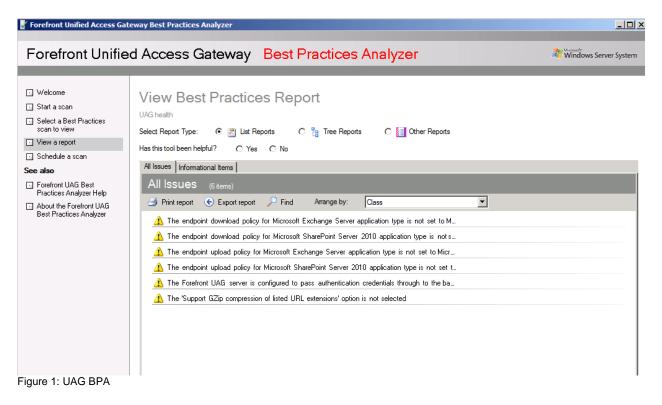
Microsoft Forefront UAG - Forefront UAG monitoring and debugging - part II

Abstract

This is a two part article series. In the first article we talked about monitoring techniques in Forefront UAG to monitor user sessions, network traffic and many more. In this article will go deeper into Forefront UAG debugging and tracing capabilities.

Let's begin

As a first step we will use the Forefront UAG Best Practice Analyzer to analyze the Forefront UAG installation against best practices from Microsoft. You can download the Forefront UAG Best Practice Analyzer from <u>here</u>. After the BPA scan has been completed you can see the results in the Forefront UAG BPA console to analyze the results against the builtin BPA help file or with corresponding Microsoft Technet articles.



Forefront UAG tracing

Forefront UAG is a complex application and if the standard troubleshooting tools like the Forefront UAG Web Monitor, UAG Activation Monitor and the Forefront TMG live logging are not sufficient to find the cause of a problem you can use the builtin tracing functionalities of Forefront UAG or as the first step the Forefront TMG diagnostic logging utility as shown in the following screenshot.

🗮 Forefront TMG		_ 8 ×											
File Action View Help													
Microsoft Forefront Threat Managemei Forefront TMG (UAG3) Dashboard Monitoring Kirewall Policy	Forefront Threat Management Gateway 2010	Enterprise											
Web Access Policy	Troubleshooting Change Tracking Traffic Simulator Diagnostic Logging Connectivity Test Use the diagnostic logging filter to view the events for a selected server.												
 Intrusion Prevention System Remote Access Policy (VPN) Networking System Logs & Reports Update Center Troubleshooting 	Filter Criteria	Diagnostic Logging Tasks											
	Message contains: Context contains:	X Delete Diagnostic Log											
	Server: UAG3 - Apply Filter Show All												
	Currently showing: server=[UAG3]												
	address: N/A Source array network: Local Host Destination IP address: N/A Destination array network: Internal												
	2660 01.04.2012 18:26:01 00003e40 Firewall Engine Forefront TMG is looking for an applicable network rule.												
	2661 01.04.2012 18:26:01 00003e40 Firewall Engine The packet was sent to or from the Local Host network Therefore, an implicit network rule with a route relationship between the source and destination is applied.												
	2662 01.04.2012 18:26:01 00003e40 Firewall Engine Forefront TMG will check only rules that are associated wit the protocol NTP (UDP).												
	2663 01.04.2012 18:26:01 00003e40 Firewall Engine Forefront TMG is evaluating the rule (System) Allow NTP												

Figure 2: TMG Diagnostic Logging

If the Forefront TMG Diagnostic logging is not sufficient to find the reason for a configuration problem with the Forefront UAG Server you are able to activate the Forefront UAG tracing feature which collects a large amount of data regarding the Forefront UAG configuration. The collected information of the UAG tracing utility are primarly designed to send this information to the Microsoft Customer Support Service (CSS) but if you are familiar with advanced Forefront UAG debugging it is possible to analyze the collected Forefront UAG trace data.

Forefront UAG provides tracing on both the Forefront UAG server, and on endpoint devices connecting to resources published via Forefront UAG. On the Forefront UAG server, tracing is available by default.

On endpoint devices connect to a Forefront UAG site or portal you must manually acivate the client-side tracing by installing the Forefront UAG client trace components.

On the Server side, default trace settings are in place:

- Tracing level is enabled for all components, and set to a verbosity level of "Error".
- By default, trace results are saved to a binary file (Forefront_UAG.BIN) located in the directory C:\WINDOWS\debug\. This directory also contains the trace file for Forefront TMG so it is possible to use the trace utility for Forefront TMG also.
- The file size is limited to 400 MB. When the size limit is reached, older trace messages are deleted, so that new trace messages can be added.

• It is possible to create only one trace file at the same time.

The graphical configuration tool for Forefront UAG tracing is called UAG Relaese Bits Tracing and can be found in the following directory on the Forefront UAG Server: *C:\program files\Microsoft Forefront Unified Access Gateway\common\bin\tracing.* Start the Trace Utility (a command line version is also available) and you are able to configure tracing for the different Forefront UAG components as shown in the following screenshot.

🔜 Release Bits Tracing						
			UAG	i Rele	ease B	its Tracing
Group	Error	Warn	Info	Func	Noise	Trace format search path:
GENERAL						
· ACE						Format As: Text Viewer
· ASFILTER						Trace File to Format
· AW						© Use C:\Windows\debug\Forefront_UAG.bin
· CERT_MANAGEMENT						
· CERTMAPPER						C Use this Browse
· Common						file
· CONFIGMGR_SERVICE						
· CONFIGURATION_GENERAL						Tracing configuration file:
· CONFIG_DATA_LAYER						Browse
+ CORE_BASE						Load Save
· CVCORE						
+ CompMgr_BASE						RT console colors
+ DAENG						Light Yellow 💌 on Gray
· DANLB_CFG						
+ DA_MGMT						
+ DCA_SRV_BASE						
· DCA_TRAY						
+ DNSALG_BASE						
· DSLIB						
+ Detector_BASE						
GLOBLIB						
• IISWRAPPER						

Figure 3: Forefront UAG Release Bits Tracking

It is possible to disable circular logging for the UAG trace file, you can specify another storage location for the trace log files and it is possible to configure the creation of trace log backup files. By default one one trace file will be saved as copy with the .BAK file extension.

Release Bits Tracing											
· WHLGENLIB_GENERAL											
+ WHLGLOBALUTILITIES_BASE											
· WHLGZIP											
+ WHLHTTPPARSER_BASE											
• WHLIISWRAPPER											
• WHLPERLCODE_GENERAL											
+ WHLRADIUSAUTH_BASE											
• WHLRDPMNG											
+ WHLSECURITYUTILITIES_BASE											
• WHLSSOCRYPT											
• WHLTRACE											
·WHLTSGAUTH											
·WHLTSGCONF											
• WHL_LOCAL_IP_MNGR											
· WIOCONFIG											
· WM_GENERAL											
	Go	0	GoRT		Stop						
Logging is currently ON											
✓ Circular log file of 400 Mbytes ✓ Auto enable tracing on startup Backup trace file on startup: Single Copy ▼ ● Use default C:\Windows\debug\Forefront_UAG.bin file Browse											

Figure 4: Forefront UAG Release Bits Tracking

Because the UAG trace file is stored binary we must have a technology which converts the trace file into readable format. You must download the trace symbol files from the following website. Extract the files to a directory on the Forefront UAG Server. If you want to send the trace file in a binary format to CSS, the tracing symbols are not required. After the UAG trace files has been downloaded you can use the Trace command line tool or the Foreront UAG Release Bits Tracing utility to specify the path to the trace files as shown in the following screenshot.

Release Bits Tracing											
UAG Release Bits Tracing											
Group	Error			Func	Noise	Trace format search path:					
· GENERAL						C:\temp\UAG_TMF_files\ Browse					
· ACE						Format As: Text Viewer Trace File to Format					
· ASFILTER · AW	য					© Use C:\Windows\debug\Forefront_UAG.bin					
Figure 5: Specify path to trace format fil	00.00	dapag	ifu o	utout							

Figure 5: Specify path to trace format files and specify output options

In the Forefront UAG Release Bits Tracking console click GO to start the trace process and after you reproduced possible problems with Forefront UAG click STOP to stop the tracing of files. You are able to store the trace results in text format or it is possible to display the results directly in a graphical viewer.

You can see a sample output of the trace utility in the following screenshot.

Errefront_UAG - Notepad
File Edit Format View Help
Setting log file to: C:\Windows\debug\Forefront_UAG.bin Examining C:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\tracing\default.tmf for message formats, 3 found.
Searching for TMF files on path: C:\Program Files\Microsoft Forefront Unified Access Gateway\common \bin\tracing;C:\temp\UAG_TMF_files\ Logfile C:\Windows\debug\Forefront_UAG.bin: OS version 6.1.7601 (Currently running on 6.1.7601) Start Time 2012-04-01-08:59:27.543 End Time Not set (Logger may not have been stopped). Timezone is @tzres.dll,-322 (Bias is -60mins) BufferSize 65536 B Maximum File Size 400 MB Buffers Written Not set (Logger may not have been stopped). Logger Mode Settings (2) (circular
ProcessorCount 1 WARNING: Circular Trace File did not have 'wrap' address EventTrace [0]c94.d64 04/01/2012-08:59:48.023 [monitormgrcore whale::monitormgr::CSQLBuiltinLog::Report SQLBuiltinLog.cpp@387] ERROR:LogWebProxyEntry() exited with exception. message id [3], message name [ServiceStartUp], exception code [-2147023143], exception description [NULL]. Unknown(85): GUID=d7da5775-d79e-fac8-3e40-29ced5a36d5e (No Format Information found). [0]c94.d64 04/01/2012-08:59:48.037 [monitormgrcore whale::monitormgr::CSQLBuiltinLog::Report SQLBuiltinLog.cpp@387] ERROR:LogWebProxyEntry() exited with exception. message id [25], message name [FailedToSendMessage], exception code [-2147023143], exception description [NULL]. Unknown(90): GUID=d7da5775-d79e-fac8-3e40-29ced5a36d5e (No Format Information found). Unknown(86): GUID=d7da5775-d79e-fac8-3e40-29ced5a36d5e (No Format Information found). Unknown(22): GUID=d7da5775-d79e-fac8-3e40-29ced5a36d5e (No Format Information found). Unknown(22): GUID=d7da5775-d79e-fac8-3e40-29ced5a36d5e (No Format Information found). Unknown(25): GUID=d7da5775-d79e-fac8-3e40-29ced5a36d5e (No Format Information found). Unknown(11): GUID=d7da5775-d79e-fac8-3e40-29ced5a36d5e (No Format Information found). Unknown(11): GUID=236ca6ba-25c2-6799-5b85-55bb28014e76 (No Format Information found). Unknown(11): GUID=236ca6ba-25c2-0799-5b85-95ebb79efd3 (No Format Information found). Unknown(11): GUID=cle41fc-66f9-3c22-0db5-9eedb73effd3 (No Format Information found). [0]c7c.c90 04/01/2012-09:01:59.178 [whlcomtrace IISWrapper.cs@0] ERROR:[212] @ [0] @ [1] @ [IISWrapper.cs] @ [0] @ [Custom DefAppPoolPingResTime value found: [600]] [0]c7c.c90 04/01/2012-09:01:59.206 [whlcomtrace IISWrapper.cs@0] ERROR:[212] @ [0] @ [1] @ [IISWrapper.cs] @ [0] @ [Custom DefAppPoolPingFreqTime value found: [60]] [0]c7c.c90 04/01/2012-09:01:59.206 [whlcomtrace IISWrapper.cs@0] ERROR:[212] @ [0] @ [1] @ [IISWrapper.cs] @ [0] @ [CreateBindingInformation WARNING: Received invalid IP []. Port: [6001]. Continuing flow.]
[0]c7c.c90 04/01/2012-09:01:59.207 [whicomtrace IISWrapper.cs@0] ERROR:[212] @ [0] @ [1] @ Figure 6: Forefront UAG Release Bits Tracking output file

The next screenshot shows the output of the Forefront UAG tracing with the graphical viewer.

_	aceView Edit Viev		ADMINI~	1.DOM\AppData\Local\To	emp\1\Forefront_	_UAG.txt		_ 8
#	CPU	Process	Thread	Time	Component	Func	File	Line
) L	0	c94	d64	04/01/2012-08:59:48.023	monitormarcore	whale::monitormgr::CSQLBuiltinLog::Report	SQLBuiltinLog.cpp	387
2	0	c94	d64	04/01/2012-08:59:48.037	monitormarcore	whale::monitormgr::CSQLBuiltinLog::Report	SQLBuiltinLog.cpp	387
	0	c7c	c90	04/01/2012-09:01:59.178	whicomtrace		IISWrapper.cs	0
	0	c7c	c90	04/01/2012-09:01:59.178	whicomtrace		IISWrapper.cs	0
	0	c7c	c90	04/01/2012-09:01:59.206	whicomtrace		IISWrapper.cs	0
	0	c7c	c90	04/01/2012-09:01:59.207	whicomtrace		IISWrapper.cs	0
	0	c94	1274	04/01/2012-13:37:27.243	monitormarcore	whale::monitormgr::CMessagesReport::GetMessages	MessagesReport.cpp	1066
	0	c94	1274	04/01/2012-13:37:27.243	monitormarcore	whale::monitormgr::CMessagesReport::GetMessagesXml	MessagesReport.cpp	1008
	0	c94	1274	04/01/2012-13:37:27.243	monitormarcore	whale::monitormgr::CMessagesReport::GetMessageXml	MessagesReport.cpp	138
0	0	c94	1274	04/01/2012-13:37:27.244	monitormarcore	whale::monitormgr::CMessagesReport::GetMessages	MessagesReport.cpp	1066
1	0	c94	1274	04/01/2012-13:37:27.244	monitormarcore	whale::monitormgr::CMessagesReport::GetMessagesXml	MessagesReport.cpp	1008
2	0	c94	1274	04/01/2012-13:37:27.244	monitormarcore	whale::monitormgr::CMessagesReport::GetMessageXml	MessagesReport.cpp	138
3	0	c94	1274	04/01/2012-13:37:27.245	monitormarcore	whale::monitormgr::CMessagesReport::GetMessages	MessagesReport.cop	1066
ŧ	0	c94	1274	04/01/2012-13:37:27.245	monitormarcore	whale::monitormgr::CMessagesReport::GetMessagesXml	MessagesReport.cop	1008
5	0	c94	1274	04/01/2012-13:37:27.245	monitormarcore	whale::monitormgr::CMessagesReport::GetMessageXml	MessagesReport.cpp	138
5	0	c94	1274	04/01/2012-13:37:27.247	monitormarcore	whale::monitormgr::CMessagesReport::GetMessages	MessagesReport.cpp	1066
7	0	c94	1274	04/01/2012-13:37:27.247	monitormarcore	whale::monitormgr::CMessagesReport::GetMessagesXml	MessagesReport.cop	1008
3	0	c94	1274	04/01/2012-13:37:27.247	monitormgrcore	whale::monitormgr::CMessagesReport::GetMessageXml	MessagesReport.cpp	138
	0	c94	1274	04/01/2012-13:37:27.247	monitormarcore	whale::monitormgr::CMessagesReport::GetMessages	MessagesReport.cpp	1066
)	0	c94	1274	04/01/2012-13:37:27.247	monitormgrcore	whale::monitormgr::CMessagesReport::GetMessagesXml	MessagesReport.cpp	1008
1	0	c94	1274	04/01/2012-13:37:27.247	monitormarcore	whale::monitormgr::CMessagesReport::GetMessageXml	MessagesReport.cpp	138
2	0	c94	1274	04/01/2012-13:37:27.249	monitormarcore	whale::monitormgr::CMessagesReport::GetMessages	MessagesReport.cpp	1066
3	ō	c94	1274	04/01/2012-13:37:27.249	monitormarcore	whale::monitormgr::CMessagesReport::GetMessagesXml	MessagesReport.cpp	1008
4	0	c94	1274	04/01/2012-13:37:27.249	monitormarcore	whale::monitormgr::CMessagesReport::GetMessageXml	MessagesReport.cpp	138
5	0	c94	1274	04/01/2012-13:37:27.250	monitormarcore	whale::monitormgr::CMessagesReport::GetMessages	MessagesReport.cpp	1066
5	0	c94	1274	04/01/2012-13:37:27.250	monitormarcore	whale::monitormgr::CMessagesReport::GetMessagesXml	MessagesReport.cpp	1008
7	0	c94	1274	04/01/2012-13:37:27.250	monitormgrcore	whale::monitormgr::CMessagesReport::GetMessageXml	MessagesReport.cpp	138
1	0	c94	1274	04/01/2012-13:37:27.250	monitormarcore	whale::monitormgr::CMessagesReport::GetMessages	MessagesReport.cpp	1066
,	Ō	c94	1274	04/01/2012-13:37:27.250	monitormarcore	whale::monitormgr::CMessagesReport::GetMessagesXml	MessagesReport.cpp	1008
)	ō	c94	1274	04/01/2012-13:37:27.250	monitormarcore	whale::monitormgr::CMessagesReport::GetMessageXml	MessagesReport.cpp	138
i	ō	c94	1038	04/01/2012-13:38:20.500	monitormarcore	whale::monitormgr::CMessagesReport::GetMessages	MessagesReport.cpp	1066
2	ŏ	c94	1038	04/01/2012-13:38:20.500	monitormarcore	whale::monitormgr::CMessagesReport::GetMessagesXml	MessagesReport.cpp	1008
	ŏ	c94	1038	04/01/2012-13:38:20.500	monitormgrcore	whale::monitormgr::CMessagesReport::GetMessageXml	MessagesReport.cpp	138
1	ŏ	c94	1038	04/01/2012-13:38:20.501	monitormarcore	whale::monitormgr::CMessagesReport::GetMessages	MessagesReport.cop	1066

Figure 7: Forefront UAG Release Bits Tracking – graphical viewer

Conclusion

In this article I tried to give you some helpful information how to debug a Forefront UAG installation / configuration if the traditional logging and monitoring capabilities of Forefront UAG are not sufficient.

Related links

UAG Tracing made simple

http://blogs.technet.com/b/ben/archive/2010/09/03/uag-tracing-made-simple.aspx Using tracing in Forefront UAG

http://technet.microsoft.com/en-us/library/gg508832.aspx

Forefront Unified Access Gateway (UAG) Tracing Symbols

http://www.microsoft.com/download/en/details.aspx?amp;displaylang=en&displaylan

<u>g=en&id=15651</u>

Planning for monitoring and logging

http://technet.microsoft.com/en-us/library/dd897042.aspx

Microsoft Forefront UAG – Overview of Microsoft Forefront UAG

http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-

Forefront-UAG.html

Forefront UAG technical overview

http://technet.microsoft.com/en-us/library/ee690443.aspx