

Windows Services Sensor

Introduction

This article should help you to configure a *Windows Services Sensor* and should guide you through different possibilities this sensor has.

Configure

Before you start the configuration, please make sure that you cover the following requirements:

- **Activate remote Powershell settings on the target host (issue the following commands in the powershell console of a target)**

```
Enable-PSRemoting -force
```

```
set-item -force WSMan:\localhost\Service\Auth\Basic $true
```

```
set-item -force WSMan:\localhost\Client\AllowUnencrypted $true
```

```
set-item -force WSMan:\localhost\Service\AllowUnencrypted $true
```

- Make sure that you have an **Account** which is member of the local Administrator Group of the Target-Host (no need to be a Domain Admin!)
- **TCP Port 5985** (and 5986) needs to be opened between GreenLight and Target-Host

Authentication Profile

We recommend to create an authentication profile in the Communication Section which you then assign later on to a single or multiple Nodes.

This account needs to have local Admin privileges on the target host (as mentioned above)

Authentication Profile

Profile Name

Username *

Password *

Protocol

Port

Communication

- Mail Profile
- Notification
- Sametime
- SNMP Profile
- Network A
- Authentication

Server Settings

Now, let's start with the configuration of Windows Services on the Node Level

- Open a Server and select *Windows*. In addition to that please select *OS Services and Statistics*

Edit Server / Network Device

Edit Server / Network Device

Step 1 of 6: Connection Settings

Host Name / IP * 10.10.50.20

Operating System

Windows

☒ OS Services and Statistics

☐ Domino Server

- Next, assign the profile which you have created before

Edit Server / Network Device

Edit Server / Network Device

Step 3 of 6: Windows Server Settings

Basic Configuration Services Performance Counter

Authentication Profile [Profile Name] 5985] (ID: [ID] ▼

Override Profile Settings ☐

Username * [Username]

- On the next Page, Open the *Services* Tab

Click the *Load Services* button in order to retrieve all Windows Services from the host

Whenever the items are loaded successfully, just drag&drop those which you want to monitor to the right side of the window

Edit Server / Network Device

Edit Server / Network Device

Step 3 of 6: Windows Server Settings

Basic Configuration
Services
Performance Counter

Services last refreshed on: 07.06.2016 15:13
Load Services...

Available Items

Filter ...

Service Name	Shortname
Application Information	Appinfo
Application Layer Gateway Se	ALG
Application Management	AppMgmt
Background Intelligent Transf	BITS
Base Filtering Engine	BFE
CNG Key Isolation	KeyIso
COM+ Event System	EventSystem
COM+ System Application	COMSysApp
Certificate Propagation	CertPropSvc

Selected Items

Filter ...

Service	Shortname
Application Experience	AeLookupSvc
DNS Client	Dnscache

< Back

Next >

- Save / Close the Server settings

Sensor Settings

Let's create a Windows Services Sensor from the Sensor Template list.

- On the *Settings* Tab, leave *Use node settings*

So all services which you have marked as monitored services will be covered by the server. This allows you to use a single sensor for monitoring different hosts with different windows services

3

Monitoring Configuration

Sensor Settings

✚

Name

Enabled ☒

Settings

Targets Actions Schedule

Monitoring Settings

Select Services

Services

- As an action you can create the following

Sensor Action Settings

Notification in GreenLight

Step 1 of 2: Alert Condition

Name

Conditions

Advanced Options Timeframe Options

☒ Run this action when ...

Services Stopped Count

☐ Run this action when ...

Sensor Action Settings

Notification in GreenLight

Step 2 of 2: Notification Message

Type Failure ☐ Send Status Reset Message ☐ Override Message Text

Message

Templates Custom ...

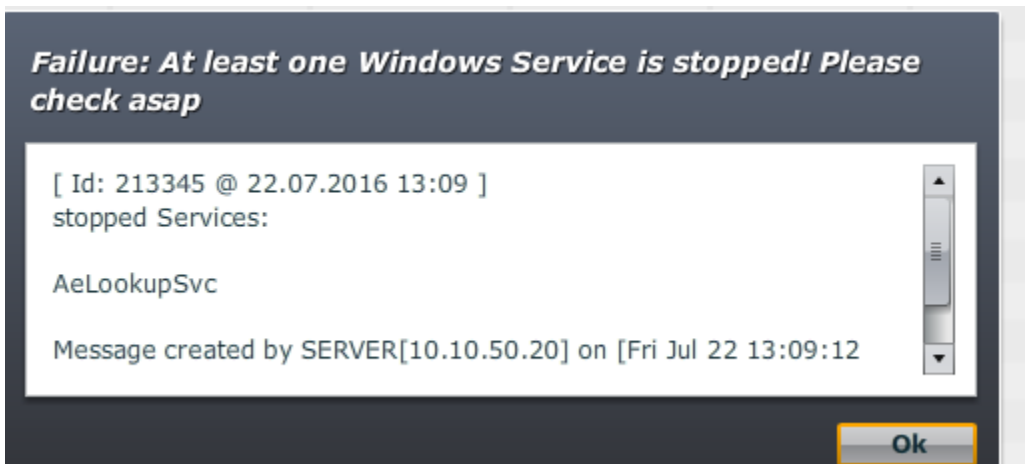
Short Text At least one Windows Service is stopped! Please check asap

Text stopped Services:
`${result.details['greenlight.osservice.stopped']}`





















Copy/paste: `${result.details['greenlight.osservice.stopped']}`

Result

The result is a notification like this



The Key/Value pairs you get from this Sensor is the following

Measurement Details			Statistics	
List View ▼			Favorites Only <input type="checkbox"/>	
★	Key	Value		
★	 greenlight.osservice.missing			
★	 greenlight.osservice.missing_count	0		
★	 greenlight.osservice.monitored	AeLookupSvc,Dnscache		
★	 greenlight.osservice.monitored_count	2		
★	 greenlight.osservice.running	Dnscache		
★	 greenlight.osservice.running_count	1		
★	 greenlight.osservice.service.AeLookupSvc.display_name	Application Experience		
★	 greenlight.osservice.service.AeLookupSvc.running	1		
★	 greenlight.osservice.service.AeLookupSvc.started	0		
★	 greenlight.osservice.service.AeLookupSvc.status	0		
★	 greenlight.osservice.service.AeLookupSvc.status_name	OK		
★	 greenlight.osservice.service.Dnscache.display_name	DNS Client		
★	 greenlight.osservice.service.Dnscache.running	1		
★	 greenlight.osservice.service.Dnscache.started	1		
★	 greenlight.osservice.service.Dnscache.status	0		
★	 greenlight.osservice.service.Dnscache.status_name	OK		
★	 greenlight.osservice.started	Dnscache		
★	 greenlight.osservice.started_count	1		
★	 greenlight.osservice.stopped	AeLookupSvc		
★	 greenlight.osservice.stopped_count	1		