

Log-Parser protokollieren

Schnellstartanleitung

Version R9

Deutsch

März 19, 2015

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at

http://<u>www.kaseya.com</u>/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Inhalt

1
2
3
4
10
11
13
14
17

Einführung

Der VSA kann die aus zahlreichen Standardprotokolldateien gesammelten Daten überwachen. **Protokoll-Monitoring** erweitert diese Fähigkeit noch weiter, indem Daten von der Ausgabe einer beliebigen textbasierten Protokolldatei extrahiert werden können. Beispiele hierfür sind Anwendungsprotokolldateien und syslog-Dateien, die für Unix-, Linux- und Apple-Betriebssysteme und für Netzwerkgeräte wie etwa Cisco-Router erstellt wurden. Damit nicht alle in diesen Protokollen enthaltenen Daten in die Kaseya Server-Datenbank hochgeladen werden, verwendet die **Protokoll-Monitoring** Analysedefinitionen und Analysesätze zum Analysieren jeder Protokolldatei und wählt nur diejenigen Daten aus, an denen Sie interessiert sind. Analysierte Nachrichten werden im Protokoll-Monitoring angezeigt, das Sie über die Registerkarte "Agent-Protokolle" der Seite Live Connect > Agent-Daten oder Rechnerübersicht oder durch Generieren eines Berichts über die Seite Agent > Protokolle > Protokoll-Monitoring aufrufen können. Benutzer können wahlweise beim Generieren eines **Protokoll-Monitoring**-Datensatzes Meldungen auslösen, laut Definition mit Analysesätze zuweisen oder Analyseübersicht.

Analysedefinitionen und Analysesätze

Bei der Konfiguration des Protokoll-Monitoring ist es hilfreich, zwischen zwei Arten von Konfigurationsdatensätzen zu unterscheiden: Analysedefinitionen und Analysesätze.

Eine Analysedefinition wird für Folgendes verwendet:

- Ermitteln der zu analysierenden Protokolldatei
- Auswählen der Protokolldaten basierend auf dem Format der Protokolldaten, laut Angabe in einer Vorlage
- Ausfüllen der Parameter mit Protokolldatenwerten
- Wahlweise Formatierung des Protokolleintrags in Protokoll-Monitoring

Mit einem Analysesatz werden die ausgewählten Daten anschließend *gefiltert*. Basierend auf den *Werten* der ausgefüllten Parameter und der definierten Kriterien kann ein Analysesatz Protokoll-Monitoring-Einträge generieren und optional Meldungen auslösen.

Falls durch den Analysesatz keine Filterung stattfinden würde, würde die Kaseya Server-Datenbank in kürzester Zeit stark anwachsen. Ein Protokolldateiparameter namens \$FileServerCapacity\$ würde beispielsweise wiederholt mit dem aktuellen Prozentsatz des freien Speicherplatzes auf einem Dateiserver aktualisiert werden. Bis dieser freie Speicherplatz jedoch auf unter 20 % fällt, braucht dies nicht im Protokoll-Monitoring aufgezeichnet zu werden und es braucht auch keine Meldung basierend auf diesem Schwellenwert ausgelöst zu werden. Jeder Analysesatz gilt nur für die Analysesätze erstellt werden. Jeder Analysesatz kann einen separaten Alarm auf jeder Rechner-ID auslösen, der er zugewiesen wurde.

Schritt 1: Neue Protokollanalysedefinition erstellen

m 7 km 💼 🔹	Machine ID: *	Q Apply Machine Grou	ip: < All Groups >	View: < No View >	🕑 🥒 Edit 🥁 Reset
	Go to: < Select Page >	Show 10	2 machines		
	Configure log file m	nanagement. Assign I	og parsers to machin	es	
Monitor		Log File P	arser		
	Apply	New < Select L	og Parser >	*	
Dashboard	Clear	Edit			
Dashboard List	Clear All	Click New butt	on to create new Log Pa	arser	
Dashboard Settings	Clear All	Adefinition.			
Status	Select All				
Alarm Summary	Unselect All Machin	ne.Group ID	File Parser	Path	Archive Path
Suspend Alarm	😳 🔲 🛛 win0d.r	oot.kserver			
Live Counter	🚯 🔲 🛛 xp17.ro	ot.unnamed			
Edit					
Monitor Lists					
Update Lists By Scan					
Monitor Sets					
SNMP Sets					
Add SNMP Object					
Agent Monitoring					
Alerts					
SNMP Traps Alert					
- Assign Monitoring					
Monitor Log					
External Monitoring					
System Check					
SNMP Monitoring					
- LAN Watch					
- Assign SNMP					
- SNMP Log					
Set SNMP Values					
Set SNMP Type					
🖃 Log Monitoring					
Parser Summary					
- Log Parser					
Assign Parser Sets					

Gehen Sie zur Registerkarte Monitor in VSA. Wählen Sie Protokollanalyse unter Protokollkontrolle. Klicken Sie auf Neu, um eine neue Definition der Protokollanalysedefinition zu erstellen.

Schritt 2: Analysenamen und Protokolldateipfad eingeben

Log File Parser	Definition	Clos
Save		
Parser Name	SysLog Parser	
Log File Path	c:\logs\message.log	
Log Archive Path		
Description		
Template	Multi-line Template	
Output Template		-
	~	
L		2

Geben Sie die folgenden Angaben ein:

Analysename - Der Name dieser Protokollanalysedefinition.

Protokolldateipfad – Der vollständige Pfad der zu verarbeitenden Protokolldatei. Der Agent muss in der Lage sein, auf diesen Pfad zuzugreifen. Die Protokolldatei sollte formatierte Protokolleinträge enthalten. Unicode-Dateien werden noch nicht unterstützt. Beispiel: c:\logs\message.log.

Hinweis: Das Sternchen (*) kann als Platzhalterzeichen im Dateinamen verwendet werden. In diesem Fall wird die aktuellste Datei verarbeitet. Beispiel: c:\logs\message*.log.

Klicken Sie nach der Eingabe des Analysenamens und des Protokolldateipfads auf **Speichern**. In dem Fenster werden jetzt auch die Parameterdefinitionen angezeigt.

Optionale Informationen

Protokollarchivpfad – Die Protokollanalyse prüft periodisch auf Änderungen in der Zielprotokolldatei. Die Protokolleinträge können in verschiedenen Archivdateien archiviert werden, bevor die Protokollanalyse diese Einträge verarbeiten kann. Sie können den Archivdateipfad im Feld des Protokollarchivpfads angeben. Beispiel: Wird message.log täglich in einer Datei im Format messageYYYYMMDD.log archiviert, so können Sie c:\logs\message*.log als Protokollarchivpfad angeben. Die Protokollanalyse kann die zuletzt verarbeitete Datei ermitteln, da sie ein Lesezeichen für die Protokolldatei speichert.

Beschreibung – Die Detailbeschreibung der Protokollanalyse.

Schritt 3: Vorlagen angeben und Parameter definieren

Vorlage

Anhand dieser Vorlage können Sie die Eingabe mit dem Protokolleintrag in der Protokolldatei vergleichen, um die erforderlichen Daten in Parameter zu extrahieren. Parameter sind in der Vorlage in \$-Zeichen eingeschlossen. Es ist wichtig, Text um die Parameter einzugeben, damit die Parameter leicht unterschieden werden können. Die Zeichen im Protokolleintrag werden unter Berücksichtigung der Groß-/Kleinschreibung mit der Vorlage verglichen.

Einzeilige Vorlage zur Analyse eines einzeiligen Protokolleintrags – Die Vorlage enthält nur einen einzeiligen Eintrag, und die Protokolldatei wird Zeile für Zeile verarbeitet.

Mehrzeilige Vorlage zur Analyse mehrzeiliger Protokolleinträge – Die Vorlage enthält mehrzeilige Einträge, und die Protokolldatei wird in Blöcken von Zeilen, die durch eine Zeilenbegrenzung abgegrenzt sind, verarbeitet.

Hinweis: Die Zeichenfolge {tab} kann als Tabstoppzeichen und die Zeichenfolge {n1} als Zeilenumbruch verwendet werden. {n1}kann nicht in einer einzeiligen Vorlage verwendet werden. %kann als Platzhalterzeichen verwendet werden.

Tipp: Es ist einfacher, den Protokolleintrag zu kopieren und in das Bearbeitungsfeld **Vorlage** einzufügen und die erforderlichen durch Parameternamen zu ersetzen, als eine Protokolleintragsvorlage von Grund auf neu zu erstellen.

Ausgabevorlage

Dies ist ein optionales Feld. Es kann zum Formatieren der Nachricht verwendet werden, wenn der Protokolleintrag in der Datenbank gespeichert wird. Andernfalls wird der Protokolleintrag selbst als die Nachricht in der Datenbank gespeichert.

Protokolldateiparameter

Nachdem Sie die Vorlage erstellt haben, müssen Sie die Liste der Parameter definieren, die von der Vorlage verwendet werden. Alle Parameter in der Liste müssen definiert werden, andernfalls gibt die Analyse einen Fehler zurück. Verfügbare Parameter sind *integer, unsigned integer, long, unsigned long, float, double, datetime, string.* Die Länge des Parameternamens ist auf 32 Zeichen beschränkt.

Datum-/Zeit-Format-Zeichenfolge

Die Vorlagenzeichenfolge kann ein Datums- und Zeitformat verwenden, anhand dessen die Datumsund Zeitinformationen in Protokolleinträgen analysiert werden. Beispiel: TT.MM.JJJJ hh:mm:ss Formate:

- yy, yyyy, YY, YYYY Jahresangabe mit zwei oder vier Ziffern
- M Monatsangabe mit einer oder zwei Ziffern
- MM Monatsangabe mit einer Ziffer
- MMM Abkürzung der Monatsbezeichnung, z. B. Jan
- MMMM Vollständige Monatsbezeichnung, z. B. "Januar"
- D, d Tagesangabe mit einer oder zwei Ziffern
- DD, dd Tagesangabe mit zwei Ziffern
- DDD, ddd Abkürzung der Bezeichnung des Wochentags, z. B. Mo
- DDDD, dddd Vollständige Bezeichnung des Wochentags, z. B. "Montag"
- H, h Stundenangabe mit einer oder zwei Ziffern
- HH, hh Stundenangabe mit zwei Ziffern

- m Minutenangabe mit einer oder zwei Ziffern
- mm Minutenangabe mit zwei Ziffern
- s Sekundenangabe mit einer oder zwei Ziffern
- ss Sekundenangabe mit zwei Ziffern
- f Sekundenbruchteilangabe mit einer oder zwei Ziffern
- ff ffffffff Zwei bis neun Ziffern
- t Tageszeitmarkierung mit einem Zeichen, z. B. "a"
- tt Tageszeitmarkierung mit zwei Zeichen, z. B. "am"

Hinweis: Jeder Datums-/Zeitparameter muss mindestens Daten für Monat, Tag, Stunde und Sekunden enthalten. Der Wert des Parameters \$Time\$ wird als Ereigniszeit verwendet, sofern er angegeben wurde. Andernfalls wird der Zeitpunkt, zu dem der Eintrag verarbeitet wurde, als Ereigniszeit in der Datenbank verwendet.

Beispiel 1 - Einzeiliger Protokolleintrag

Beginnen Sie mit einem typischen Protokolleintrag aus der Protokolldatei, die Sie überwachen möchten:

<189> 2009 Aug 31 06:57:48 (FVS114-ba-b3-d2) 71.121.128.42 ICMP Packet[Destination Unreachable] - Source:192.168.0.186 - Destination:192.168.0.1 - [Receive]

Identifizieren Sie die Teile des Protokolleintrags, in die Sie Parameter einfügen möchten:

<<u>189</u>> <u>2009 Aug 31 06:57:48</u> (FVS114-ba-b3-d2) 71.121.128.42 ICMP Packet[Destination Unreachable] - Source:<u>192.168.0.186</u> - Destination:<u>192.168.0.1</u> - [Receive]

Ersetzen Sie in der Vorlage den unterstrichenen Text durch Parameter:

<\$code\$> \$Time\$ (\$device\$) \$HostName\$ \$PackType\$ Packet[\$Action\$] - Source:\$SrcAddr\$ - Destination:\$DestAddr\$ - \$Msg\$

Protokolldateiparameter

Hinweis: Klicken Sie mindestens einmal auf die Schaltfläche Speichern, um den Bereich Protokolldateiparameter des Dialogfelds anzuzeigen.

Text, der nicht zum Ausfüllen mit Parametern verwendet wird, muss dem Text im Protokolleintrag entsprechen. Zum Beispiel: Die Zeichenfolge " muss dem Text im Protokolleintrag entsprechen, einschließlich des Leerzeichens vor dem Bindestrich.

Definieren Sie die Parameter:

Parametername	Parametertyp	Analyseergebnis
Code	Ganzzahl	189
Zeit	Datum/Zeit im Format "JJJJ MMM JJ hh:mm:ss", nicht UTC	2006-11-08 11:57:48
device	String	FVS114-ba-b3-d2
HostName	String	71.121.128.42
PackType	String	ICMP
Aktion	String	Destination Unreachable
SrcAddr	String	192.168.0.186
DestAddr	String	192.168.0.1
Msg	String	[Receive]

Schritt 3: Vorlagen angeben und Parameter definieren

Log File Parser De	finition			Close
Save Sav	e As Delete Shar	re Click to set the	access rights for the Log Parser	
Parser Name	SysLog Parser			
Log File Path	c:\logs\message.log			
Log Archive Path				
Description				
Template 🔲 Mu	Iti-line Template			
<\$code\$> \$Time Destination:\$E	2\$ (\$device\$) \$HostNam DestAddr\$ - \$Msg\$	ne\$ \$PackType\$ P	Packet[\$Action\$] - Source:\$SrcAddr\$ -	~
Output Template				
				~
				~
Log File Paramete	ers			
Apply C	lear All			
Name				
Type < Select Par	rameter Type > 🔽			
Name		Туре	Date Format	UTC
≻ 🖹 code		Integer		
🔀 🗐 Time		Date Time	YYYY MMM DD hh:mm:ss	
🔀 🖾 device		String		
🔀 🗐 HostName		String		
🔀 🗐 PackType		String		
🔀 🖻 Action		String		
🔀 🖻 SrcAddr		String		
≻ 🖹 DestAddr		String		
🗡 🗐 Msg		String		

Beispiel 2 – Einschließlich des Symbols % (Platzhalterzeichen)

Beginnen Sie mit einem typischen Protokolleintrag aus der Protokolldatei, die Sie überwachen möchten:

```
<189> 2009 Aug 31 06:57:48 (FVS114-ba-b3-d2) 71.121.128.42 ICMP Packet[Destination Unreachable] - Source:192.168.0.186 - Destination:192.168.0.1 - [Receive]
```

Identifizieren Sie unnötigen Text in der Protokolldatei, die Sie überwachen möchten:

```
<<u>189</u>> <u>2009 Aug 31 06:57:48</u> (FVS114-ba-b3-d2) <u>71.121.128.42</u> ICMP Packet[Destination
Unreachable] - Source:<u>192.168.0.186</u> - Destination:<u>192.168.0.1</u> - [Receive]
```

Ersetzen Sie in der Vorlage den nicht benötigten, durchgestrichenen Text durch ein Prozentzeichen (%) als Stellvertreterzeichen. Ersetzen Sie anderen Text durch Parameter:

<\$code\$> \$Time\$ % \$HostName\$ \$PackType\$ Packet% Source:\$SrcAddr\$ Destination:\$DestAddr\$ -

Definieren Sie die Parameter:

Parametername	Parametertyp	Analyseergebnis
Code	Ganzzahl	189
Zeit	Datetime im Format YYYY MMM DD hh:mm:ss	2006-11-08 11:57:48

HostName	String	71.121.128.42
PackType	String	ICMP
SrcAddr	String	192.168.0.186
DestAddr	String	192.168.0.1

Beispiel 3 - Mehrzeilige Protokolleinträge

Beginnen Sie mit einem typischen mehrzeiligen Protokolleintrag aus der Protokolldatei, die Sie überwachen möchten:

Identifizieren Sie den Text, der ignoriert werden soll, und den Text, der mit Parametern ausgefüllt werden soll.

Summary Of This Scan

Ersetzen Sie in der Vorlage den durchgestrichenen Text durch ein Prozentzeichen (%) als Stellvertreterzeichen. Ersetzen Sie den unterstrichenen Text durch Parameter:

Summary Of This Scan %scanning time:\$ScanTime\$ %scanned:\$Scanned\$ %identified:\$Identified\$ %ignored:\$Ignored\$ %critical objects:\$Critical\$ Definieren Sie die Parameter:

Parametername	Parametertyp	Analyseergebnis
ScanTime	String	00:02:32.765
Scanned	Ganzzahl	91445
Identified	Ganzzahl	0
Ignoriert	Ganzzahl	0
Kritisch	Ganzzahl	0

Schritt 3: Vorlagen angeben und Parameter definieren

Log File Parser	Definition			Close
Save	ave As Delete]		
Parser Name	Ad-Aware Results Sum	imary		
Log File Path	c:\Logs\ad-aware log.b	đ		
Log Archive Path				
Description				
Description	A del Kara Tarandata			
Template 🗹	viuiti-line Template		-	
Summary Of T	his Scan%scanning anned\$	g time:\$ScanTime\$,	Â
%identified:	\$Identified\$			E
<pre>%ignored:\$Ig</pre>	nored\$			
%critical ob	jects:\$Critical\$			-
Output Template				
				^
				-
Log File Param	eters			
Apply	Clear All			
Name				
Type < Select F	arameter Type > 💌			
Name		Туре	Date Format	UTC
× 🖹 ScanTime		String		
× 🖹 Scanned		Integer		
🗡 🗐 Identified		Integer		
× Ignored		Integer		
× ≊ Critical		Integer		
•				,
Done		6	Internet Protected Mode: Off	🔍 100% 🔻

Beispiel 4 – Ausgabevorlage

Beginnen Sie mit einem typischen mehrzeiligen Protokolleintrag aus der Protokolldatei, die Sie abrufen möchten:

Die obigen Daten werden als Textkörper der Nachricht im Kontrollprotokoll aufgezeichnet, falls keine Ausgabevorlage angegeben wurde. Es folgt ein Beispiel der Ausgabe in der Protokollkontrolle ohne Angabe einer Ausgabevorlage:

Sele	ect Log Log Monit	oring	•	Ad-Aware Results Summ 🔻	Events per Page	30	•
Star	t Date :	8	1	Refresh			
End	Date :	8	1	Log Record Count: 6			
dell	-dim9200.unnan	ned					
<<	9:18:03 am 13-May	-08	-	>>			
	Time	Message					
9:18	:03 am 13-May-0	8 Summary	Of Th	iis Scan			
		>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	****	*****	9 X		
		Total scan	ning	time:00:02:32.765			
		Objects so	canne	ed:91445			
		Objects id	entifie	ed:U			
		Objects ig	nored	1:0			
		New critica	ai obj	ects:U			
		Scanili	ne: u	10:02:32.765			
		Scanne	a: 91	445			
		Identifie	ea: U				
		Gritiaal	. 0				
		Critical					

Geben Sie in der Ausgabevorlage eine Ausgabe durch Verwendung vordefinierter Parameter an: Total \$Scanned\$ objects are scanned in \$ScanTime\$. Found object: \$Identified\$ identified, \$Ignored\$ ignored, and \$Critical\$ critical.

Es folgt ein Beispiel der Ausgabe in der Protokollkontrolle nach Angabe einer Ausgabevorlage:

Select Log	Log Monitoring	▼ A	d-Aware Results Summ 👻	Events per Page	30 👻	
Start Date :	9	(Refresh			
End Date :	8	L	og Record Count: 7			
dell-dim92	00.unnamed					-
9:36:17	' am 13-May-08	-	>>			
Tin	ne Message					
9:36:17 am	13-May-08 Total 91445 ScanTim	object e: 00:	ts are scanned in 00:02:32 	2.765. Found object:	: 0 identif	fied, 0 ignored, and 0 critical.
	Scanned	I: 9144	5			
	Identifie	d:0				
	lanored	0				

Schritt 4: Protokollanalysedefinition zuweisen

Eine abgeschlossen Protokolldatei-Analysedefinition muss mithilfe der Funktion **Protokollanalyse** einer oder mehreren Rechner-IDs zugewiesen werden. Wählen Sie die Rechner-IDs aus, auf die die Definition angewendet werden soll, und klicken Sie auf **Anwenden**. Dies bedeutet, dass die Analysedefinition von den ausgewählten Rechnern verwendet werden kann. Die Analyse findet jedoch erst dann statt, wenn Sie die Filterkriterien für die gesammelten Protokolldaten auswählen und ihnen Alarmbedingungen zuweisen, wie in den Schritten 5 und 6 beschrieben.

田?吟首 »	Machine ID: *	Q Apply Machine Group	All Groups > View	v: < No View > 💉 🖋 Edit	Reset
	Go to: < Select Page >	🗙 < > Show 10 💌	2 machines		
Monitor	Configure log file m	anagement. Assign lo	g parsers to machines		
	Apply	Log File Pa	rser		
•		New SysLog Par	ser	~	
Dashboard	Clear Click	Apply button to assign se	lected log file		
··· Dashboard List	Clear All parse	to all selected Machine	IDs.		
Dashboard Settings		Aud Log Parser	C Replace Log Parsers		
Status	Select All Machin	o Group ID	Eile Darsor	Path	Archivo Path
- Alarm Summary		ie.Group ID	File Parser	Paul	Archive Paul
- Suspend Alarm	Winua.r	oot.kserver	No. I. D		
Live Counter	💟 🗹 xp17.ro	ot.unnamed	SysLog Parser	c:\logs\message.log	
🖃 Edit					
Monitor Lists					
Update Lists By Scan					
Monitor Sets					
SNMP Sets					
Add SNMP Object					
Agent Monitoring					
Alerts					
- SNMP Traps Alert					
- Assign Monitoring					
Monitor Log					
External Monitoring					
System Check					
SNMP Monitoring					
LAN Watch					
Assign SNMP					
SNMP Log					
Set SNMP Values					
Set SNMP Type					
E Log Monitoring					
Parser Summary					
Log Parser					
Assign Parser Sets					

Schritt 5: Sammlungs- und Alarmbedingungen definieren

Klicken Sie auf **Analysesätze zuweisen** unter **Protokollkontrolle** in der Funktionsliste. Wählen Sie die Protokollanalysedefinition aus der Dropdown-Liste **Protokollanalyse auswählen**. Wählen Sie dann <<u>New</u> **Parser Sets** aus der Drop-down-Liste **Parser-Sets definieren** aus. *Ein Log-Parser-Set ist ein Satz von Bedingungen, der für die Analyse eines Protokolleintrags erfüllt sein muss, damit dieser in das "Protokoll-Monitoring-Protokoll" aufgenommen und optional eine Benachrichtigung dafür erstellt wird.* Auf diese Weise wird sichergestellt, dass nur relevante Protokolleinträge in das

"Protokoll-Monitoring-Protokoll" aufgenommen werden. Beachten Sie, dass ein Protokollanalysesatz spezifisch für eine Protokollanalyse ist. Sie könnten mehrere Protokollanalysesätze für die gleiche Protokollanalyse definieren und für jeden Protokollanalysesatz einen anderen Satz von Alarmen auslösen.



Definieren Sie die Alarmbedingungen. Im folgenden Beispiel wird ein Eintrag im "Protokoll-Monitoring-Protokoll" erstellt, wenn ein Protokolleintrag analysiert wird, sodass der Parameter Action den Text Unreachable enthält.

Parser S	Set Definition				Close			
	Parser Set Name							
Renar	me Check Action				Delete			
Add	Parser Column Action	Operator - Contain	s -	Parameter Filter Unreachable				
No Log File Filters defined								
No alerts will be generated until Logs Filters are added.								

Operatoren für Parameter

- String begins with, does not begin with, contains, does not contain, ends with, does not end with, equals, does not equal
- Numerisch equal, not equal, over, under
- Zeit equal, not equal, over, under

Der Parameterfilter für Time kann eines der folgenden Formate aufweisen. Eine Filterzeichenfolge, die auf Z endet, weist auf eine UTC-Zeit hin.

- YYYY-MM-DDThh:mm.ss
- YYYY/MM/DDThh:mm.ss
- YYYY-MM-DD hh:mm.ss
- YYYY/MM/DD hh:mm.ss
- YYYY-MM-DDThh:mm.ssZ
- YYYY/MM/DDThh:mm.ssZ
- YYYY-MM-DD hh:mm.ssZ
- YYYY/MM/DD hh:mm.ssZ

Beispiel: 2008-04-01 15:30:00.00

Analysesätze und Bedingungen

Die Bedingungen werden in einem Analysesatz definiert. Sie können einem Analysesatz mehrere Bedingungen zuweisen. Sie können auch einer Protokollanalyse mehrere Analysesätze zuweisen. Ein Protokolleintrag muss alle Bedingungen in einem Analysesatz erfüllen, damit eine Datensammlung bzw. ein Alarm ausgelöst wird. Dieses Verhalten unterscheidet sich von Ereignisprotokollalarmen und anderen Monitorsets. Zum Beispiel:

Protokollinhalt:

```
05/09/2008 12:21:34 192.168.0.1 error "lookup failed"
05/09/2008 12:21:35 192.168.0.1 error "syslog stopped"
05/09/2008 12:21:37 192.168.0.1 information "syslog starts"
05/09/2008 12:21:38 192.168.0.2 warning "ping failed"
05/09/2008 12:22:04 192.168.0.2 warning "unknown message"
```

Einzeilige Vorlage:

\$Time\$ \$hostname\$ \$errortype\$ \$message\$

Um Einträge zu erfassen, die eine der folgenden Bedingungen erfüllen, müssen Sie zwei Analysesätze definieren und sie beide der Protokollanalyse zuweisen:

\$errortype\$ is "error"

\$errortype\$ is "warning" AND \$message\$ contains "failed"

Es folgen die entsprechenden Bildschirmabbildungen für diese beiden Analysesätze:

Parser Set	Definition			Close
Rename	Parser Set Name Error			Delete
Add e	arser Column errortype 👻	Operator <select opera'="" td="" ▼<=""><td>Parameter Filter</td><td></td></select>	Parameter Filter	
Edit er	rrortype	Equal	error	×
Parser Set	Definition			Close
Parser Set	Definition Parser Set Name			<u>Close</u>
Parser Set Rename	Definition Parser Set Name Failure			Close Delete
Parser Set Rename Add n	Definition Parser Set Name Failure arser Column nessage	Operator <select opera'="" td="" ▼<=""><td>Parameter Filter</td><td><u>Close</u> Delete</td></select>	Parameter Filter	<u>Close</u> Delete
Parser Set Rename Add n Edit er	Definition Parser Set Name Failure arser Column nessage v rortype	Operator <select opera'="" ▼<br="">Equal</select>	Parameter Filter warning	Close Delete
Parser Set Rename Pa Add n Edit er Edit m	Definition Parser Set Name Failure arser Column nessage rortype essage	Operator <select opera'="" ▼<br="">Equal Contains</select>	Parameter Filter warning failed	Close Delete X

Schritt 6: Analysesatz zuweisen

Wählen Sie eine Rechner-ID, Alarmoptionen und Arten von Alarmen aus und klicken Sie anschließend auf **Anwenden**, um den Protokollanalysesatz einer Rechner-ID zuzuweisen. Sobald die Rechner-ID die Protokollanalysedefinition erhält, beginnt der Agent auf dem verwalteten Rechner mit der Analyse der Protokolldatei, *wann immer die Protokolldatei aktualisiert wird*.

Benachrichtigung

Der Agent erfasst Protokolleinträge und erstellt einen Eintrag im "Protokoll-Monitoring"-Protokoll, basierend auf den im Analysesatz definierten Kriterien, *egal, ob irgendwelche Benachrichtigungsmethoden aktiviert sind oder nicht.* Sie brauchen nicht jedes Mal benachrichtigt zu werden, wenn ein neuer Protokoll-Monitoring-Eintrag erstellt wird. Sie können einfach nach Bedarf das "Protokoll-Monitoring"-Protokoll überprüfen.



Schritt 7: Das "Protokoll-Monitoring-Protokoll" überprüfen

Protokoll-Monitoring-Einträge werden in **Protokoll-Monitoring** angezeigt, die Sie folgendermaßen aufrufen können:

- Agents > Agent-Protokolle > Protokoll-Monitoring > (Analysedefinition)
- Live Connect > Agent-Daten > Agent-Protokolle > Protokoll-Monitoring > (Analysedefinition) Live Connect kann durch Klicken auf das Check-in-Statussymbol einer ausgewählten Rechner-ID angezeigt werden.
- Inventarisierung > Rechnerübersicht > Registerkarte Agent-Protokolle > Protokoll-Monitoring > (Analysedefinition). Die Rechnerübersichtsseite kann auch durch *Alt-Klicken* auf das Check-in-Statussymbol einer ausgewählten Rechner-ID angezeigt werden.
- Der Bericht Info Center > Reporting > Berichte > Monitor Protokolle > Protokoll-Monitoring.

Diese Beispielbilder zeigen den Parameter \$Time\$, der für Protokollkontrolleinträge verwendet wird. Die Datums- und Uhrzeitfilterung in Ansichten und Berichten basiert auf der Uhrzeit des Protokolleintrags. Bei Einschluss eines Parameters \$Time\$ mit dem Datentyp Date Time in Ihre Vorlage verwendet das Protokoll-Monitoring die im Parameter \$Time\$ gespeicherte Zeit als Uhrzeit des Protokolleintrags. Falls kein Parameter \$Time\$ in Ihre Vorlage eingeschlossen ist, dient die Zeit, zu der der Eintrag in das Protokoll-Monitoring hinzugefügt wurde, als Uhrzeit des Protokolleintrags. Wählen Sie unbedingt einen Datumsbereich, für den Protokolleintragsdaten angezeigt werden.

Agent Go to: < Select Page > V < > Show 10 V 2 machines Win0d root.kserver Select Log Log Monitoring V SysLog Parser V Events per Page 30 V Machine Status Start Date: 8/31/2009 T Refresh End Date : 9/4/2009 T Log Record Count: 1
Agent win0d.root.kserver xp17.root.unnamed Select Log Log Monitoring SysLog Parser Events per Page 30 V Start Date: 8/31/2009 E Refresh End Date : 9/4/2009 E Log Record Count: 1
Machine Status
Start Date 8/3 1/2009 Refresh Imachine Status End Date : 9/4/2009 Imachine Status
Machine Status End Date : 9/4/2009 End Date : 9/4/2009 Log Record Count: 1
Agent Status xp17.root.unnamed
Agent Logs 6:57:48 am 31-Aug-09 >>
- Log History Time Message
Event Log Settings 6:57:48 am 31-Aug-09 <189> 2009 Aug 31 06:57:48 (FVS114-ba-b3-d2) 71.121.128.42 ICMP Packet
Destination Unreachable - Source: 192, 168, 0, 186 - Destination: 192, 168, 0, 1 -
- Deploy Agents [Receive] code: 199
- Create code: 103 device: FVS114-ba-b3-d2
HostName: 71.121.128.42
Rename PackType: ICMP
- Change Group Action: Destination Unreachable
Link Viscovery SrcAddr: 192.168.0136
Lak Walch Deskdout, 132, 100,01
nisturayons mog. process
View AD Computers
View AD Users
View vPro
Configure Agents
- Copy Settings
- Import Export
- Suspend
- Agent Menu
- Check-in Control
- Temp Directory
- Edit Profile
- Portal Access
□ Set Credential
Upgrade Version
└ Update Agent

Im Gegensatz hierzu basieren die Alarmdaten auf dem Datum, an dem der Alarm erstellt wurde, und nicht auf dem Datum der Einträge im Protkoll-Monitoring-Protokoll.

四?脸凰 »	Machine ID:	Q Apply Machine Group: < All	Groups > 🗸 🗸	View: < No	View >	🖌 🧷 Edit 🥁 Reset		
	Go to: < Select Page >	✓ < > Show 10 ✓ 2 m	nachines					
Monitor	Alarm State:	Open 🗸	(Update		Alarm Filters		
 ⇒ Dashboard ⇒ Dashboard List > Dashboard Settings ⇒ Status > Alarm Summary > Suspend Alarm > Live Counter ⇒ Edit → Monitor Lists > Update Lists By Scan → Monitor Sets > SNMP Sets > Add SNMP Object ⇒ Add SNMP Object ⇒ SNMP Traps Alert > Assign Monitoring → Monitor Log ⇒ SNMP Traps Alert > SNMP Traps Alert > SNMP Monitoring → LAN Watch > Assign SNMP > SNMP Values > Set SNMP Type ⇒ Log Monitoring → Parser Summary > Log Parser > Assign Parser Sets 	Alarm State: Notes: Oelete <	Open Machine.Group ID xp17.root.unnamed [xp17.root.unnamed] SysL essage: SysLog Parser log parser ge (FVS114-ba-b3-d2) 71.121.1 The following parameter crite Action Contain Unreachable:	State Al Open 10 .og Parser log par nerated an alert on 2 28.42 ICMP Packet[D vria was met: Value = Destination	Iarm Date 0:22:30 am 4 rser generate xp17.root.unna Destination Unre Unreachable	Alarm ID: Monitor Type: Alarm State: Alarm Type: Alarm Text: Filter Alarm C 4-Sep-09 Log I ed an alert med, the followin; eachable] - Source	Alarm Filters Alarm Filters Alarm Filters All Types > All States > All States > All Types > Ount: 1 Ticket Monitoring processing. glog entry occurred: <189x e: 192.168.0.186 - Destination	Name > 2009 Aug 30 oon:192.168.0.1	10:53:48 - [Receive]

Inhaltsverzeichnis

Ε

Einführung • 1

S

Schritt 1 Neue Protokollanalysedefinition erstellen • 2 Schritt 2 Analysenamen und Protokolldateipfad eingeben • 3 Schritt 3 Vorlagen angeben und Parameter definieren • 4 Schritt 4 Protokollanalysedefinition zuweisen • 10 Schritt 5 Sammlungs- und Alarmbedingungen definieren • 11 Schritt 6 Analysesatz zuweisen • 13 Schritt 7 Das "Protokoll-Monitoring-Protokoll" überprüfen • 14