

## Start-LogShark

### Version

V0.1 beta

Klaus Salger, AXOQUENT GmbH, 06.2010

### SYNOPSIS

Starts LogShark with a generated configuration file.

### SYNTAX

Start-LogShark [-ComputerName] <computername> [[-LogSharkConfigTemplate] <LogSharkConfigTemplate>] [-WrapperConfigFile] <WrapperConfigFile> [-<CustomVariable> <CustomValue>]\*

### DETAILED DESCRIPTION

Start-LogShark will replace tags in a LogShark configuration file template and run LogShark with the generated configuration file. The computer that LogShark will connect to is given via command line together with optional parameters that allow the setting of config files and custom variables to be replaced in the template.

The template file is the file to be used for LogShark config file generation. It may contain various tags that will be replaced by variables. Variables may come from the wrapper config file or command line parameters. With the paths to be monitored being the most important variable.

More than one path per tag may be configured in the WrapperConfigFile. The *first* accessible path will be used for the replacement. So language or OS version dependent paths may be handled, e.g.

„C:\programme\gemeinsame dateien“ on German and „c:\program files\common files“ on English operating systems.

The following is a sample WrapperConfigFile with the command starting LogShark in the Config section and 2 Pathgroups with one tag and one or more paths. Further variables are defined in the SimpleVars section.

```
<<?xml version="1.0" encoding="utf-8"?>
<WrapperConfig>
  <Description>
    <Text>Universal LogShark Wrapper Config, V0.1</Text>
  </Description>

  <Config>
    <Command>"#PROGRAMFILES#\Java\jre6\bin\javaw.exe" -Xmx512m -jar
"#PROGRAMFILES#\LogShark\logshark.jar" "#ResultConfigFile#"</Command>
  </Config>

  <Paths>
    <Pathgroup>
      <Tag>WinDir</Tag>
      <Path>#computer#\Admin$</Path>
    </Pathgroup>
    <Pathgroup>
      <Tag>ProgramFiles</Tag>
      <Path>#computer#\c$\program files (x86)</Path>
      <Path>#computer#\c$\programme (x86)</Path>
      <Path>#computer#\c$\program files</Path>
      <Path>#computer#\c$\programme</Path>
    </Pathgroup>
  </Paths>
</WrapperConfig>
```

```

</Paths>

<SimpleVars>
  <Var>
    <Tag>ErrorForeground</Tag>
    <Value>000000</Value>
  </Var>
  <Var>
    <Tag>ErrorBackground</Tag>
    <Value>FF0000</Value>
  </Var>
</SimpleVars>
</WrapperConfig>

```

## PARAMETERS

### -ComputerName <computername>

The name of the computer that hosts the log directories. May be any name that is accepted in a UNC path. Mandatory.

Named or positional parameter.

### -LogSharkConfigTemplate <LogSharkConfigTemplate>

The LogShark template file to be used.

May be a full or relative path or just a filename.

If this is just a filename it will be loaded from the scripts directory.

Optional, default="LogSharkTemplate.lsc" (will look for the file in the same directory as the script).

Named or positional parameter.

### -WrapperConfigFile <WrapperConfigFile>

The wrapper configuration file to be used.

May be a full or relative path or just a filename.

If this is a filename it will be loaded from the scripts directory.

Optional, default="Start-LogShark.xml" (will look for the file in the same directory as the script).

Named or positional parameter.

### -CustomTag <CustomValue>

A tag that should be replaced by a the value with the parameter name defining the tag and the actual parameter defining the value. It defines a variable like a SimpleVar in the wrapper config xml but lets the user determine the tag-value pairs on the command line. Custom tags will be replaced in the template *before* replacing the tags defined in the wrapper config file. So defaults may be defined in the wrapper config file but changed via command line if necessary.

More than one CustomTag and Customvalue may be used.

Optional

Named parameter.

## EXAMPLES

### Example 1

```
Powershell -file Start-LogShark -ComputerName Comp0815
```

Will start powershell from a command prompt, starting Start-LogShark to monitor directories on the computer "Comp0815". The standard configuration files for the template and the wrapper xml will be used.

### Example 2

```
.\Start-LogShark -Computername Comp0816  
-LogSharkConfigTemplate "c:\program files\logshark\enteoClient.lsc"  
-WrapperConfigFile "c:\program files\logshark\enteoWrapper.xml"  
-HoursBack 12 -KeepOpen True
```

Will start the applet from within powershell, starting to monitor directories on the computer "Comp0816". The configuration files given on the command line will be used. The tag "#HoursBack#" will be replaced by "12", the tag "KeepOpen" will be replaced by "True".