NiCE Log File MP

Using the NiCE Log File MP to Create Performance Views from Log Files

for use with System Center Operations Manager

Whitepaper
NiCE LogFile Management Pack
Version 01.3x
May 2017

NiCE
IT Management Solutions

Contents

Purpose of this Document

This document describes an use case scenario for the NiCE Log File MP, highlighting where it can be used to generate a performance view based on entries in a log file.

The NiCE Log File MP Whitepaper provides useful information in addition to the Log File MP Quick Start Guide, without replacing it or parts of it. It should be seen as a supplement to better understand and use the Log File MP features.

Overview

The NiCE Log File Management Pack monitors log files on the Windows platform and alerts based on matching patterns. The MP also gives the ability to use the data in the log files and generate performance view. This paper walks you through how this can be achieved using the NiCE Log File MP Performance Rule wizard.

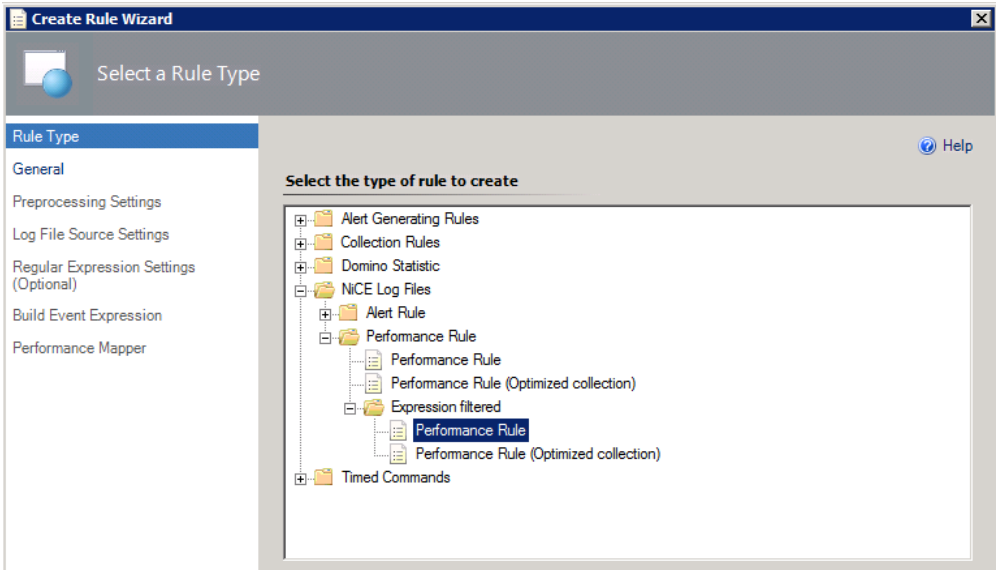
Use Case Scenario

The user has a script that will run on a schedule and collect ping data for a bunch of their servers. They want to use the data to generate a performance view in SCOM and so can see trend data for a particular server.

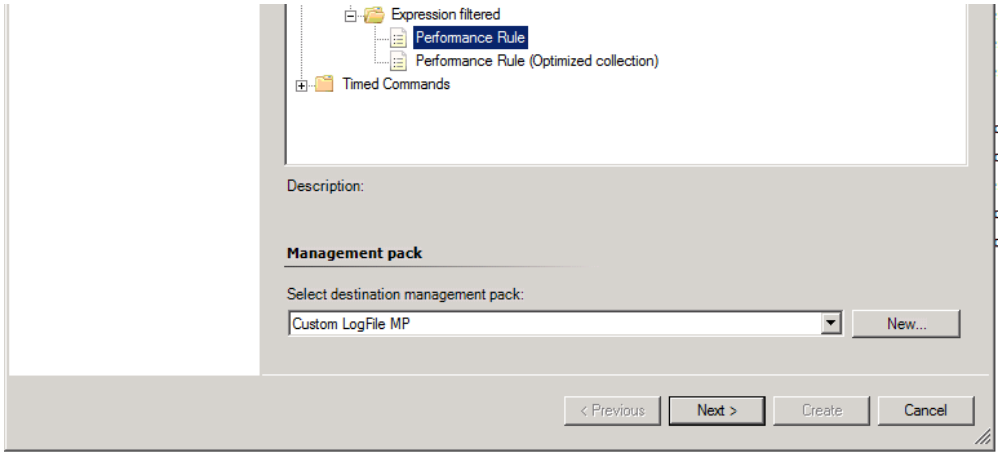
This can be accomplished by setting up a NiCE Log File MP **Performance Rule** that reads the log file and pulls data for a specific server and generates a performance view in SCOM.

Steps to Setup an Example Performance Rule

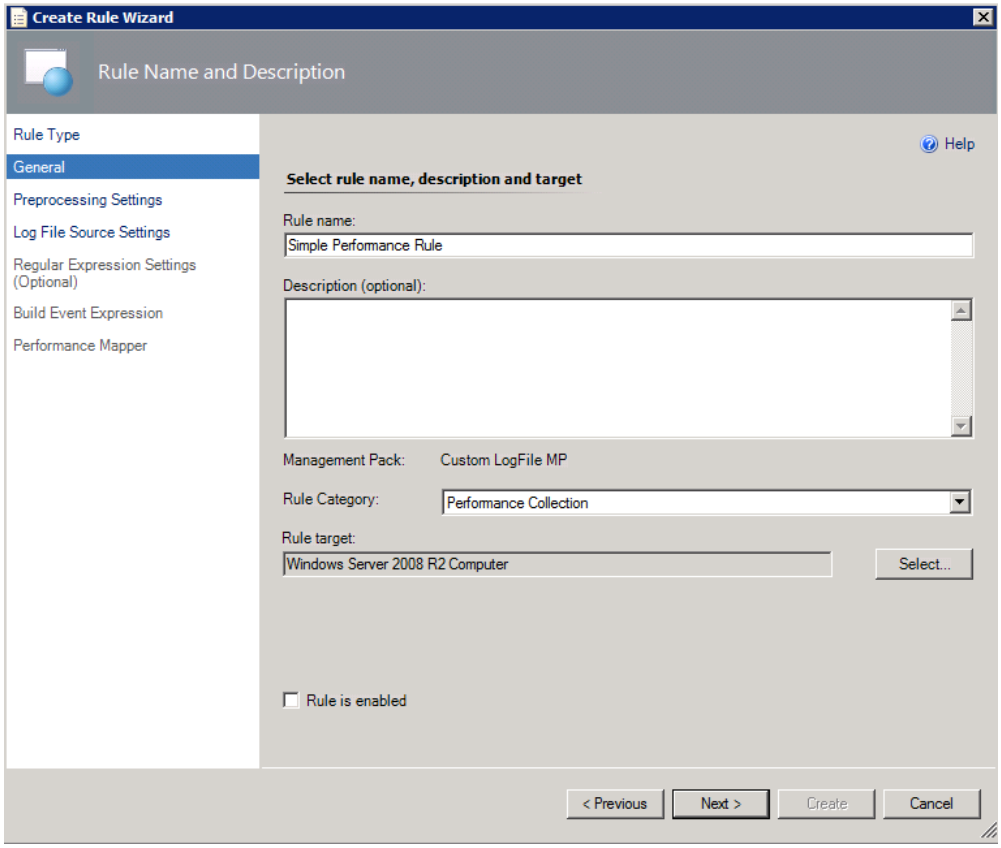
1. Launch the **Rule** wizard from the SCOM Console and select **Performance Rule.**



2. Select an existing or generate a new Management Pack where the rule is going to be saved.

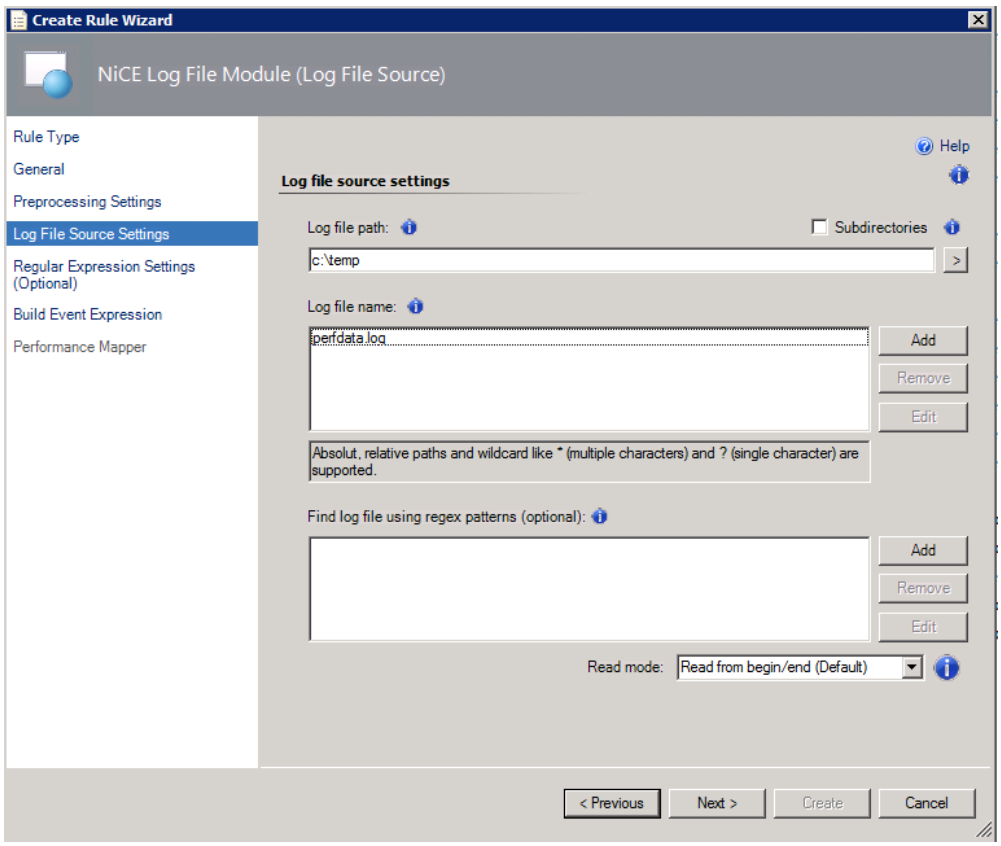


3. Navigate through the **General** page and specify the Rule name and the Rule target values. Ideally, set the rule to be disabled and you can override it to the specific node/group.



4. Navigate through the Log File Source Settings page and specify the log file details. You can specify the log file path either with absolute values as shown below or using environment variables. You can specify the log file name also either with the actual log file or wildcards.

   By default, the rule is going to read the log file from the beginning the first time it runs and then from that point on it will read any new entries. You can see more details in the Log File MP Quick Start Guide about Read Mode.

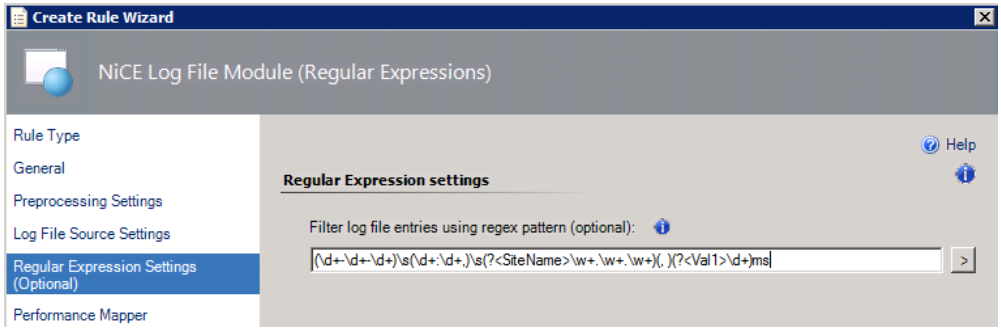


5. On the Regular Expression Settings page, define the pattern matching that will be used to identify if a line is going to be read from the log file.

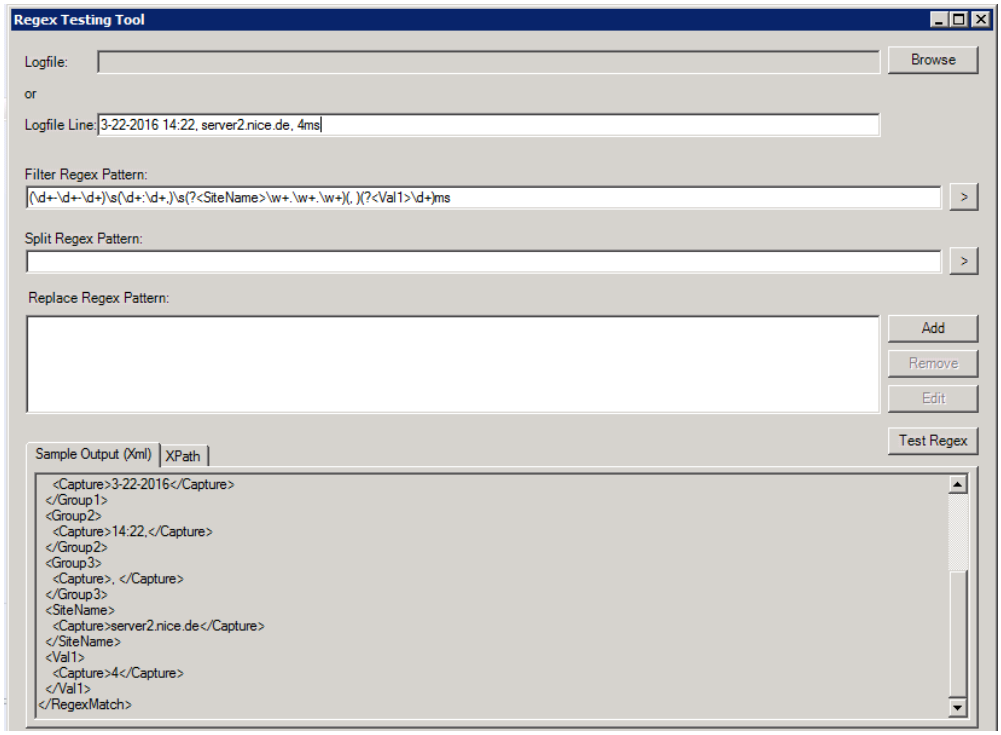
   In this example, the log file being read has lines like this

   3-22-2016 14:18, server1.nice.de, 31ms
   3-22-2016 14:22, server2.nice.de, 4ms

   The regular expression shown below will match the above lines. It will store the server name to the variable “SiteName” and the data that will be used to generate the performance view to variable “Val1”.



   The wizard has a built-in Regex testing tool that you can use to validate the regular expression using the log file line that you are trying to match.

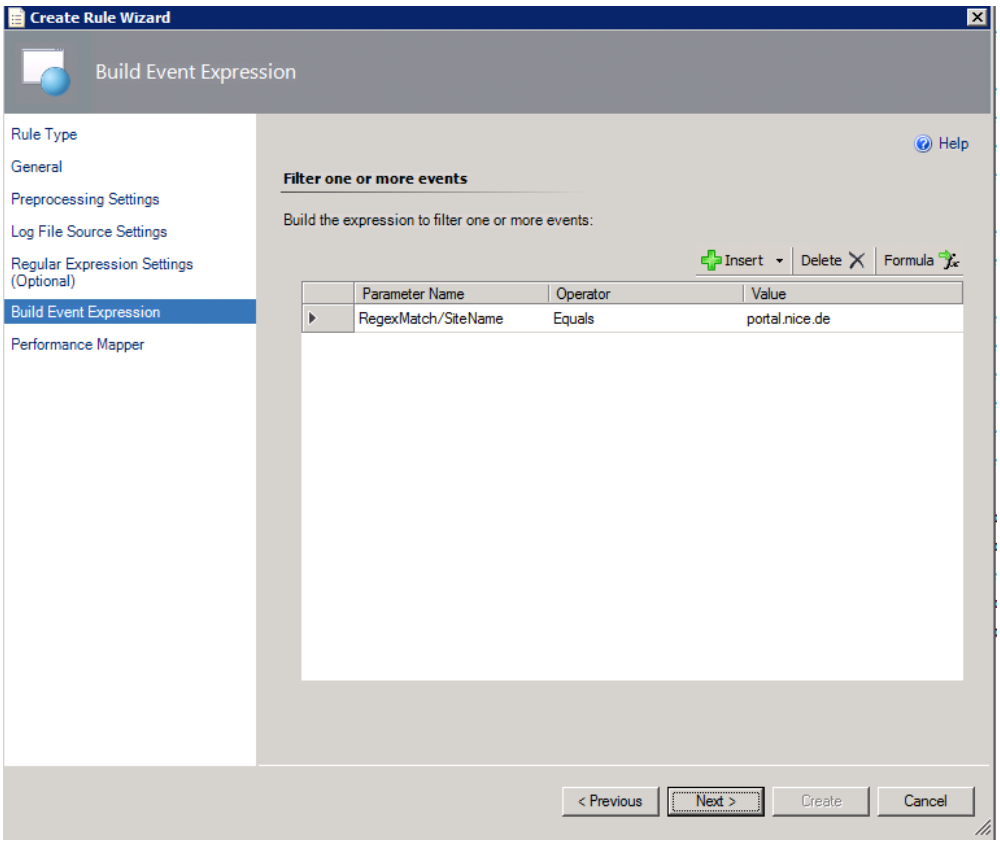


6. On the **Build Event Expression** page, you define the filtering logic that will be used to collect the performance data from the matched log file lines.

   In the previous step we defined how the lines are going to be read from the log file. Here we define what specific lines that match the pattern are of interest to us when generating the performance view.

   This page defines the value that will be compared with XPath data to determine if the log entry is used or ignored in the performance view. You can see more details on XPath in the Log File MP Quick Start Guide.

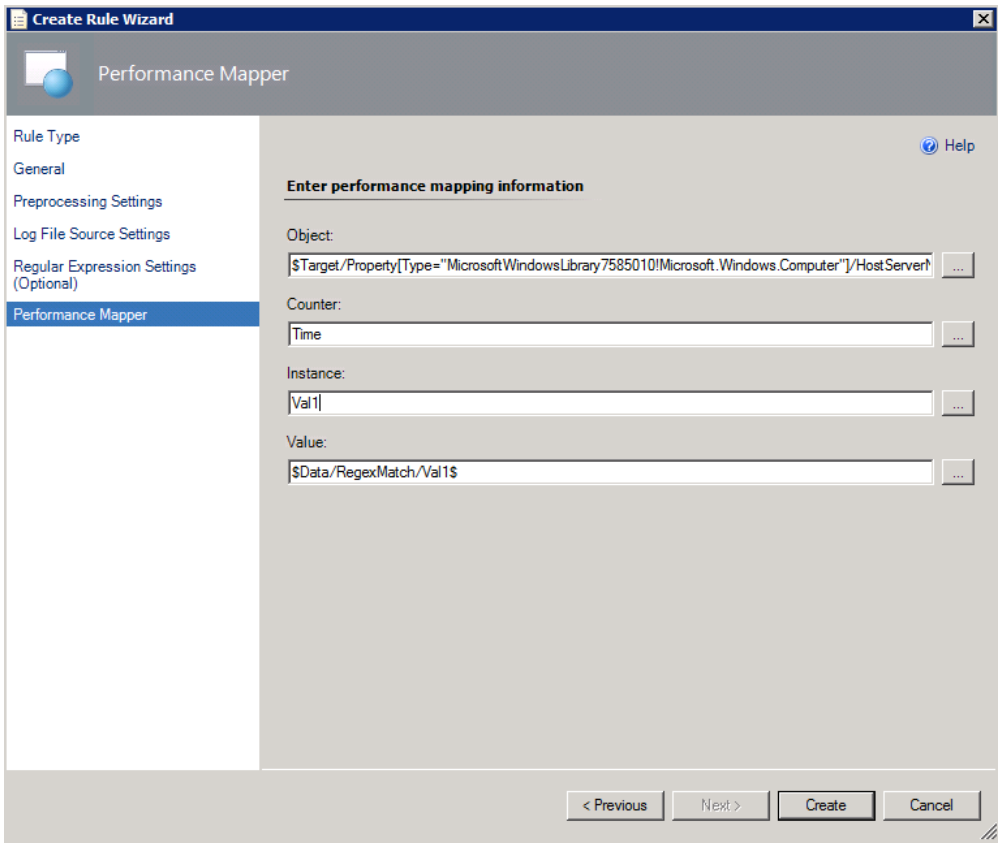
   In the example below, the rule is set up such that it will use data only if the pattern matched entries in the log file also meets the criteria that they have “portal.nice.de” in them.



7. In the Performance Mapper page, specify the place holder for the data that is going to be used when generating the performance view.

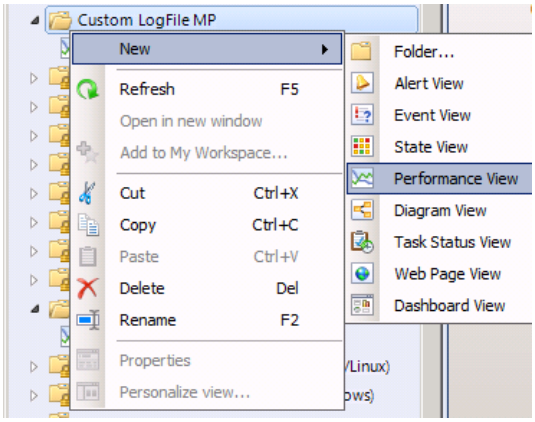
   Object, Counter and Instance fields can be any value, either free text or Target that is appropriate for the data being mapped. Value defines the actual data being mapped and XPath is used. Once again, you can see more details in the Log File MP Quick Start Guide on XPath.

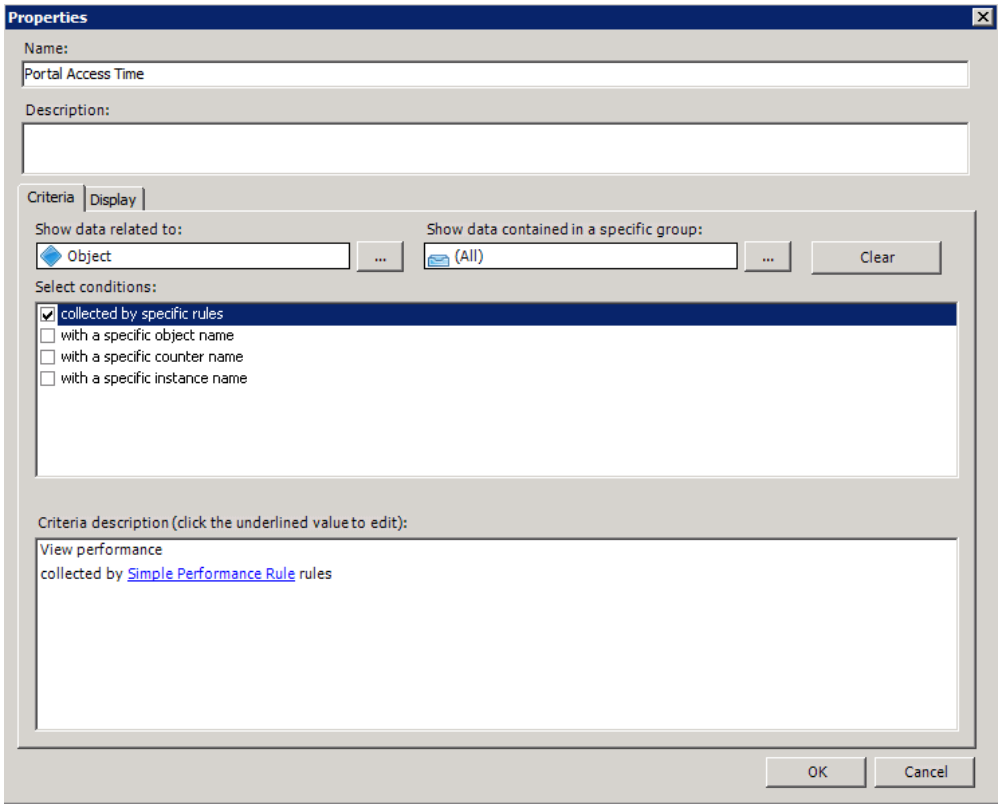
   In our example, the data was stored in variable Val1 and so we map Value to $Data/RegexMatch/Val1$.



8. Save the rule and the Performance Log rule is now created in the custom MP.

9. In the SCOM Console under **Monitoring** pane, you will see the new folder for the custom MP that was created. Create a new **Performance View** in this folder.



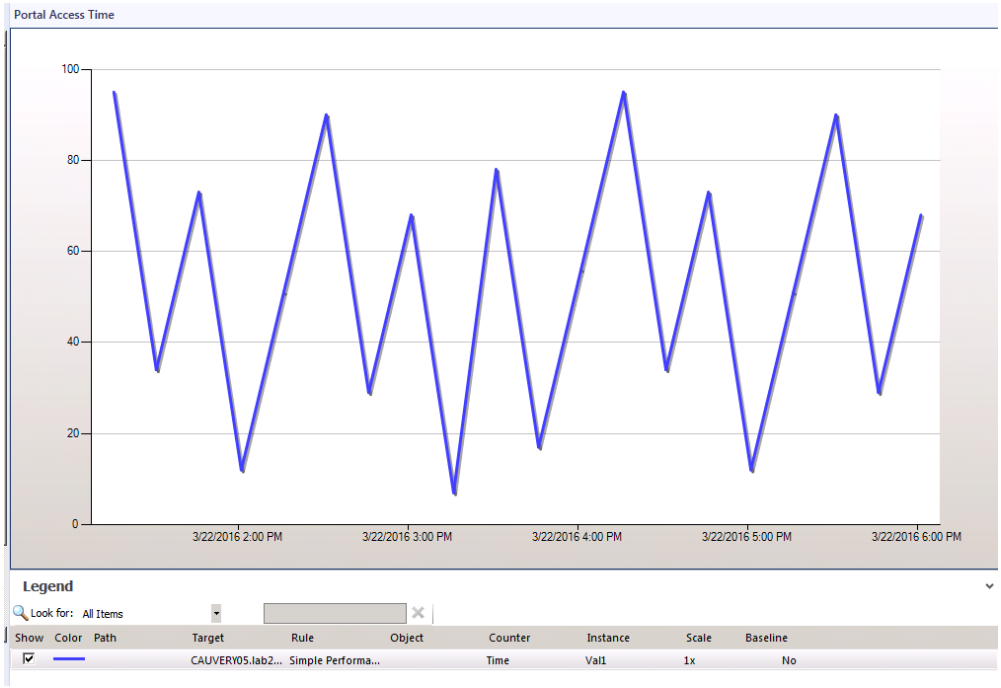


You can also define how the view should look like in the Display tab in the above screenshot.

10. Override the performance rule as appropriate for your environment so it gets enabled on the node where you have the log file that needs to be monitored.

11. If all goes as expected, then the performance rule would look for the matching pattern and filter in the log file and collect the performance data that will show in the Performance View that we created.

Here is an example performance view from sample data collected from such a log file.



Appendix

You can see below the custom MP that would be created based on the steps listed above. Copy and paste it to any document editor and save it as **Custom.LogFile.MP.xml.**

```
<?xml version="1.0" encoding="utf-8"?><ManagementPack ContentReadable="true"
SchemaVersion="2.0" OriginalSchemaVersion="1.1"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
 <Manifest>
  <Identity>
   <ID>Custom.LogFile.MP</ID>
   <Version>1.0.0.0</Version>
  </Identity>
  <Name>Custom LogFile MP</Name>
  <References>
   <Reference Alias="SCDW">
    <ID>Microsoft.SystemCenter.DataWarehouse.Library</ID>
    <Version>7.1.10226.0</Version>
    <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
   </Reference>
   <Reference Alias="NiCELogFileLibrary">
    <ID>NiCE.LogFile.Library</ID>
    <Version>1.33.80.0</Version>
    <PublicKeyToken>058cf9bbd5db72a4</PublicKeyToken>
   </Reference>
   <Reference Alias="MicrosoftWindowsLibrary7585010">
    <ID>Microsoft.Windows.Library</ID>
    <Version>7.5.8501.0</Version>
    <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
   </Reference>
   <Reference Alias="Performance">
    <ID>System.Performance.Library</ID>
    <Version>7.0.8433.0</Version>
    <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
   </Reference>
   <Reference Alias="SystemLibrary7585010">
    <ID>System.Library</ID>
    <Version>7.5.8501.0</Version>
    <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
   </Reference>
   <Reference Alias="SystemCenter">
    <ID>Microsoft.SystemCenter.Library</ID>
    <Version>7.0.8433.0</Version>
    <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
   </Reference>
   <Reference Alias="MicrosoftWindowsServer2008Discovery6070610">
```

```
      <ID>Microsoft.Windows.Server.2008.Discovery</ID>
      <Version>6.0.7061.0</Version>
      <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
    </Reference>
    <Reference Alias="Health">
      <ID>System.Health.Library</ID>
      <Version>7.0.8433.0</Version>
      <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
    </Reference>
  </References>
 </Manifest>
 <Monitoring>
  <Rules>
   <Rule ID="MomUIGeneratedRule11139f1796c14fdf8736e71840d497ab" Enabled="false"
Target="MicrosoftWindowsServer2008Discovery6070610!Microsoft.Windows.Server.2008.R2.C
omputer" ConfirmDelivery="true" Remotable="false" Priority="Normal" DiscardLevel="100">
      <Category>PerformanceCollection</Category>
      <DataSources>
       <DataSource ID="DS"
TypeID="NiCELogFileLibrary!NiCE.LogFile.Library.Performance.Advanced.Filtered.LogFileProvider
.DS">
         <ProviderConfig>
          <Interval>60</Interval>
          <Unit>Seconds</Unit>
          <SyncTime />
          <WorkingDirectory />
          <Command />
          <Arguments />
          <EnvironmentVariables />
          <Timeout>0</Timeout>
          <Tracing>false</Tracing>
         </ProviderConfig>
         <LogFileProviderConfig>
          <Directory>c:\temp</Directory>
          <SubDirectories>false</SubDirectories>
          <Files>
           <FileNamePattern>perfdata.log</FileNamePattern>
          </Files>
          <ReadMode>Default</ReadMode>
          <RegexFilter>(\d+-\d+-\d+)\s(\d+:\d+,)\s(?&lt;SiteName&gt;\w+.\w+.\w+)(,
)(?&lt;Val1&gt;\d+)ms</RegexFilter>
          <RegexSplit />
          <RegexReplace />
         </LogFileProviderConfig>
         <Expression>
          <SimpleExpression>
           <ValueExpression>
```

```
            <XPathQuery Type="String">RegexMatch/SiteName</XPathQuery>
           </ValueExpression>
           <Operator>Equal</Operator>
           <ValueExpression>
            <Value Type="String">portal.nice.de</Value>
           </ValueExpression>
          </SimpleExpression>
         </Expression>

<ObjectName>$Target/Property[Type="MicrosoftWindowsLibrary7585010!Microsoft.Windows.
Computer"]/HostServerName$</ObjectName>
         <CounterName>Time</CounterName>
         <InstanceName>Val1</InstanceName>
         <Value>$Data/RegexMatch/Val1$</Value>
        </DataSource>
       </DataSources>
       <WriteActions>
        <WriteAction ID="WriteToDB"
TypeID="SystemCenter!Microsoft.SystemCenter.CollectPerformanceData" />
        <WriteAction ID="WriteToDW"
TypeID="SCDW!Microsoft.SystemCenter.DataWarehouse.PublishPerformanceData" />
       </WriteActions>
     </Rule>
    </Rules>
    <Overrides>
     <RulePropertyOverride
ID="OverrideForRuleMomUIGeneratedRule11139f1796c14fdf8736e71840d497abForContextMic
rosoftWindowsComputerbb60e3813b4a4123ba1ecd4abf736a10"
Context="MicrosoftWindowsLibrary7585010!Microsoft.Windows.Computer"
ContextInstance="4de310c0-17ef-64b5-c9b8-31ccc081c422" Enforced="false"
Rule="MomUIGeneratedRule11139f1796c14fdf8736e71840d497ab" Property="Enabled">
       <Value>true</Value>
     </RulePropertyOverride>
    </Overrides>
  </Monitoring>
  <Presentation>
    <Views>
     <View ID="View_14363e6b08894bafb9d90643ab8ac039" Accessibility="Public"
Enabled="true" Target="SystemLibrary7585010!System.Entity"
TypeID="SystemCenter!Microsoft.SystemCenter.PerformanceViewType" Visible="true">
       <Category>Operations</Category>
       <Criteria>
        <RuleList>
         <Rule>54ed5979-9113-3e34-cd94-ee952e78e86a</Rule>
        </RuleList>
       </Criteria>
       <Presentation>
```

<SortedColumnIndex>0</SortedColumnIndex>
<SortOrder>0</SortOrder>
<StartTime>2016-03-20T17:05:00.966854-07:00</StartTime>
<EndTime>2016-03-21T17:05:00.966854-07:00</EndTime>
<DynamicTimeTicks>432000000000</DynamicTimeTicks>
<IsDynamic>true</IsDynamic>
<Is3DMode>false</Is3DMode>
<ShowAlerts>false</ShowAlerts>
<ShowMaintenanceMode>false</ShowMaintenanceMode>
<BaselineMode>false</BaselineMode>
<ShowPointLabels>false</ShowPointLabels>
<EnableSmartLabels>true</EnableSmartLabels>
<RightAngleAxes>false</RightAngleAxes>
<ClusterSeries>false</ClusterSeries>
<Title />
<TitleFont>Microsoft Sans Serif,12,Regular</TitleFont>
<ChartFont>Microsoft Sans Serif,8.25,Regular</ChartFont>
<ShowBands>false</ShowBands>
<BandColor>-1579033</BandColor>
<ChartType>Line</ChartType>
<Depth>100</Depth>
<GapDepth>100</GapDepth>
<Perspective>10</Perspective>
<GraphXRotation>0</GraphXRotation>
<GraphYRotation>0</GraphYRotation>
<XLabelAngle>0</XLabelAngle>
<LabelColor>-16777216</LabelColor>
<LabelFont>Microsoft Sans Serif,8.25,Regular</LabelFont>
<XAxisVisible>True</XAxisVisible>
<XShowMajorGridlines>false</XShowMajorGridlines>
<XShowMinorGridlines>false</XShowMinorGridlines>
<ShowInterlaceStrips>false</ShowInterlaceStrips>
<XInterlaceColor>16777215</XInterlaceColor>
<XShowSideMargin>true</XShowSideMargin>
<XAxisFont>Microsoft Sans Serif,8.25,Regular</XAxisFont>
<AutoAxis>true</AutoAxis>
<AxisMax>100</AxisMax>
<AxisMin>0</AxisMin>
<YAxisVisible>True</YAxisVisible>
<YShowMajorGridlines>true</YShowMajorGridlines>
<YShowMinorGridlines>false</YShowMinorGridlines>
<YShowInterlaceStrips>false</YShowInterlaceStrips>
<YShowSideMargin>true</YShowSideMargin>
<YAxisFont>Microsoft Sans Serif,8.25,Regular</YAxisFont>
<BackgroundColor1>-1</BackgroundColor1>
<BackgroundColor2>-1</BackgroundColor2>
<GradientType>None</GradientType>

```
        <Series />
       </Presentation>
       <Target />
      </View>
    </Views>
    <Folders>
     <Folder ID="Folder_34a1aa9279754176b3b6705b4df274b1" Accessibility="Public"
ParentFolder="SystemCenter!Microsoft.SystemCenter.Monitoring.ViewFolder.Root" />
    </Folders>
    <FolderItems>
     <FolderItem ElementID="View_14363e6b08894bafb9d90643ab8ac039"
ID="ibffd641db96a434597f565b70042f313"
Folder="Folder_34a1aa9279754176b3b6705b4df274b1" />
    </FolderItems>
  </Presentation>
  <LanguagePacks>
    <LanguagePack ID="ENU" IsDefault="false">
     <DisplayStrings>
       <DisplayString ElementID="Custom.LogFile.MP">
         <Name>Custom LogFile MP</Name>
       </DisplayString>
       <DisplayString ElementID="Folder_34a1aa9279754176b3b6705b4df274b1">
         <Name>Custom LogFile MP</Name>
       </DisplayString>
       <DisplayString ElementID="MomUIGeneratedRule11139f1796c14fdf8736e71840d497ab">
         <Name>Simple Performance Rule</Name>
       </DisplayString>
       <DisplayString ElementID="View_14363e6b08894bafb9d90643ab8ac039">
         <Name>Portal Access Time</Name>
       </DisplayString>
       <DisplayString ElementID="MomUIGeneratedRule11139f1796c14fdf8736e71840d497ab"
SubElementID="WriteToDW">
         <Name>Performance data publisher</Name>
       </DisplayString>
       <DisplayString ElementID="MomUIGeneratedRule11139f1796c14fdf8736e71840d497ab"
SubElementID="DS">
         <Name>Performance filtered Log file Provider</Name>
       </DisplayString>
       <DisplayString ElementID="MomUIGeneratedRule11139f1796c14fdf8736e71840d497ab"
SubElementID="WriteToDB">
         <Name>Performance Data Collection Write Action</Name>
       </DisplayString>
     </DisplayStrings>
    </LanguagePack>
  </LanguagePacks>
</ManagementPack>
```