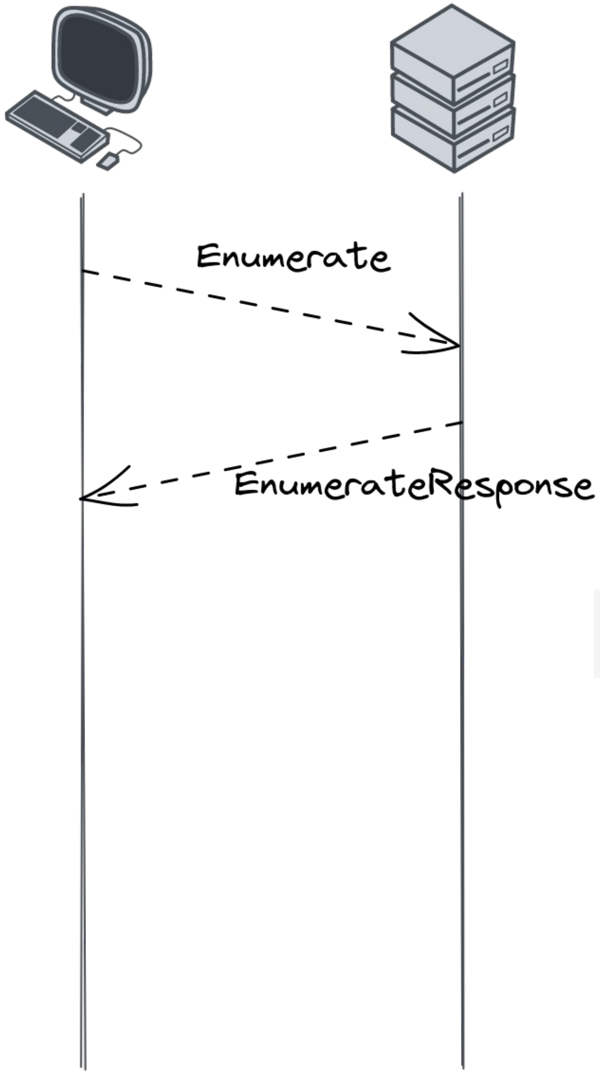
- Name
- Event query
- Delivery mode
- Version

Bookmark

- A **pointer** in the client event stream
- **Sent by the client** with every event batch
- The collector **stores** the last bookmark sent by each client for each subscription
- The collector can tell to the client where we are at in its event stream

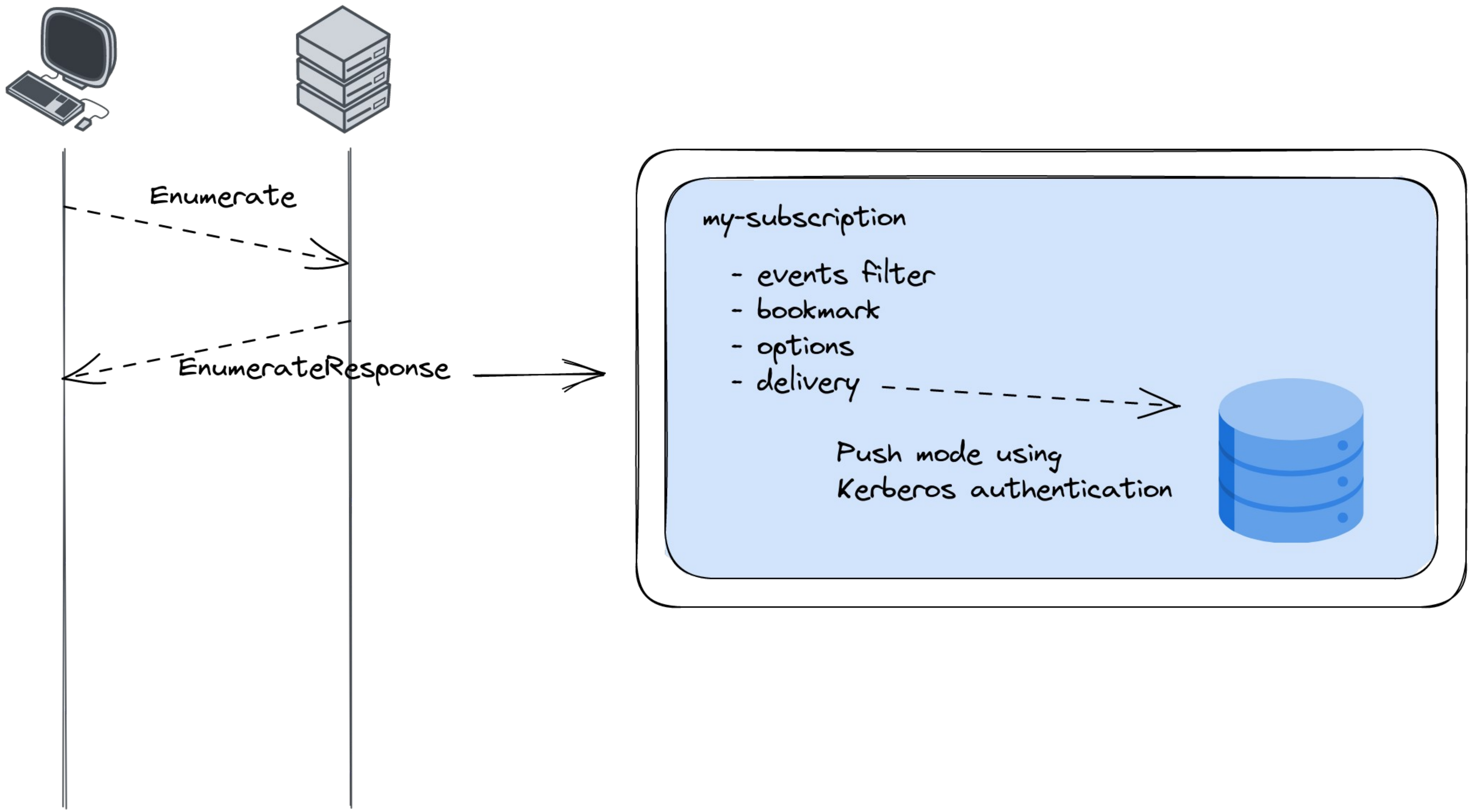
```
<BookmarkList>
    <Bookmark Channel="Microsoft-Windows-WinRM/Operational" RecordId="149161"
IsCurrent="true"/>
</BookmarkList>
```

Protocol

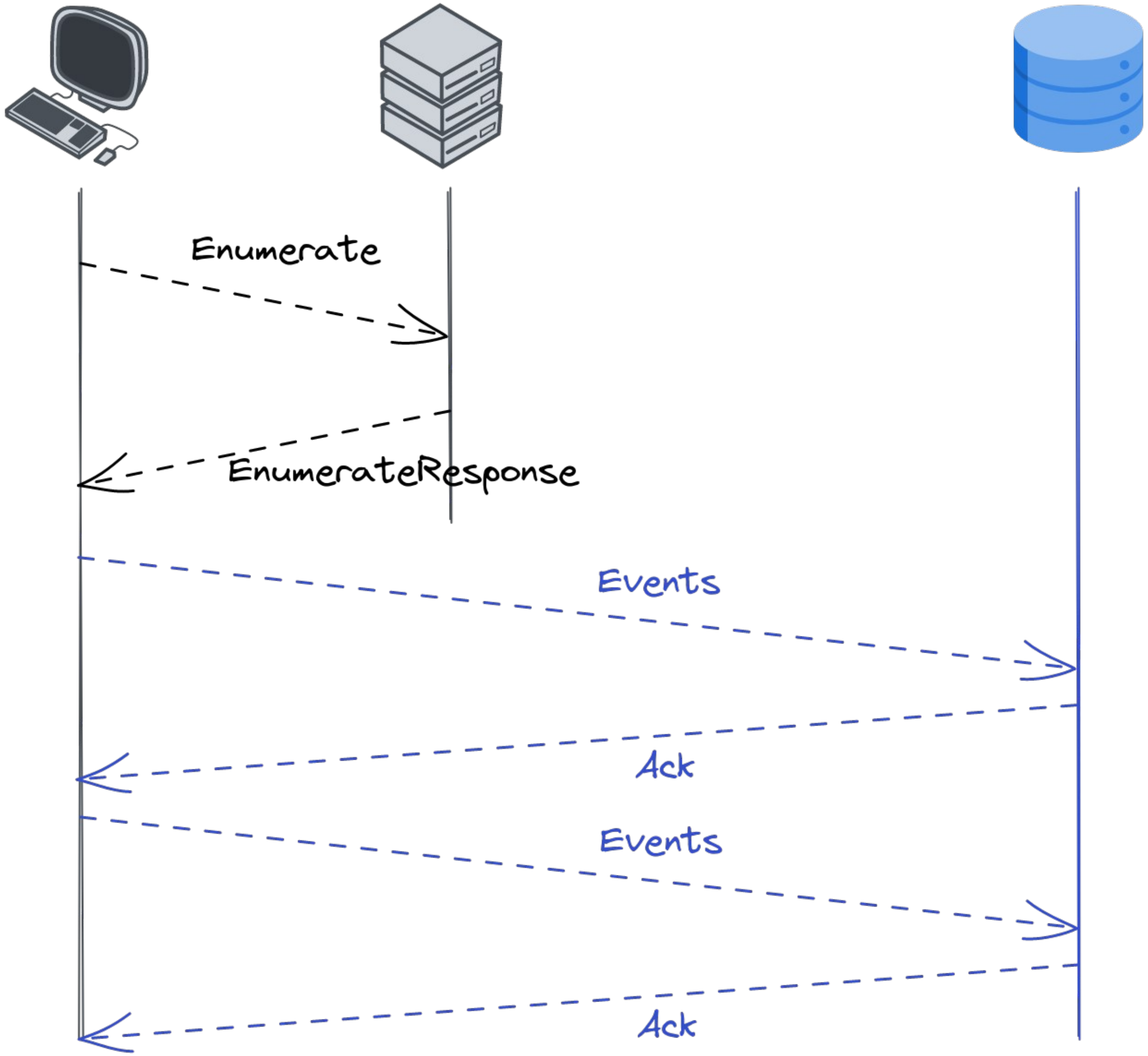


```
Server=http://srv.windomain.local:5985/...,Refresh=30
```

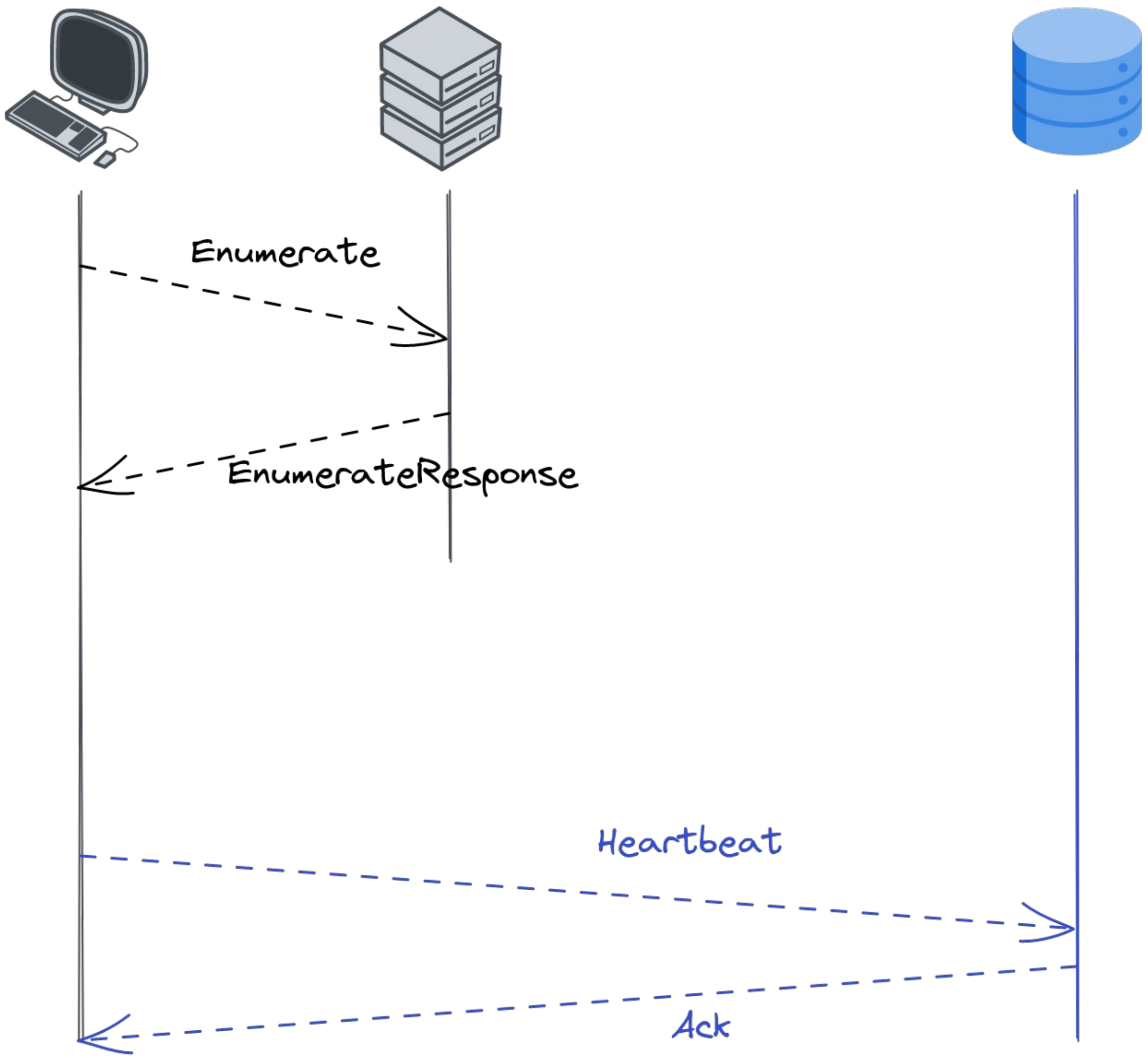
Protocol


Enumerate
EnumerateResponse
my-subscription
- events filter
- bookmark
- options
- delivery
Push mode using
Kerberos authentication

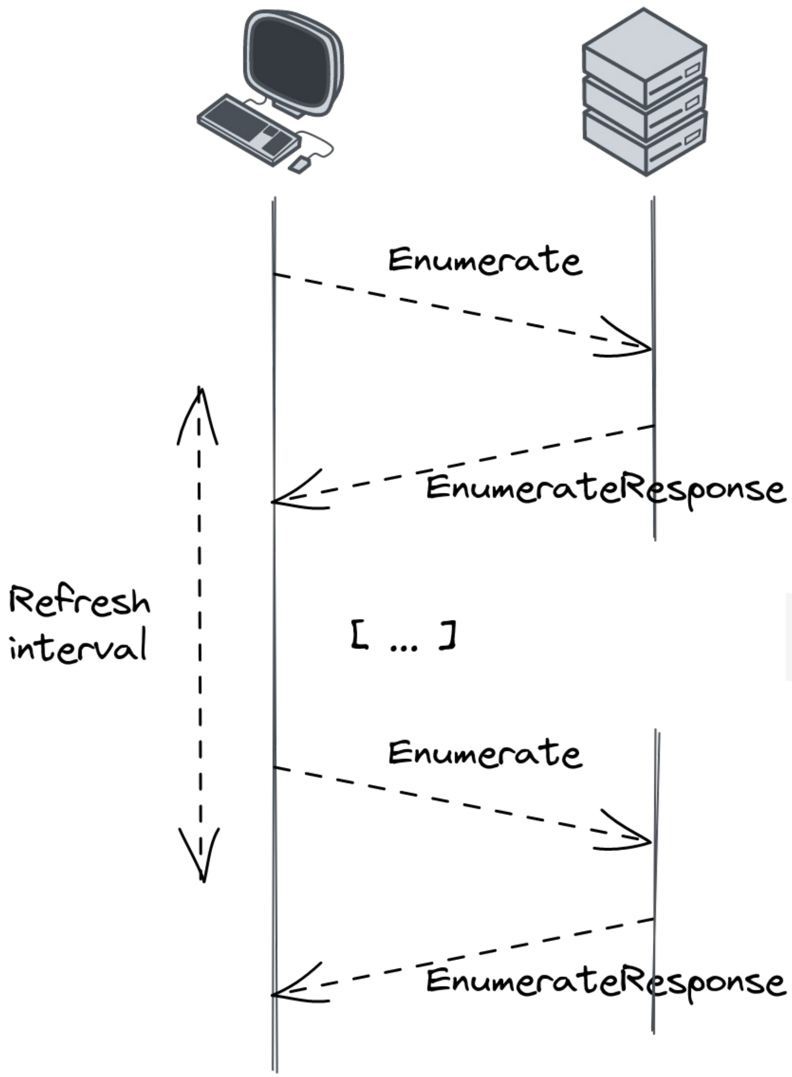
Protocol



Protocol

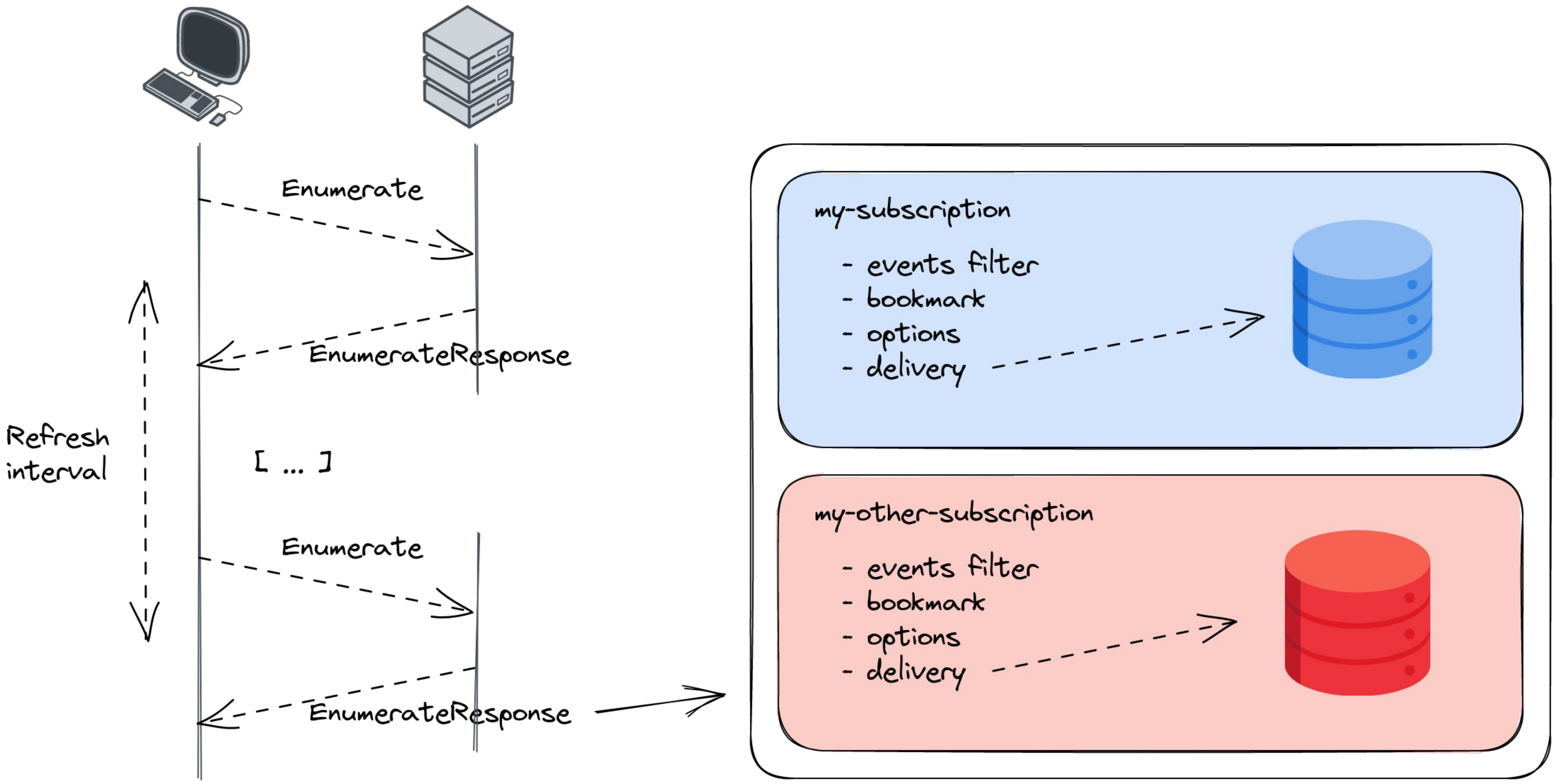


Protocol

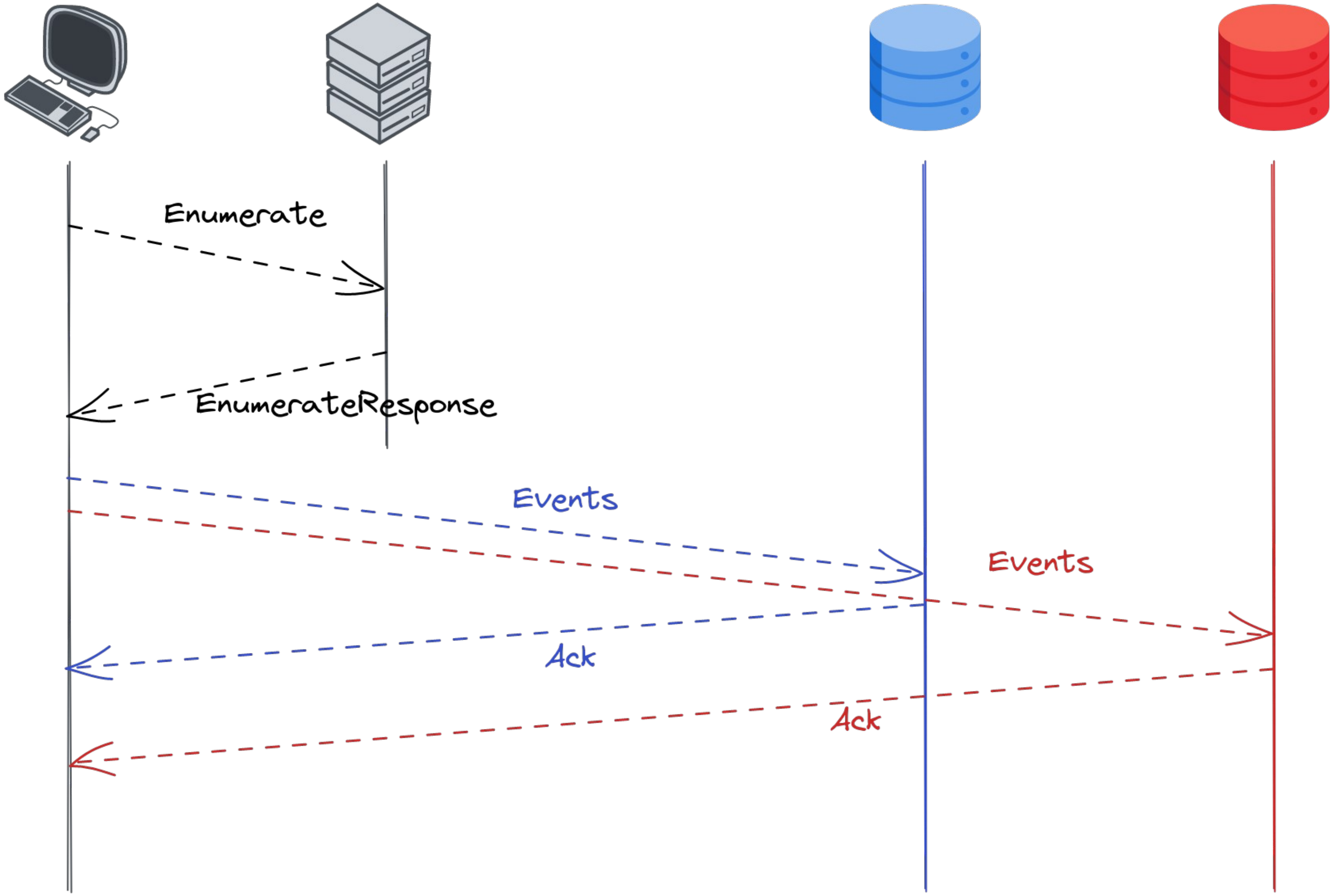


```
Server=http://srv.windomain.local:5985/...,Refresh=30
```

Protocol


Enumerate
EnumerateResponse
Refresh interval
[...]
Enumerate
EnumerateResponse
my-subscription
- events filter
- bookmark
- options
- delivery
my-other-subscription
- events filter
- bookmark
- options
- delivery

Protocol



3. Seems doable, let’s go !

OpenWEC

First try

- 2021:
  - PoC in Python
  - Only TLS support
  - Thanks Romain ❤️

- 2022: a new start !

Our requirements

- WEF implementation:
  - Only « **Push** » delivery mode
  - Only **Kerberos** support (for authentication and encryption)
  - **Compression** support
- In **Rust**
- For **Linux**
- Multiple output options (file, Kafka, …)
- Redundancy and load balancing

OpenWEC

https://github.com/cea-sec/openwec

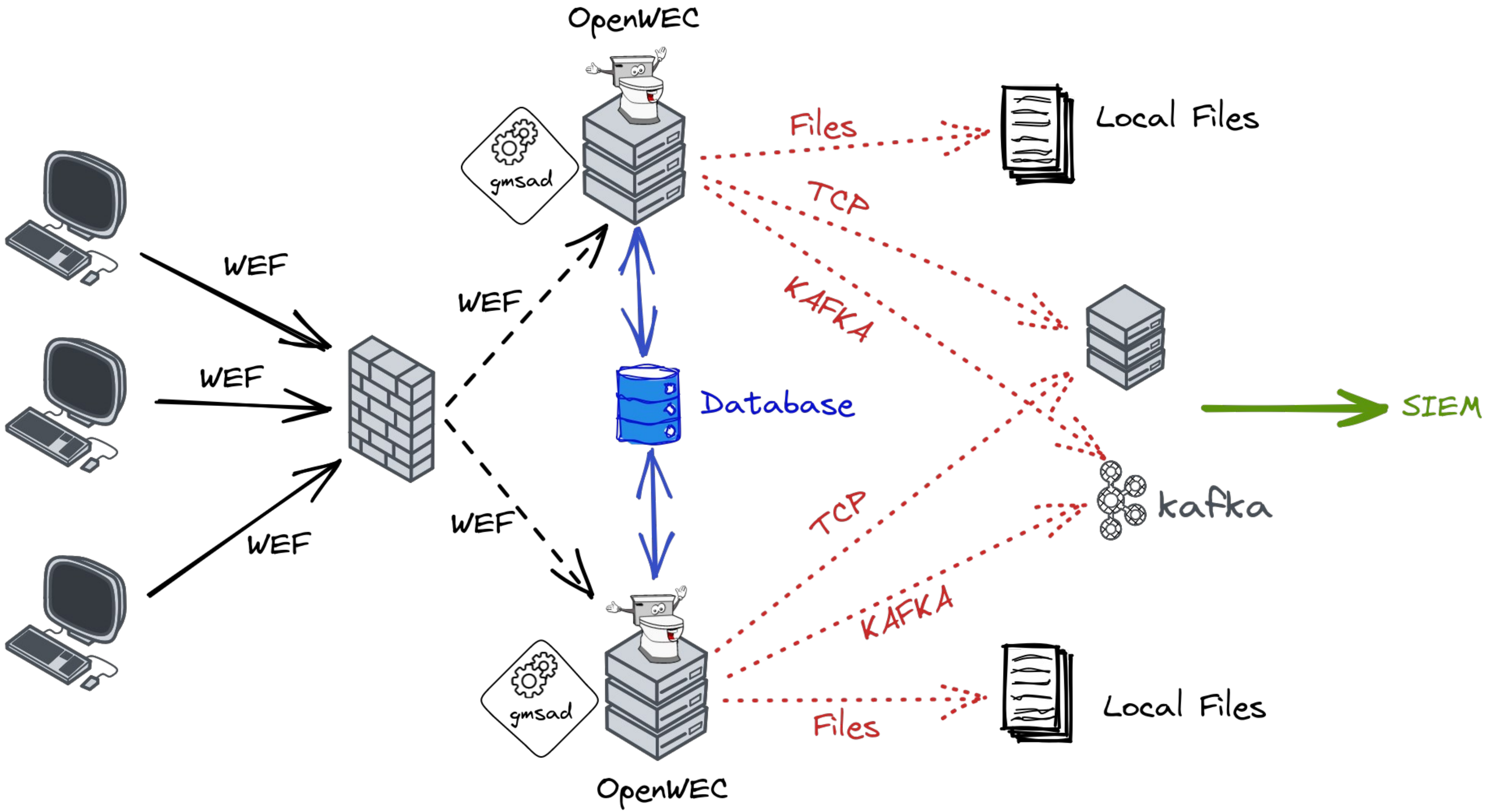
OpenWEC

- Subscriptions and their metadata (bookmarks, …) are stored in a database:
  - SQLite
    - Single node
    - Does not enable redundancy/load balancing
  - Postgres
    - Designed for CockroachDB
    - Multiple nodes

OpenWEC

- Each subscription can specify how events are output
- OpenWEC outputs have a format:
  - Raw (XML)
  - Json
- 3 output types exist for now:
  - Files
  - TCP
  - Kafka

Architecture



Feedback

- Deployed for a few thousands of computers
- WEF deployment issues (not specific to OpenWEC)
  - Event queries: limited number of sources, volume for each source
  - Permissions on sources

  - Useful resouces: ANSSI guide (in french) « Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory »

TODO

- Add **TLS support**
- Linux distribution integration (packaging)
- Implement other **outputs** (types and formats)

https://github.com/cea-sec/openwec

William BRUNEAU & Vincent RUELLO - SSTIC 2023

CEA DAM

Centre de Bruyères-le-Châtel

91297 Arpajon Cedex

Établissement public à caractère
industriel et commercial