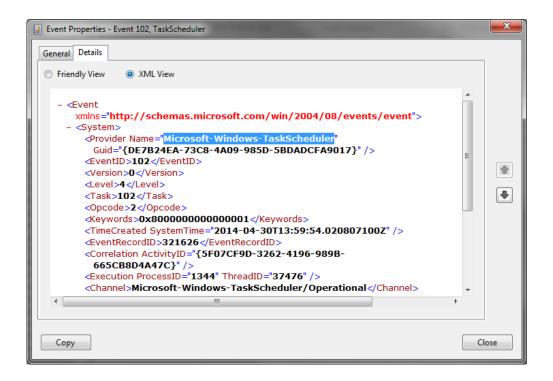


Collecting and Monitoring Tiered Windows Event Logs

https://campus.barracuda.com/doc/98217294/

The process is very similar to monitoring standard Windows events, however, specific details are needed to properly collect the event as the Source and Log name may differ from what it displayed in the Windows event viewer. When adding your Log and Source you must open the details of the Windows event in XML view.

Now proceed to locate the entry for Provider Name, this will be the event Source name entered into your monitor. It will appear similar to the following:



Now you will need to locate the Channel entry, this will be the Log name entered into the monitor. It will appear similar to the following:

Barracuda RMM



General Details		
Friendly View	XML View XML View	
- <syste <pro Gu <eve <ver <tas <opc <key <tim <eve <cor 66 <exe< td=""><td>"http://schemas.microsoft.com/win/2004/08/events/event"> m> vider Name="Microsoft-Windows-TaskScheduler" id="{DE7B24EA-73C8-4A09-985D-5BDADCFA9017}" /> ntID>102 sion>0 el>4 k>102 code>2 words>0x80000000000001 eCreated SystemTime="2014-04-30T13:59:54.020807100Z" /> intRecordID>321626 relation ActivityID="{5F07CF9D-3262-4196-989B- 5CB8D4A47C}" /> cution ProcessID="1344" ThreadID="37476" /> innel>Microsoft-Windows-TaskScheduler/Operational</td><td>•</td></exe<></cor </eve </tim </key </opc </tas </ver </eve </pro </syste 	"http://schemas.microsoft.com/win/2004/08/events/event"> m> vider Name="Microsoft-Windows-TaskScheduler" id="{DE7B24EA-73C8-4A09-985D-5BDADCFA9017}" /> ntID>102 sion>0 el>4 k>102 code>2 words>0x80000000000001 eCreated SystemTime="2014-04-30T13:59:54.020807100Z" /> intRecordID>321626 relation ActivityID="{5F07CF9D-3262-4196-989B- 5CB8D4A47C}" /> cution ProcessID="1344" ThreadID="37476" /> innel>Microsoft-Windows-TaskScheduler/Operational	•

Once this information has been properly added, save the monitor and if possible use event create or generate the event through other means to test the alert.

Additional Information

- Eventcreate command line reference
- Event Viewer Technet reference

Barracuda RMM



Figures

- 1. tier.png
- 2. Tiered1.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.