Winning on Windows with a WiNC and a smile

Vianney Boncorps
Nanjoo Ban
Forward-looking statements

This is a rolling (up to three year) Roadmap and is subject to change without notice.

This document contains forward looking statements regarding future operations, product development, product capabilities and availability dates. This information is subject to substantial uncertainties and is subject to change at any time without prior notification. Statements contained in this document concerning these matters only reflect Hewlett Packard's predictions and / or expectations as of the date of this document and actual results and future plans of Hewlett-Packard may differ significantly as a result of, among other things, changes in product strategy resulting from technological, internal corporate, market and other changes. This is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions.
HP confidential information

This is a rolling (up to three year) Roadmap and is subject to change without notice.

This Roadmap contains HP Confidential Information.

If you have a valid Confidential Disclosure Agreement with HP, disclosure of the Roadmap is subject to that CDA. If not, it is subject to the following terms: for a period of 3 years after the date of disclosure, you may use the Roadmap solely for the purpose of evaluating purchase decisions from HP and use a reasonable standard of care to prevent disclosures. You will not disclose the contents of the Roadmap to any third party unless it becomes publically known, rightfully received by you from a third party without duty of confidentiality, or disclosed with HP’s prior written approval.
Agenda

• Overview
• Introducing...
• Is it a good fit?
• Summary
• Q & A
Windows event log 101

Concepts and terms used in this presentation

- Administrative VS Operational logs
- Custom application logs
- Windows Event Forwarding (WEF)
- Windows Event Collector (WEC)
- WUC, WDC, WLC
Yet another Windows Connector?

WDC, WLC, WUC...

- New eventlog format in Windows Vista+
- Limitations in supporting new features
  - Non-administrative logs
  - Custom application logs
  - Event filtering
  - WEF support but in a limited way
- No IPv6 support
Introducing...

SmartConnector for Microsoft Windows Event Log – Native (beta)
Microsoft Windows Event Log – Native Connector (beta)

- Separation of responsibilities
  - Listener subscribes to the events from the hosts and sends them to the connector
  - Connector processes the events through its parsers
- Push model using subscriptions
- Leverages Windows APIs with extended feature set
- New set of parsers as well as flex parser support
- Easier configuration
Similarities with WUC

• Host discovery
• Host table configuration
• Out of the box collection and parsing support – Security, System
• Same level of flex parser supported
• Ability to populate Windows version (for WEF, optional)
Architecture overview

Connector and Listener are installed together on the same Host

1. Receive events
2. Aggregate into batch
3. Send batch
4. Process the events

SmartConnector

Connector Java
Listener C#
System requirements

- Platform requirements for Connector installation
  - **Windows** 2008, 2012
  - .NET 4.5+

- Supported versions for event collection
  - Windows Vista, 2008, 2008 R2, 2012, 7 and 8
Is the Windows Native Connector a good fit?
Use case 1

The quick demo

• Collect application, security and system logs from localhost
• For an immediate demonstration of the Windows Native Connector
Use case 1 – cont’d

WUC – many configuration panels

- Configure the localhost on the third panel
- Many configuration parameters in the first panel
- Lots of head scratching
Use case 1 – cont’d

WiNC – one click configuration

One panel
Default selection – done!
Use case 2

The collector

• Events are forwarded to Forwarded Events log in localhost
• Collect Forwarded Security and System Events
Use case 2 – cont’d

WUC – limited support

• Check “WEF Enabled”
• Many panels
• Can use only administrative logs → not Forwarded Events
• Channel and OS Version are not in the event
  • Need source host file or AD to find host information
  • Custom event source mappings may be needed to allow parsing
Use case 2 – cont’d

WiNC – another one panel configuration

- Still one panel
- Select the logs – done!
- Windows version?
  - Not required!
  - Check ‘This is a WEC Server’
  - Upload source hosts file, or use AD
Use case 3

The special agenda

• Large volume of events overall
• Only interested in logon failures
  • From the last hour
  • Logon failures (event id 4625)
  • NPS provider
  • Event level: Critical + Error
Use case 3 – cont’d

WUC – not easy

• No filtering at collection
• Filter the events after processing (ESM)
• Waste of resources!
Use case 3 – cont’d

WiNC – event query
Use case 3 – cont’d

WiNC – what to enter in the filter
Use case 4

The large enterprise

• Large number of hosts
• Geographically dispersed
• Latency is one of the main bottlenecks
• IPv6 or hybrid environment
Use case 4 – cont’d

- No IPv6 support
- Round robin collection
  - Still goes to the host even if there are no events
  - Response comes back with padded data
  - Bandwidth wasted
- Have to choose a good Event Poll Count value
- Manual fine tuning may prevent time drift
Use case 4 – cont’d

WiNC – smile

• IPv6 supported implicitly
• Event subscription – push model
  • Listener will be notified for new events, hence more scalable
  • No fixed buffer ➞ no padding
• More efficient with resources!
Use case 5

The IT nightmare

• Unstable or slow connection to some of the hosts
• Disparity in the event volume among the hosts
• Some very big application events (2MB)
Use case 5 – cont’d

WUC – ouch!

• Round robin
  • Holding up all the other hosts if one times out
  • Endpoints with low throughput send as much data
• Big event does not fit into the buffer
• Troublesome!
Use case 5 – cont’d

WiNC – woohoo!

• Endpoints do not interfere with each other
• No tuning necessary at the host level
• Big events can be handled with no extra adjustment
• More stable!
Use case 6

The Flex Expert (Flexpert?)

• Collect events from non-administrative logs
• Create Flex Connector parsers for custom application logs
• Special event formats
Use case 6 – cont’d

WUC – yes, but...

- Supports collection from administrative logs only
- Supports parsing for some custom application logs
- Forwarded events can have a problematic format
  - XML parser extra-processor might be needed
  - Special values will shift the whole list
Use case 6 – cont’d

WiNC – so cool!

- Supports operational logs as well as administrative logs
- New flex framework for custom parsers
- All the events, all the time!
  - As long as Event Viewer can show the XML
  - Special sections can be handled by JSON parsers
Use case 6 – cont’d

WiNC – so cool!

Log Properties - Operational (Type: Operational)

- Full Name: Microsoft-Windows-PrintService/Operational
- Log path: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-PrintService%4Operation
- Log size: 1.07 MB (1,118,208 bytes)
- Created: Monday, September 23, 2013 10:01:40 AM
- Modified: Wednesday, August 20, 2014 9:01:01 AM
- Accessed: Monday, September 23, 2013 10:01:40 AM

Enable logging
- Maximum log size (KB): 32640
- When maximum event log size is reached:
  - Overwrite events as needed (oldest events first)
  - Archive the log when full, do not overwrite events
  - Do not overwrite events (Clear logs manually)

Clear Log
Use case 6 – cont’d

WiNC – so cool!
Raw event transformation

From XML to JSON

```xml
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-DNS-Client" Guid="{1C95126E-7EEA-49A9-A3FE-A378B03DDB4D}" />
    <EventID>1014</EventID>
    <Version>0</Version>
    <Level>3</Level>
    <Task>0</Task>
    <Opcode>0</Opcode>
    <Keywords>0x4000000000000000</Keywords>
    <TimeCreated SystemTime="2014-07-21T14:13:35.821782300Z" />
    <EventRecordID>40318</EventRecordID>
    <Computer>svsvm0032.conperf.com</Computer>
    <Security UserID="S-1-5-20" />
  </System>
  <EventData>
    <Data Name="QueryName">204.15.in-addr.arpa</Data>
    <Data>28</Data>
    <Data Name="Address">170003500000002002104D001F</Data>
  </EventData>
</Event>
```

```json
{
  "System": {
    "EventId": "1014",
    "Version": "0",
    "Channel": "System",
    "ProviderName": "Microsoft-Windows-DNS-Client",
    "ProviderId": "1c95126e-7eea-49a9-a3fe-a378b03d004d",
    "Computer": "svsvm0032.conperf.com",
    "EventRecordId": "40318",
    "Keywords": "0x4000000000000000",
    "Level": "Information",
    "Opcode": "0",
    "ProcessId": "1052",
    "ThreadId": "1660",
    "Task": "0",
    "RelatedActivityId": "",
    "Qualifiers": "",
    "TimeCreated": "2014-07-21T14:13:35.821782300Z",
    "UserId": "NT AUTHORITY\NETWORK SERVICE"
  },
  "EventData": {
    "QueryName": "204.15.in-addr.arpa",
    "%2": "16",
    "Address": "1700003500000002002104D001F"
  }
}
```
Parsing the JSON event

```
{
  "System": {
    "EventId": "1014",
    "Version": "0",
    "Channel": "System",
    "ProviderName": "Microsoft-Windows-DNS-Client",
    "ProviderID": "1c95126e-7eea-49a9-a3fe-a378b03ddb4d",
    "Computer": "win7-PC.windc12a.winevt.com",
    "TimeCreated": "2014-07-21T14:13:35.821782300Z",
    "UserId": "NT AUTHORITY\NETWORK SERVICE"
  },
  "EventData": {
    "QueryName": "204.15.in-addr.arpa",
    "AddressLength": "16",
    "Address": "17000035000000002002104D001F"
  },
  "UserData": {
    "updatelist": {
      "@_xmlns_": "http://manifests.microsoft.com/windows/eventlog",
      "#text": "- Microsoft.BingTravel"
    }
  }
}
```

- **System**
  - Header of all Windows events is parsed by a common parser
    - \winc\main\eventheader.sdkkeyvalueparser.properties

- **EventData**
  - Event body present in EventData section is parsed by
    - \winc\<Channel>\<ProviderName>.sdkkeyvalueparser.properties

- **UserData**
  - Event body present in other sections is parsed by
    - \winc\<Channel>\<ProviderName>.<Section>.jsonparserr.properties
Windows Native Connector does it better

- One step closer to the Windows eventing protocol
- Supports collection from all event log types
- Supports advanced features such as filtering
- More efficient event collection
- Easier to configure and use
## WiNC vs. WUC feature comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>WUC</th>
<th>WiNC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Systems Supported</td>
<td>Windows</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>✓</td>
</tr>
<tr>
<td>Event Log Types</td>
<td>Security</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>System</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Administrative logs</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Non-administrative logs</td>
<td>✓</td>
</tr>
<tr>
<td>Other Features</td>
<td>IPv6</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Filtering at the source</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>WEF support</td>
<td>✓</td>
</tr>
</tbody>
</table>
Please give me your feedback

Session TT3120  Speakers Vianney Boncorps & Nanjoo Ban

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.
For more information

Attend these sessions

• TT3119, Resting your mind at peace with HP Service Manager REST Connector (Wed 10 am)
• TT3097, HP ArcSight SmartConnector map files for fun and profit (Wed 4:30 pm)
• TB3044, Using Windows Event Forwarding with the Windows Unified Connector (Thurs 11am)

After the event

• Inquire about the beta
• Contact your sales rep
• Try the connector!

Your feedback is important to us. Please take a few minutes to complete the session survey.
Thank you!