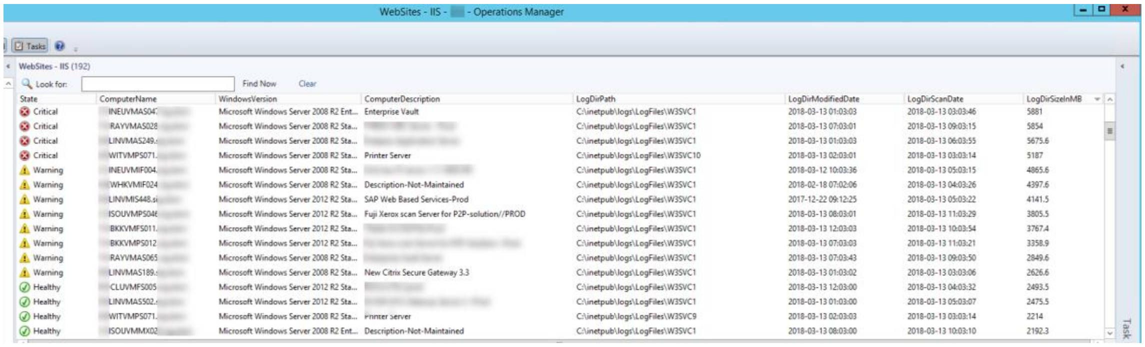
Monitoring Webservers’ Log directory size with SCOM

IIS, Apache and Tomcat can write log files. It happens not seldom that a webservice log directory occupies large space or even causes disk filling up.

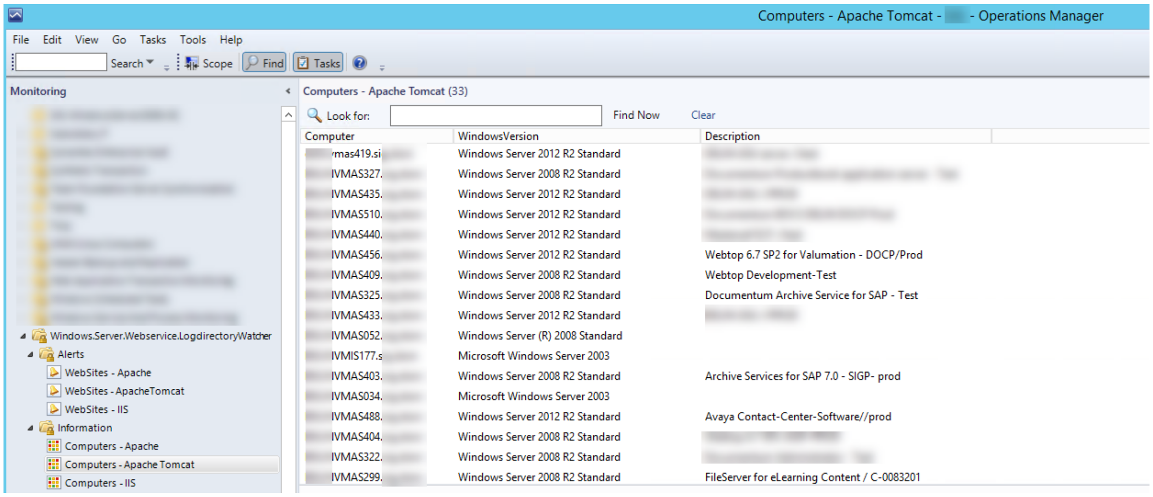
By default, a warning state occurs once 2.5 GB disk space is used by logs. An error state plus a message is thrown once more than 5 GB is taken.

Thresholds and alert behavior can be overridden as usual.



State	ComputerName	WindowsVersion	ComputerDescription	LogDirPath	LogDirModifiedDate	LogDirScanDate	LogDirSizeInMB
Critical	INEUVMAS047[redacted]	Microsoft Windows Server 2008 R2 Ent...	Enterprise Vault	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 01:03:03	2018-03-13 03:03:46	5881
Critical	RAYVMAS028[redacted]	Microsoft Windows Server 2008 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 07:03:01	2018-03-13 09:03:15	5854
Critical	LINVMAS249.[redacted]	Microsoft Windows Server 2008 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 01:03:03	2018-03-13 06:03:55	5675.6
Critical	WITVMPS071.[redacted]	Microsoft Windows Server 2008 R2 Sta...	Printer Server	C:\inetpub\logs\LogFiles\W3SVC10	2018-03-13 02:03:01	2018-03-13 03:03:14	5187
Warning	INEUVMIF004.[redacted]	Microsoft Windows Server 2008 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-12 10:03:36	2018-03-13 05:03:15	4865.6
Warning	WHKVMIF024[redacted]	Microsoft Windows Server 2008 R2 Sta...	Description-Not-Maintained	C:\inetpub\logs\LogFiles\W3SVC1	2018-02-18 07:02:06	2018-03-13 04:03:26	4397.6
Warning	LINVMIS448.si[redacted]	Microsoft Windows Server 2012 R2 Sta...	SAP Web Based Services-Prod	C:\inetpub\logs\LogFiles\W3SVC1	2017-12-22 09:12:25	2018-03-13 05:03:22	4141.5
Warning	ISOUVMPS046[redacted]	Microsoft Windows Server 2012 R2 Sta...	Fuji Xerox scan Server for P2P-solution//PROD	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 08:03:01	2018-03-13 11:03:29	3805.5
Warning	BKKVMFS011.[redacted]	Microsoft Windows Server 2012 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 12:03:03	2018-03-13 10:03:54	3767.4
Warning	BKKVMPS012[redacted]	Microsoft Windows Server 2012 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 07:03:03	2018-03-13 11:03:21	3358.9
Warning	RAYVMAS065[redacted]	Microsoft Windows Server 2008 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 07:03:43	2018-03-13 09:03:50	2849.6
Warning	LINVMAS189.[redacted]	Microsoft Windows Server 2008 R2 Sta...	New Citrix Secure Gateway 3.3	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 01:03:02	2018-03-13 03:03:06	2626.6
Healthy	CLUVMFS005[redacted]	Microsoft Windows Server 2012 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 12:03:00	2018-03-13 04:03:32	2493.5
Healthy	LINVMAS502.[redacted]	Microsoft Windows Server 2012 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 01:03:00	2018-03-13 05:03:07	2475.5
Healthy	WITVMPS071.[redacted]	Microsoft Windows Server 2008 R2 Sta...	Printer Server	C:\inetpub\logs\LogFiles\W3SVC9	2018-03-13 02:03:03	2018-03-13 03:03:14	2214
Healthy	ISOUVMMX02[redacted]	Microsoft Windows Server 2008 R2 Ent...	Description-Not-Maintained	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 08:03:00	2018-03-13 10:03:10	2192.3

Another positive site is effect is that you become aware on which machine web servers and in which version they are running.



Computer	WindowsVersion	Description
[redacted]mas419.si[redacted]	Windows Server 2012 R2 Standard	[redacted]
[redacted]IVMAS327.[redacted]	Windows Server 2008 R2 Standard	[redacted]
[redacted]IVMAS435.[redacted]	Windows Server 2012 R2 Standard	[redacted]
[redacted]IVMAS510.[redacted]	Windows Server 2012 R2 Standard	[redacted]
[redacted]IVMAS440.[redacted]	Windows Server 2012 R2 Standard	[redacted]
[redacted]IVMAS456.[redacted]	Windows Server 2012 R2 Standard	Webtop 6.7 SP2 for Valumation - DOCP/Prod
[redacted]IVMAS409.[redacted]	Windows Server 2008 R2 Standard	Webtop Development-Test
[redacted]IVMAS325.[redacted]	Windows Server 2008 R2 Standard	Documentum Archive Service for SAP - Test
[redacted]IVMAS433.[redacted]	Windows Server 2012 R2 Standard	[redacted]
[redacted]IVMAS052.[redacted]	Windows Server (R) 2008 Standard	
[redacted]IVMIS177.s[redacted]	Microsoft Windows Server 2003	
[redacted]IVMAS403.[redacted]	Windows Server 2008 R2 Standard	Archive Services for SAP 7.0 - SIGP- prod
[redacted]IVMAS034.[redacted]	Microsoft Windows Server 2003	
[redacted]IVMAS488.[redacted]	Windows Server 2012 R2 Standard	Avaya Contact-Center-Software//prod
[redacted]IVMAS404.[redacted]	Windows Server 2008 R2 Standard	[redacted]
[redacted]IVMAS322.[redacted]	Windows Server 2008 R2 Standard	[redacted]
[redacted]IVMAS299.[redacted]	Windows Server 2008 R2 Standard	FileServer for eLearning Content / C-0083201

Following lines explain the briefly the components of the management pack and the logic behind it. – To ensure the code also runs on Windows Server 2008 R2 it’s compatible to PowerShell version 2.

Change History

Date	Build No.	Changes
2018-03-13	1.0.0.114	Initial Upload to GitHub

Management Pack components

Classes

Everything in SCOM that has a Health State is an object. Instead of checking all Windows computers for the existing of those files and changing their health state (green/yellow/red) directly, a dedicated computer class is defined.

Webserver definition:

```
ID="Windows.Server.Webservice.LogdirectoryWatcher.Computer"
Base="Windows!Microsoft.Windows.ComputerRole"
Accessibility="Public" Abstract="true", Hosted="true" Singleton="false"

        ID="Windows.Server.Webservice.LogdirectoryWatcher.Computer.IIS"
        Base="Windows.Server.Webservice.LogdirectoryWatcher.Computer"
        Accessibility="Public" Abstract="false" Hosted="true" Singleton="false"

        ID="Windows.Server.Webservice.LogdirectoryWatcher.Computer.Apache"
        Base="Windows.Server.Webservice.LogdirectoryWatcher.Computer"
        Accessibility="Public" Abstract="false" Hosted="true" Singleton="false"

        ID="Windows.Server.Webservice.LogdirectoryWatcher.Computer.ApacheTomcat"
        Base="Windows.Server.Webservice.LogdirectoryWatcher.Computer"
        Accessibility="Public" Abstract="false" Hosted="true" Singleton="false"
```

Website log directory definition:

```
ID="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.Base" Base="System!System.LogicalEntity"
Accessibility="Public" Abstract="true" Hosted="false" Singleton="false"

        ID="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.IIS"
        Base="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.Base"
        Accessibility="Public" Abstract="false" Hosted="false" Singleton="false"

        ID="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.ApacheBase"
        Base="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.Base"
        Accessibility="Public" Abstract="true" Hosted="false" Singleton="false"

                ID="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.Apache"
                Base="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.ApacheBase"
                Accessibility="Public" Abstract="false" Hosted="false" Singleton="false"

                ID="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.ApacheTomcat"
                Base="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.ApacheBase"
                Accessibility="Public" Abstract="false" Hosted="false"
                Singleton="false"
```

Discoveries

The mechanism of finding objects that match the definition and storing it in the SCOM database is called discovery. There are different types of discoveries, starting from matching registry values over results of an WMI query to scripts that can cover everything. Targets define on which component the discovery shall run.

Finding webservers:

```
ID="Windows.Server.Webservice.LogdirectoryWatcher.Discovery.Windows.Server.Webservice.Computer.Apa
cheTomcat"
Target="Windows!Microsoft.Windows.Server.Computer"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.Computer.ApacheTomcat"
TypeID="Windows!Microsoft.Windows.FilteredRegistryDiscoveryProvider">

ID="Windows.Server.Webservice.LogdirectoryWatcher.Discovery.Windows.Server.Webservice.Computer.IIS
"
Target="Windows!Microsoft.Windows.Server.Computer"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.Computer.IIS”
TypeID="Windows!Microsoft.Windows.FilteredRegistryDiscoveryProvider"

ID="Windows.Server.Webservice.LogdirectoryWatcher.Discovery.Windows.Server.Webservice.Computer.Apa
che"
Target="Windows!Microsoft.Windows.Server.Computer"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.Computer.Apache"
TypeID="Windows!Microsoft.Windows.FilteredRegistryDiscoveryProvider">
```

Finding web sites log directories:

```
ID="Windows.Server.Webservice.LogdirectoryWatcher.Discovery.Windows.WebService.WebSite.Apache"
Target="Windows.Server.Webservice.LogdirectoryWatcher.Computer.Apache"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.Apache"
TypeID="SC!Microsoft.SystemCenter.HealthServiceShouldManageEntity"
TypeID="Windows!Microsoft.Windows.TimedPowerShell.DiscoveryProvider"

ID="Windows.Server.Webservice.LogdirectoryWatcher.Discovery.Windows.WebService.WebSite.IIS"
Target="Windows.Server.Webservice.LogdirectoryWatcher.Computer.IIS"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.IIS"
TypeID="SC!Microsoft.SystemCenter.HealthServiceShouldManageEntity"
TypeID="Windows!Microsoft.Windows.TimedPowerShell.DiscoveryProvider">

ID="Windows.Server.Webservice.LogdirectoryWatcher.Discovery.Windows.WebService.WebSite.ApacheTomca
t" Target="Windows.Server.Webservice.LogdirectoryWatcher.Computer.ApacheTomcat"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.ApacheTomcat"
TypeID="SC!Microsoft.SystemCenter.HealthServiceShouldManageEntity"
TypeID="Windows!Microsoft.Windows.TimedPowerShell.DiscoveryProvider"
```

Monitors

Monitors are for finding out which Health State an object has. – An object

Unit Monitors:

```
ID="Windows.Server.Webservice.LogdirectoryWatcher.Monitor.LogDirectorySize.ApacheTomcat"
Target="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.ApacheTomcat
ParentMonitorID="Health!System.Health.AvailabilityState"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.Monitor.ThreeState.Test.MonitorType"
AlertOnState Error
IntervalSeconds 600

ID="Windows.Server.Webservice.LogdirectoryWatcher.Monitor.LogDirectorySize.IIS"
Target="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.IIS"
ParentMonitorID="Health!System.Health.AvailabilityState"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.Monitor.ThreeState.Test.MonitorType"
AlertOnState Error
IntervalSeconds 600

ID="Windows.Server.Webservice.LogdirectoryWatcher.Monitor.LogDirectorySize.Apache"
Target="Windows.Server.Webservice.LogdirectoryWatcher.WebSite.Apache"
ParentMonitorID="Health!System.Health.AvailabilityState"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.Monitor.ThreeState.Test.MonitorType"
AlertOnState Error
IntervalSeconds 600
```

Custom momitor type

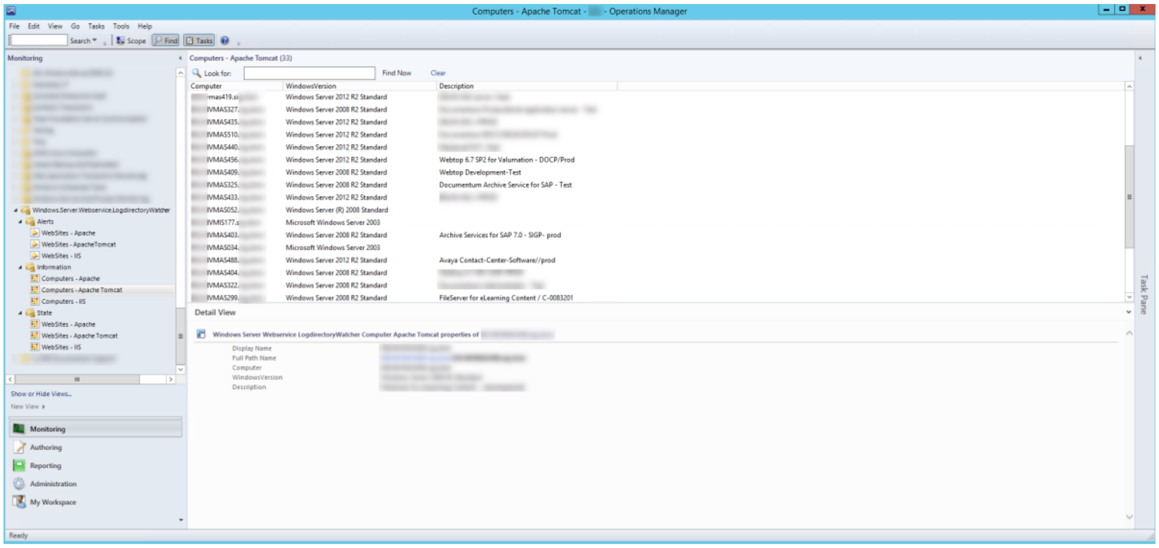
```
ID="Windows.Server.Webservice.LogdirectoryWatcher.Monitor.ThreeState.Test.MonitorType"

ID="DataSource"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.Monitor.ThreeState.Test.PropertyBag.Filtered
"
ID="Probe"
TypeID="Windows.Server.Webservice.LogdirectoryWatcher.Monitor.ThreeState.Probe"
```

Views

To make all discovered objects and their health state visible a state views are used.

State Views:

Showing discovered web servers plus some meta information.



Computers - Apache Tomcat (33)

Look for: Find Now Clear

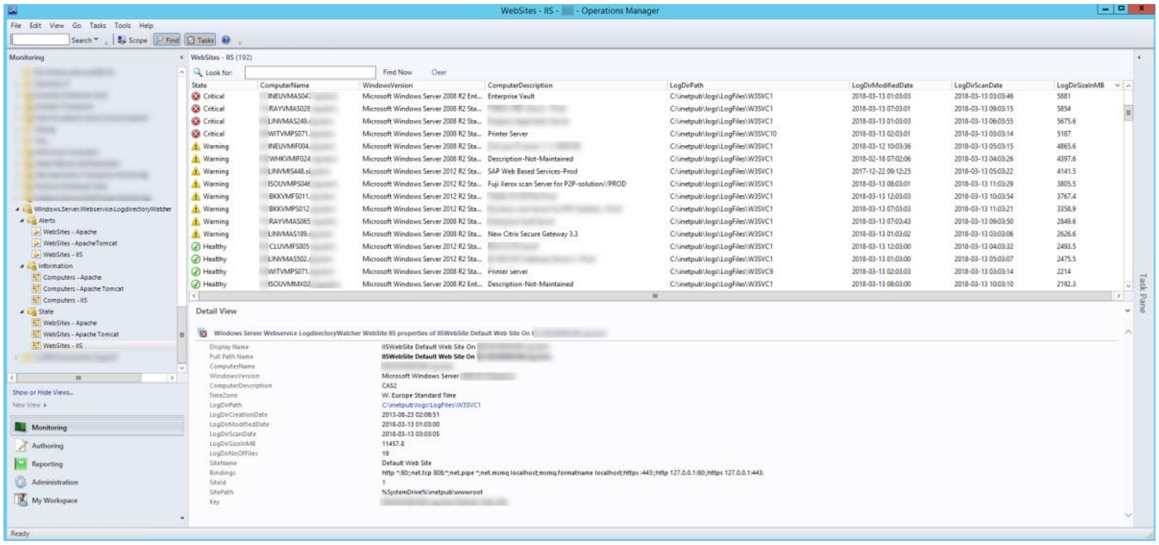
Computer	WindowsVersion	Description
[redacted]mas419.si[redacted]	Windows Server 2012 R2 Standard	[redacted]
[redacted]IVMAS327.[redacted]	Windows Server 2008 R2 Standard	[redacted]
[redacted]IVMAS435.[redacted]	Windows Server 2012 R2 Standard	[redacted]
[redacted]IVMAS510.[redacted]	Windows Server 2012 R2 Standard	[redacted]
[redacted]IVMAS440.[redacted]	Windows Server 2012 R2 Standard	[redacted]
[redacted]IVMAS456.[redacted]	Windows Server 2012 R2 Standard	Webtop 6.7 SP2 for Valumation - DOCP/Prod
[redacted]IVMAS409.[redacted]	Windows Server 2008 R2 Standard	Webtop Development-Test
[redacted]IVMAS325.[redacted]	Windows Server 2008 R2 Standard	Documentum Archive Service for SAP - Test
[redacted]IVMAS433.[redacted]	Windows Server 2012 R2 Standard	[redacted]
[redacted]IVMAS052.[redacted]	Windows Server (R) 2008 Standard	
[redacted]IVMIS177.s[redacted]	Microsoft Windows Server 2003	
[redacted]IVMAS403.[redacted]	Windows Server 2008 R2 Standard	Archive Services for SAP 7.0 - SIGP- prod
[redacted]IVMAS034.[redacted]	Microsoft Windows Server 2003	
[redacted]IVMAS488.[redacted]	Windows Server 2012 R2 Standard	Avaya Contact-Center-Software//prod
[redacted]IVMAS404.[redacted]	Windows Server 2008 R2 Standard	[redacted]
[redacted]IVMAS322.[redacted]	Windows Server 2008 R2 Standard	[redacted]
[redacted]IVMAS299.[redacted]	Windows Server 2008 R2 Standard	FileServer for eLearning Content / C-0083201

Detail View

Windows Server Webservice LogdirectoryWatcher Computer Apache Tomcat properties of [redacted]

Display Name	[redacted]
Full Path Name	[redacted]
Computer	[redacted]
WindowsVersion	[redacted]
Description	[redacted]

Showing discovered website log directory plus some additional information.



WebSites - IIS (192)

Look for: Find Now Clear

State	ComputerName	WindowsVersion	ComputerDescription	LogDirPath	LogDirModifiedDate	LogDirScanDate	LogDirSizeInMB
Critical	[redacted]INEUVMAS047[redacted]	Microsoft Windows Server 2008 R2 Ent...	Enterprise Vault	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 01:03:03	2018-03-13 03:03:46	5881
Critical	[redacted]RAYVMAS028[redacted]	Microsoft Windows Server 2008 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 07:03:01	2018-03-13 09:03:15	5854
Critical	[redacted]LINVMAS249.[redacted]	Microsoft Windows Server 2008 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 01:03:03	2018-03-13 06:03:55	5675.6
Critical	[redacted]WITVMPS071.[redacted]	Microsoft Windows Server 2008 R2 Sta...	Printer Server	C:\inetpub\logs\LogFiles\W3SVC10	2018-03-13 02:03:01	2018-03-13 03:03:14	5187
Warning	[redacted]INEUVMIF004.[redacted]	Microsoft Windows Server 2008 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-12 10:03:36	2018-03-13 05:03:15	4865.6
Warning	[redacted]WHKVMIF024[redacted]	Microsoft Windows Server 2008 R2 Sta...	Description-Not-Maintained	C:\inetpub\logs\LogFiles\W3SVC1	2018-02-18 07:02:06	2018-03-13 04:03:26	4397.6
Warning	[redacted]LINVMIS448.si[redacted]	Microsoft Windows Server 2012 R2 Sta...	SAP Web Based Services-Prod	C:\inetpub\logs\LogFiles\W3SVC1	2017-12-22 09:12:25	2018-03-13 05:03:22	4141.5
Warning	[redacted]ISOUVMPS046[redacted]	Microsoft Windows Server 2012 R2 Sta...	Fuji Xerox scan Server for P2P-solution//PROD	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 08:03:01	2018-03-13 11:03:29	3805.5
Warning	[redacted]BKKVMFS011.[redacted]	Microsoft Windows Server 2012 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 12:03:03	2018-03-13 10:03:54	3767.4
Warning	[redacted]BKKVMPS012[redacted]	Microsoft Windows Server 2012 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 07:03:03	2018-03-13 11:03:21	3358.9
Warning	[redacted]RAYVMAS065[redacted]	Microsoft Windows Server 2008 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 07:03:43	2018-03-13 09:03:50	2849.6
Warning	[redacted]LINVMAS189.[redacted]	Microsoft Windows Server 2008 R2 Sta...	New Citrix Secure Gateway 3.3	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 01:03:02	2018-03-13 03:03:06	2626.6
Healthy	[redacted]CLUVMFS005[redacted]	Microsoft Windows Server 2012 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 12:03:00	2018-03-13 04:03:32	2493.5
Healthy	[redacted]LINVMAS502.[redacted]	Microsoft Windows Server 2012 R2 Sta...	[redacted]	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 01:03:00	2018-03-13 05:03:07	2475.5
Healthy	[redacted]WITVMPS071.[redacted]	Microsoft Windows Server 2008 R2 Sta...	Printer Server	C:\inetpub\logs\LogFiles\W3SVC9	2018-03-13 02:03:03	2018-03-13 03:03:14	2214
Healthy	[redacted]ISOUVMMX02[redacted]	Microsoft Windows Server 2008 R2 Ent...	Description-Not-Maintained	C:\inetpub\logs\LogFiles\W3SVC1	2018-03-13 08:03:00	2018-03-13 10:03:10	2192.3

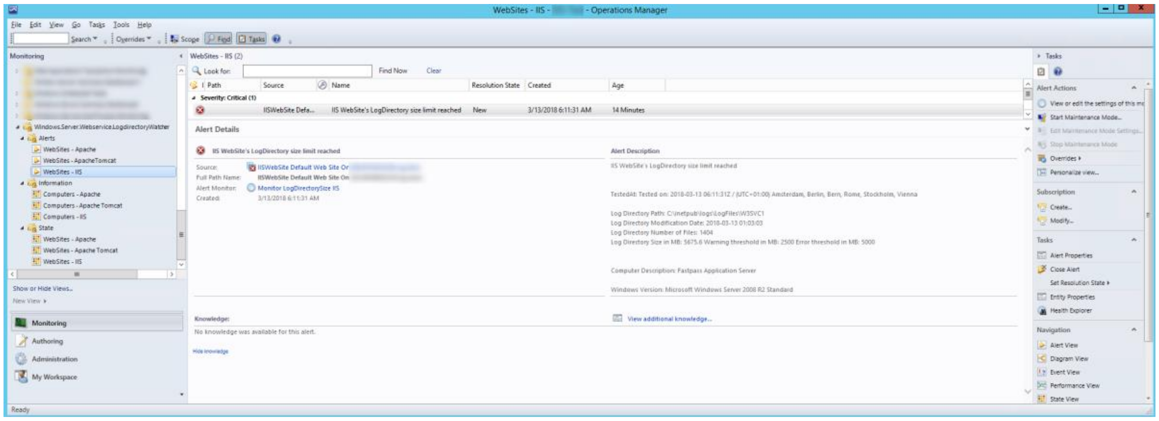
Detail View

Windows Server Webservice LogdirectoryWatcher WebSite IIS properties of IISWebSite Default Web Site On [redacted]

Display Name	IISWebSite Default Web Site On [redacted]
Full Path Name	**IISWebSite Default Web Site On** [redacted]
ComputerName	[redacted]
WindowsVersion	Microsoft Windows Server [redacted]
ComputerDescription	CAS2
TimeZone	W. Europe Standard Time
LogDirPath	C:\inetpub\logs\LogFiles\W3SVC1
LogDirCreationDate	2013-08-23 02:08:51
LogDirModifiedDate	2018-03-13 01:03:00
LogDirScanDate	2018-03-13 03:03:05
LogDirSizeInMB	11457.8
LogDirNoOfFiles	19
SiteName	Default Web Site
Bindings	http *:80:;net.tcp 808:*;net.pipe *;net.msmq localhost;msmq.formatname localhost;https :443:;http 127.0.0.1:80:;https 127.0.0.1:443:
SiteId	1
SitePath	%SystemDrive%\inetpub\wwwroot
Key	[redacted]

Alert Views:

Alerts of website log directories’ which size exceeds the thresholds.



Path	Source	Name	Resolution State	Created	Age
Severity: Critical (1)					
	IISWebSite Defa...	IIS WebSite's LogDirectory size limit reached	New	3/13/2018 6:11:31 AM	14 Minutes

Alert Details

IIS WebSite's LogDirectory size limit reached

Source: IISWebSite Default Web Site On [redacted]
Full Path Name: IISWebSite Default Web Site On [redacted]
Alert Monitor: Monitor LogDirectorySize IIS
Created: 3/13/2018 6:11:31 AM

Alert Description

IIS WebSite's LogDirectory size limit reached

TestedAt: Tested on: 2018-03-13 06:11:31Z / (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Log Directory Path: C:\inetpub\logs\LogFiles\W3SVC1
Log Directory Modification Date: 2018-03-13 01:03:03
Log Directory Number of Files: 1404
Log Directory Size in MB: 5675.6 Warning threshold in MB: 2500 Error threshold in MB: 5000

Computer Description: Fastpass Application Server

Windows Version: Microsoft Windows Server 2008 R2 Standard

Knowledge:

No knowledge was available for this alert.

View additional knowledge...

Hide knowledge