Kaseya 2

Log-Parser protokollieren

Benutzerhandbuch

Versión R8

Deutsch

Oktober 23, 2014

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://www.kaseya.com/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

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**.

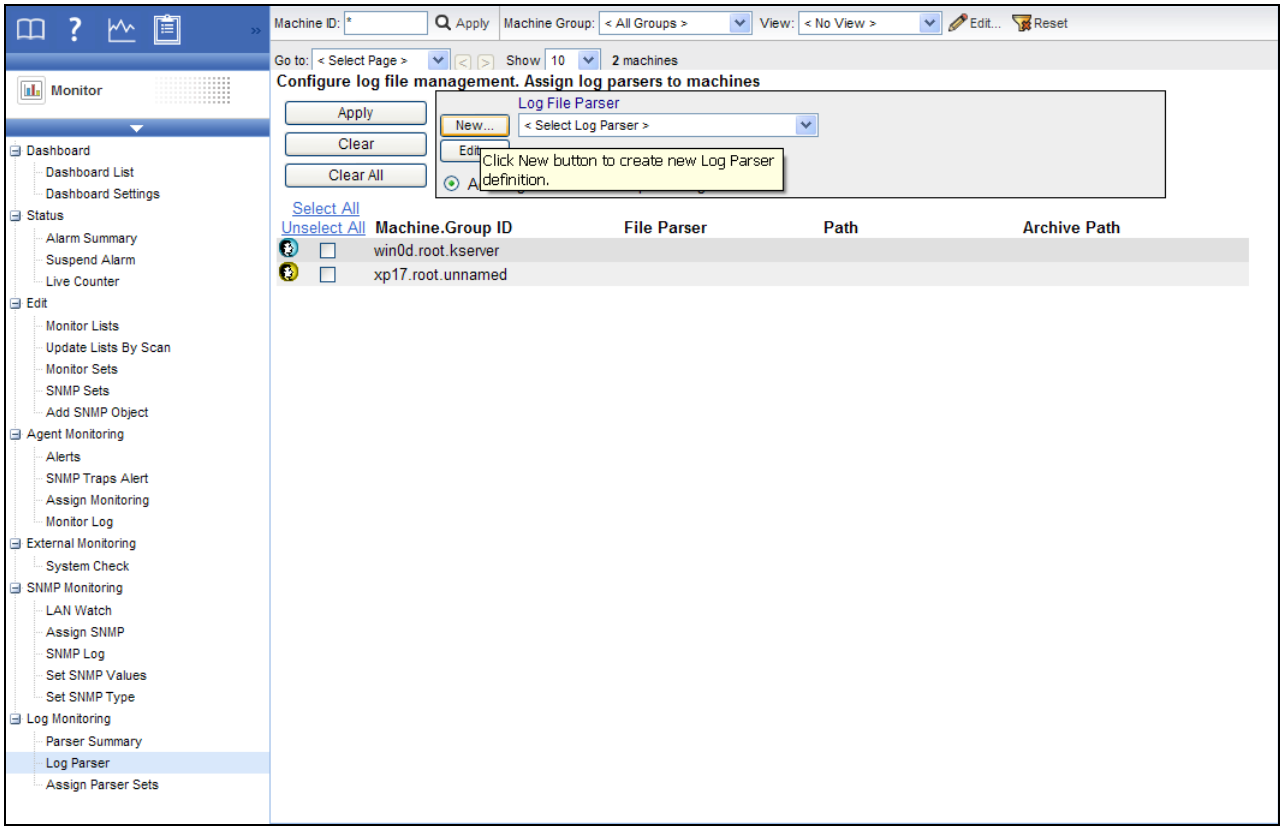
Eine **Analysedefinition** wird für Folgendes verwendet:

- 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.

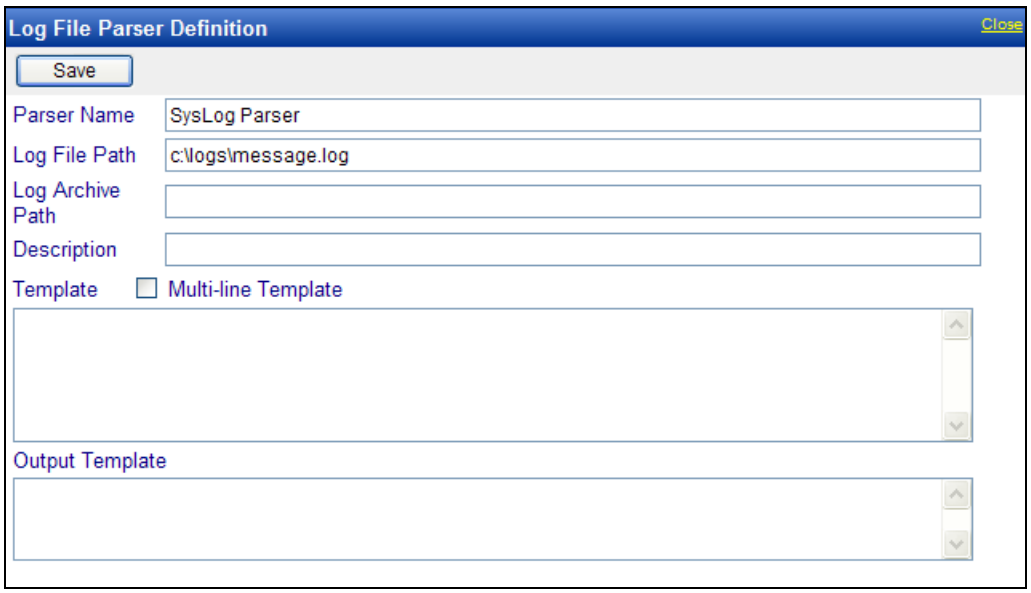
Falls durch den Analysesatz keine Filterung stattfinden würde, würde die Kaseya Server-Datenbank in kürzester Zeit stark anwachsen. Ein Protokolldateiparameter namens $FileServerCapacity$ würde beispielsweise wiederholt mit dem aktuellen Prozentsatz des freien Speicherplatzes auf einem Dateiserver aktualisiert 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 Analysedefinition, für deren Filterung er erstellt wurde. Für jede Analysedefinition können mehrere Analysesätze erstellt werden. Jeder Analysesatz kann einen separaten Alarm auf jeder Rechner-ID auslösen, der er zugewiesen wurde.

Schritt 1: Neue Protokollanalysedefinition erstellen



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



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 `{nl}` als Zeilenumbruch verwendet werden. `{nl}`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 Datums- und 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` – fffffffff – 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:

```
<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]
```

Ersetzen Sie in der Vorlage den unterstrichenen Text durch Parameter:

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

Protokolldateiparameter

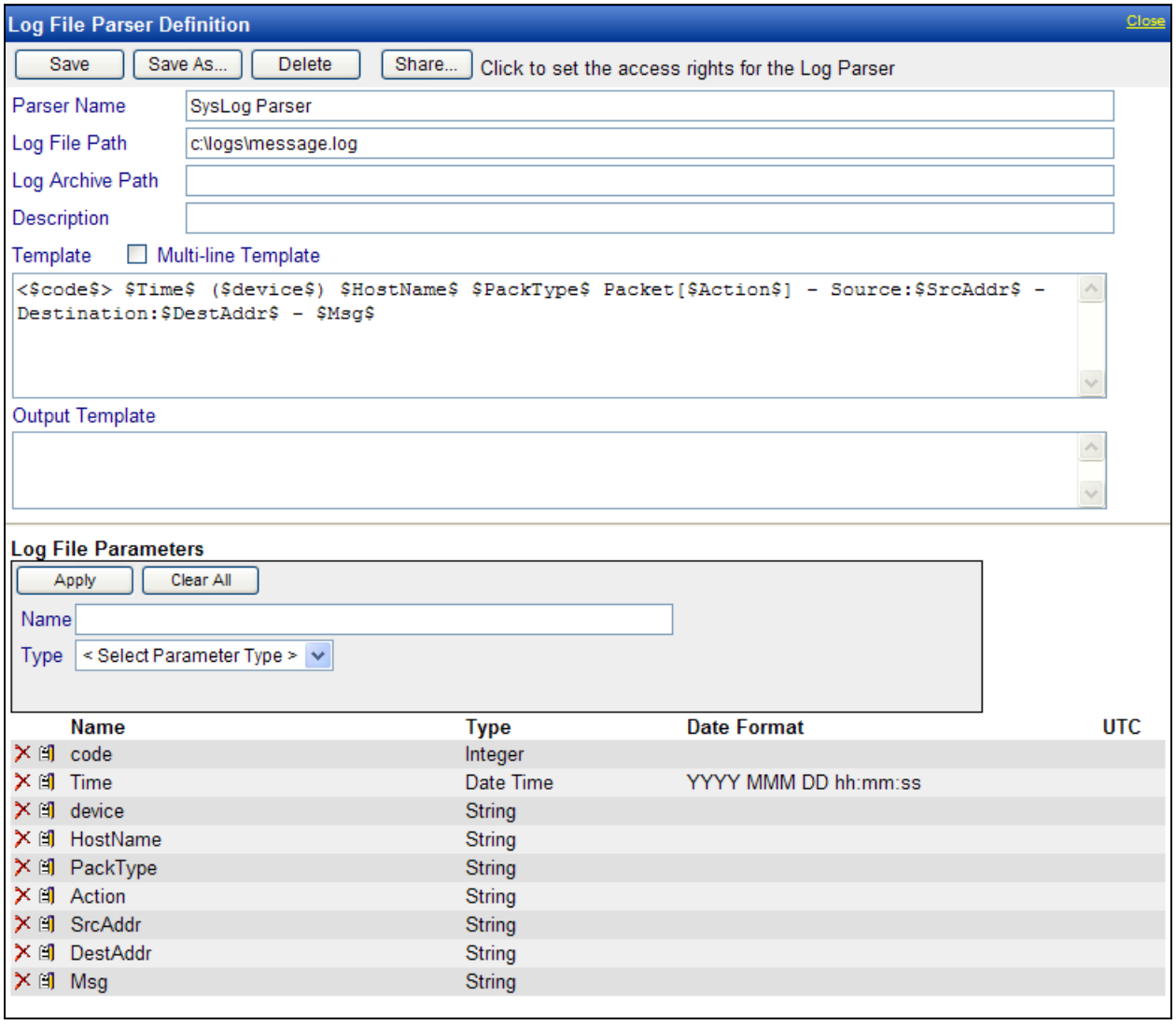
Hinweis: Klicken Sie mindestens einmal auf die Schaltfläche **Speichern**, um den Bereich **Protokolldateiparameter** des Dialogfelds anzuzeigen.

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



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:

```
<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]
```

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:

```
Summary Of This Scan
»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»
Total scanning time:00:02:32.765
Objects scanned:91445
Objects identified:0
Objects ignored:0
New critical objects:0
```

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

```
Summary Of This Scan
»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»
Total scanning time:00:02:32.765
Objects scanned:91445
Objects identified:0
Objects ignored:0
New critical objects:0
```

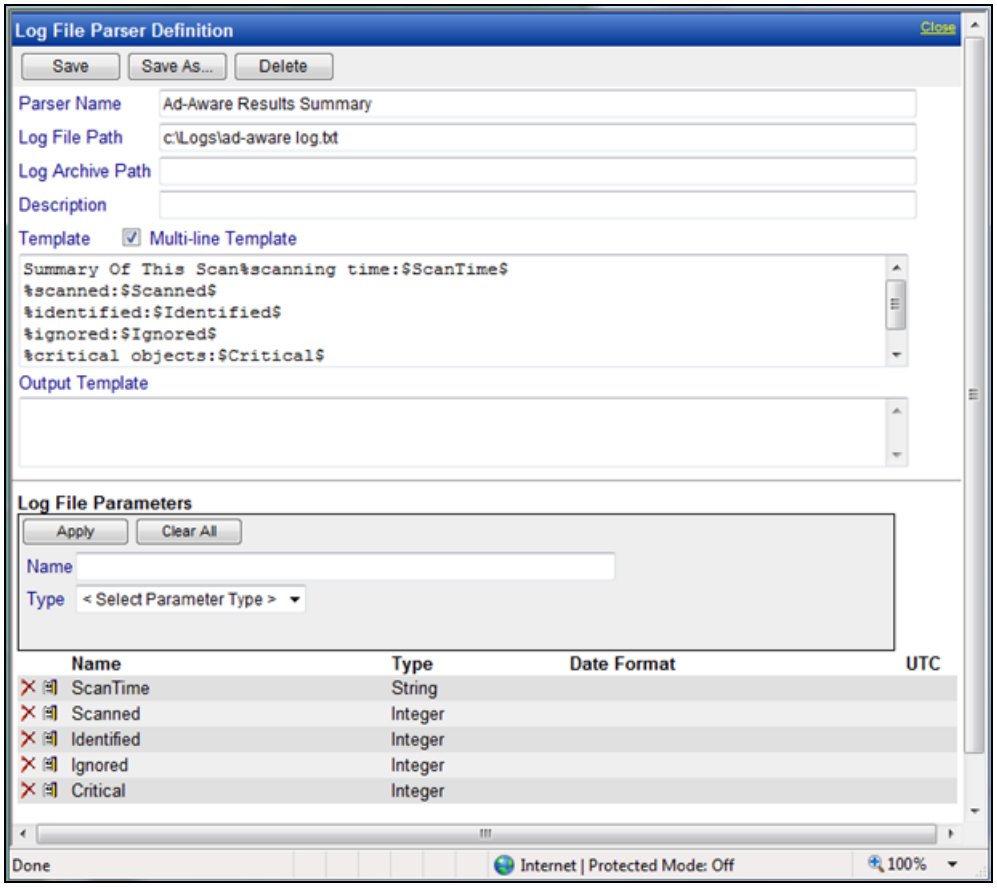
Ersetzen Sie in der Vorlage den durchgestrichenen Text durch ein Prozentzeichen (%) als Stellvertreterzeichen. Ersetzen Sie den unterstrichenen Text durch Parameter:

```
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

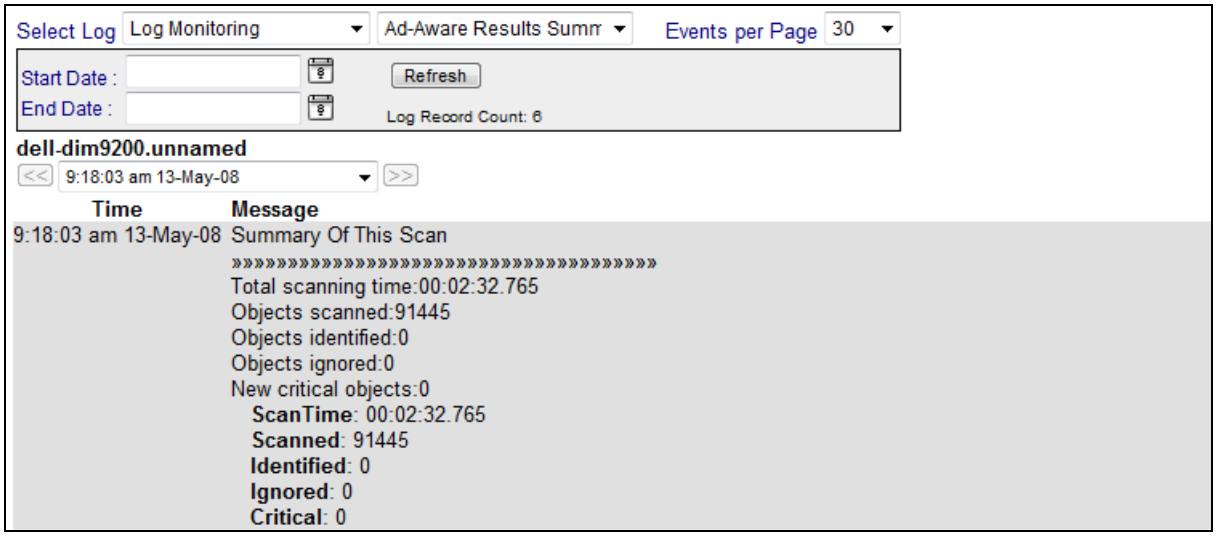


Beispiel 4 – Ausgabevorlage

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

```
Summary Of This Scan
»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»
Total scanning time:00:02:32.765
Objects scanned:91445
Objects identified:0
Objects ignored:0
New critical objects:0
```

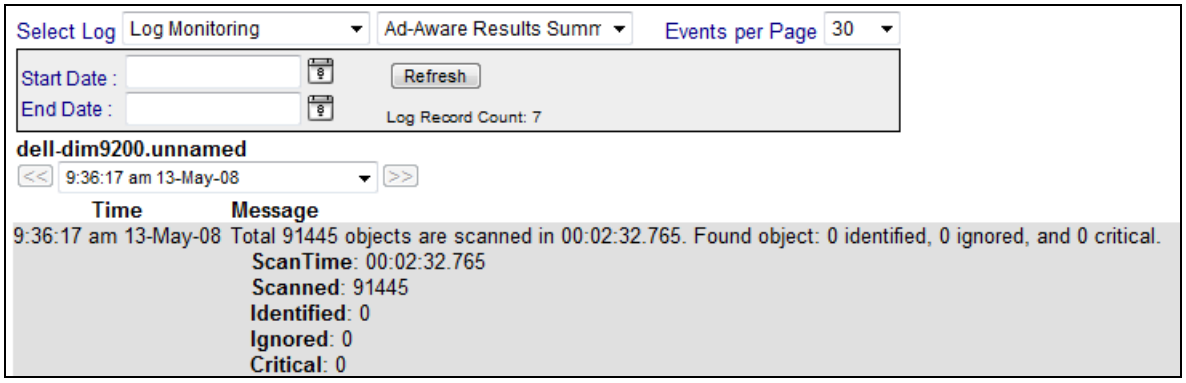
Die obigen Daten werden als Textkörper der Nachricht im Kontrollprotokoll aufgezeichnet, falls keine Ausgabevorlage angegeben wurde. Es folgt ein Beispiel der Ausgabe in der Protokollkontrolle ohne Angabe einer Ausgabevorlage:



Geben Sie in der Ausgabevorlage eine Ausgabe durch Verwendung vordefinierter Parameter an:

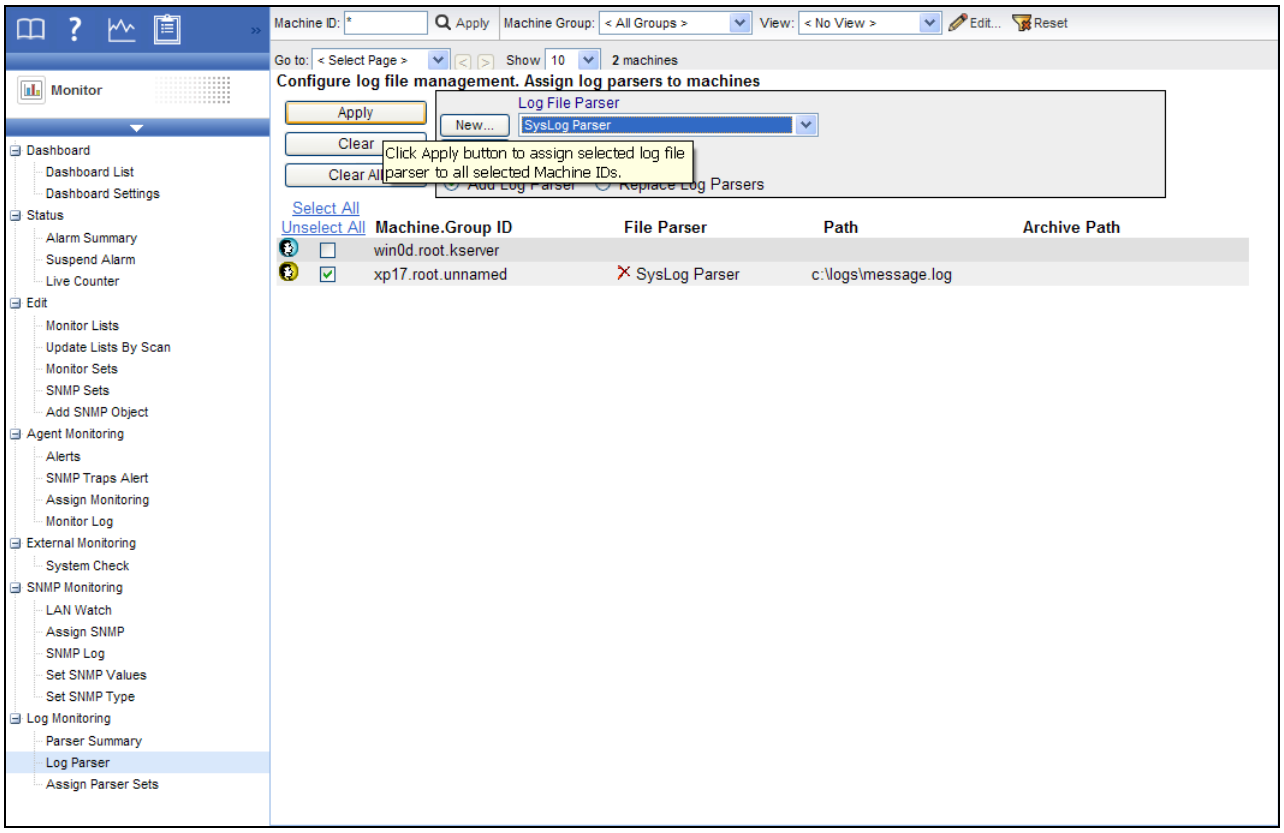
```
Total $Scanned$ objects are scanned in $ScanTime$. Found object: $Identified$
identified, $Ignored$ ignored, and $Critical$ critical.
```

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



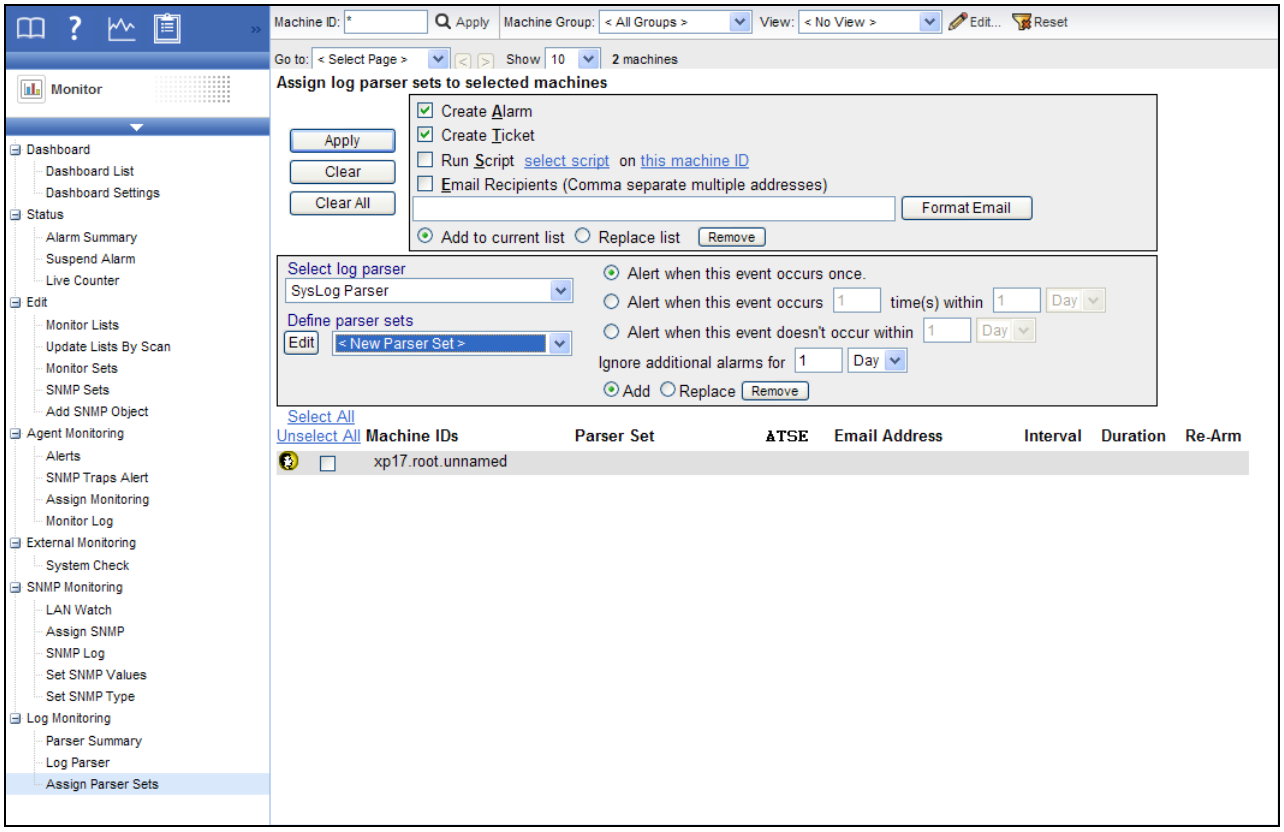
Schritt 4: Protokollanalysedefinition zuweisen

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.

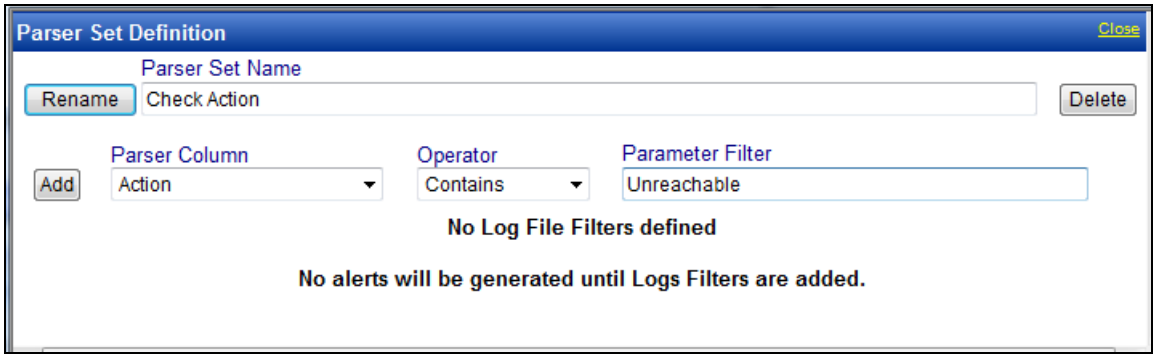


Schritt 5: Sammlungs- und Alarmbedingungen definieren

Klicken Sie auf **Analysesätze zuweisen** unter **Protokollkontrolle** in der Funktionsliste. Wählen Sie die Protokollanalysedefinition aus der Dropdown-Liste **Protokollanalyse auswählen**. Wählen Sie dann `<New 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.



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"
```

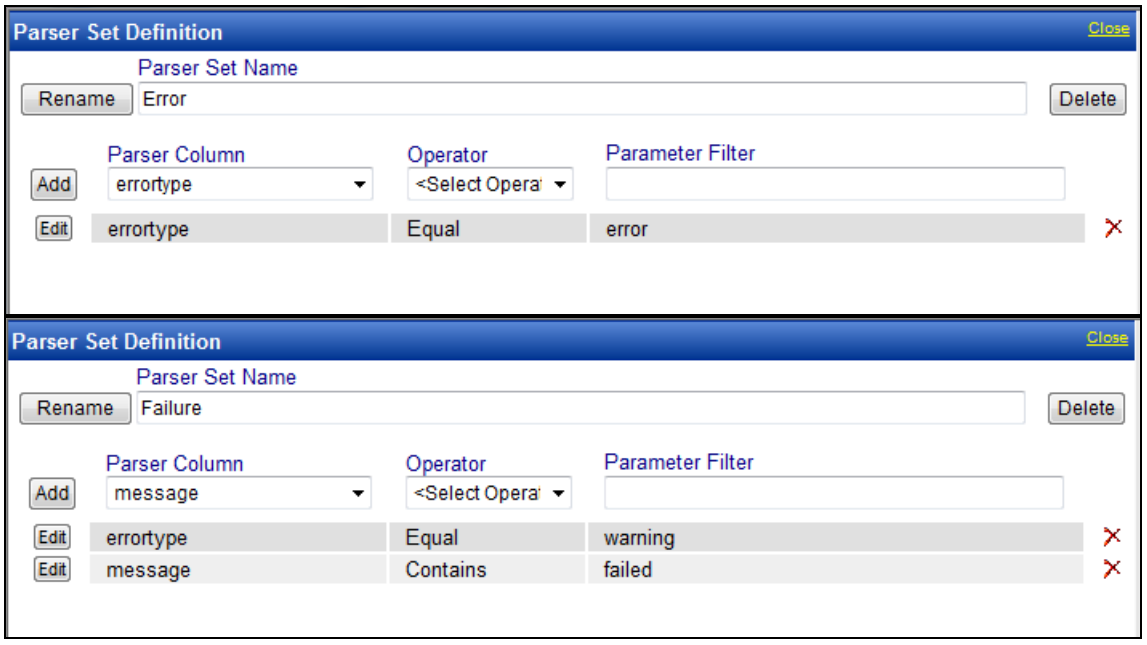
Einzeilige Vorlage:

```
$Time$ $hostname$ $errortype$ $message$
```

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:

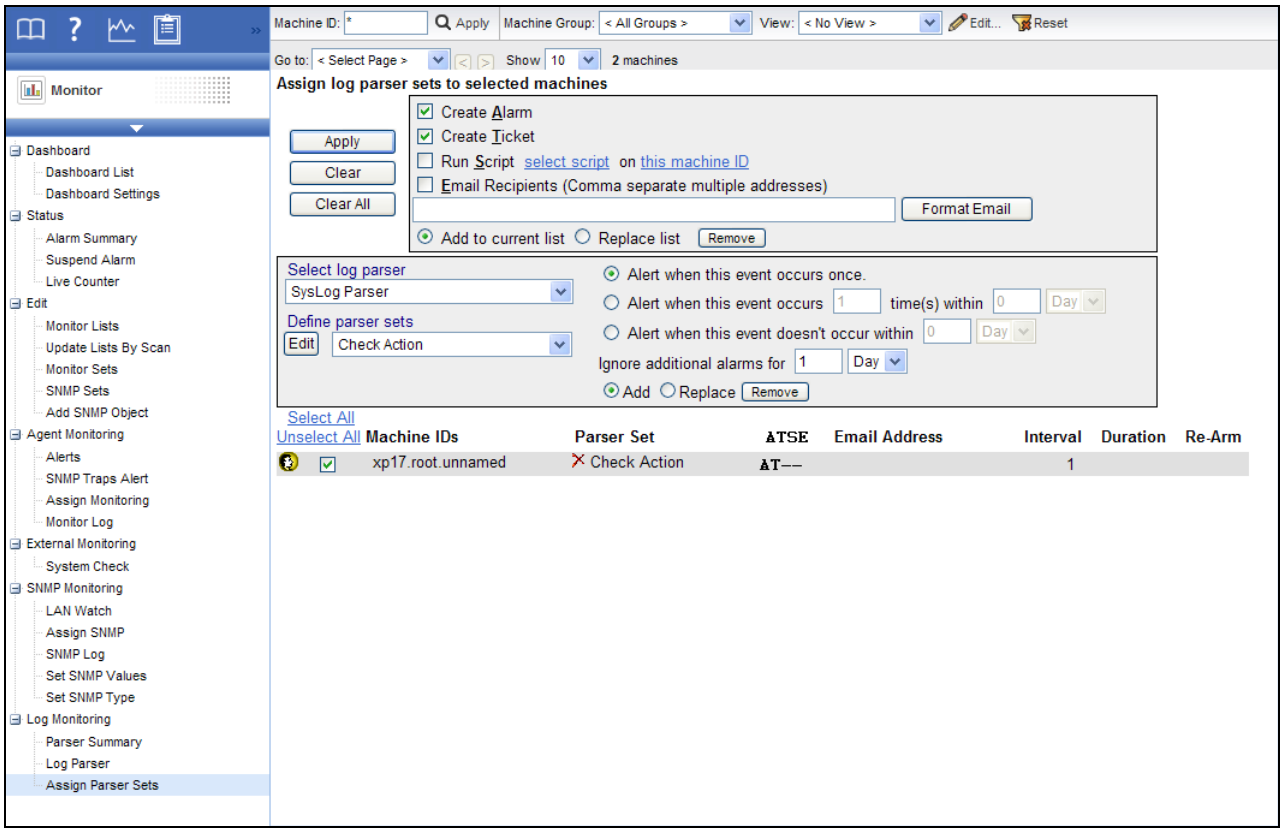


Schritt 6: Analysesatz zuweisen

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.

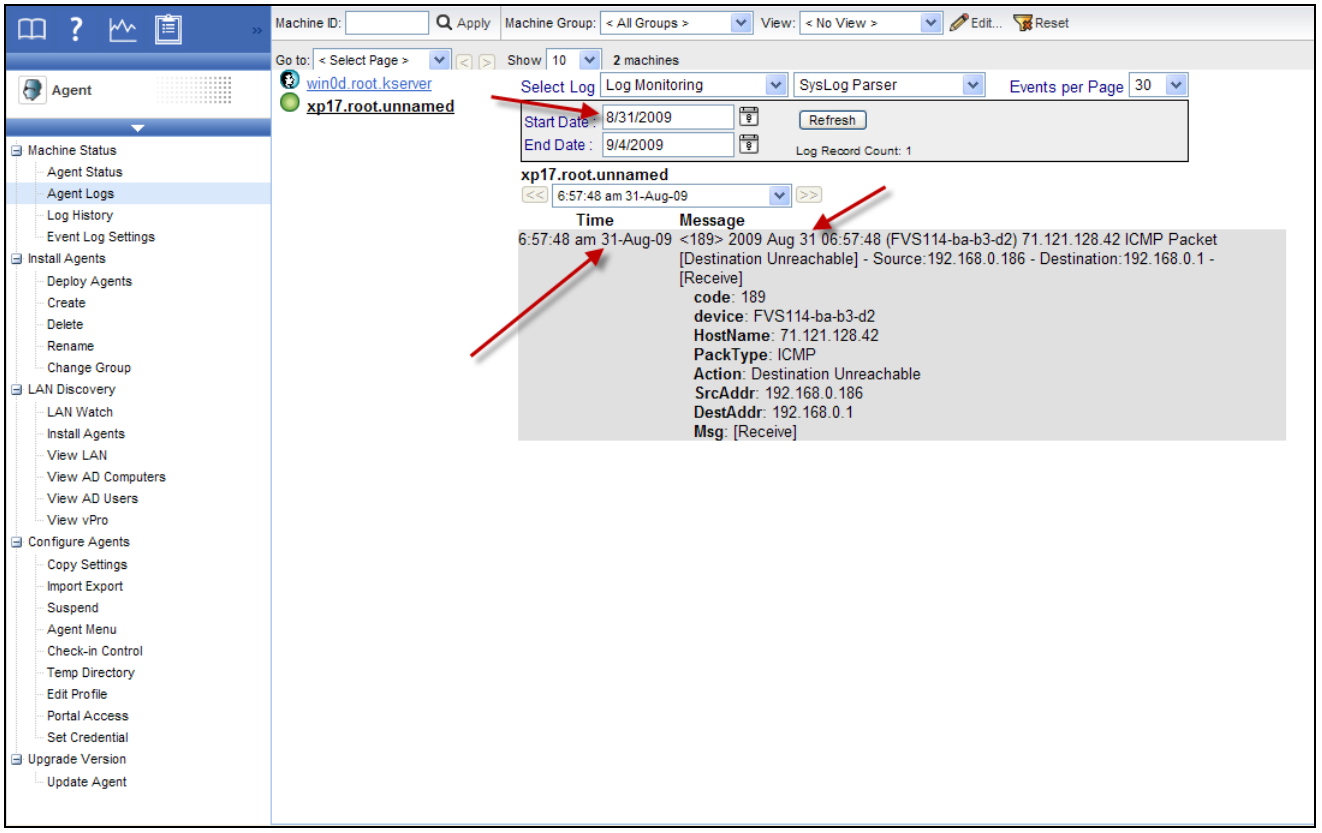


Schritt 7: Das "Protokoll-Monitoring-Protokoll" überprüfen

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

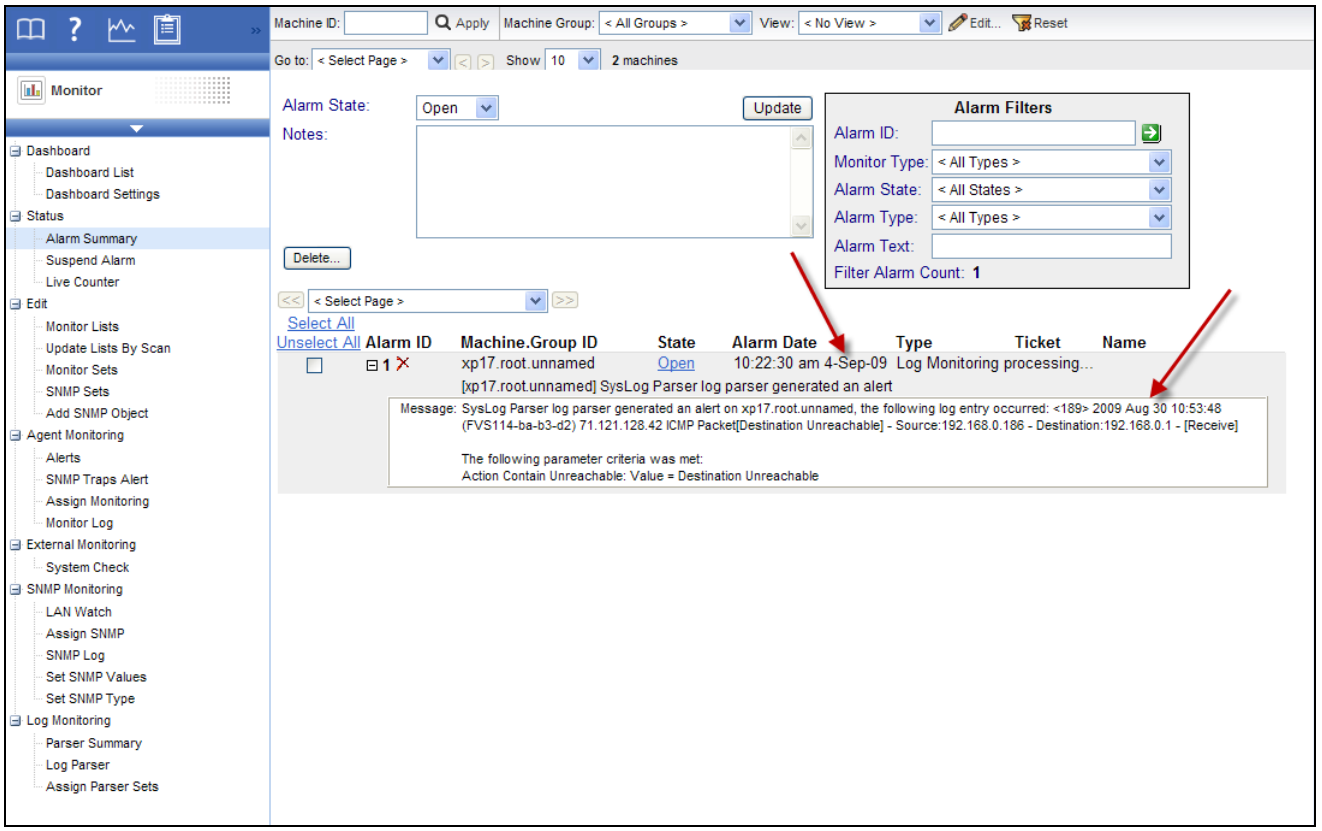
- Agents > Agent-Protokolle > Protokoll-Monitoring > (Analysedefinition)
- Live Connect > Agent-Daten > Agent-Protokolle > Protokoll-Monitoring > (Analysedefinition) Live Connect kann durch Klicken auf das Check-in-Statussymbol einer ausgewählten Rechner-ID angezeigt werden.
- Inventarisierung > Rechnerübersicht > 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.



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

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.



Inhaltsverzeichnis

E

S