Kaseya 2

Analisadores de logs

Guia do usuário

Version 7.0

Português

October 8, 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."

Conteúdo

Introdução

O VSA é capaz de monitorar os dados coletados de diversos arquivos de log padrão. O **Monitoramento de Registros** amplia essa capacidade extraindo dados da saída de qualquer arquivo de registro baseado em texto. Os exemplos incluem arquivos de logs de aplicativos e arquivos syslog criados para sistemas operacionais Unix, Linux e Apple, e dispositivos de rede, tais como roteadores Cisco. Para evitar carregar todos os dados contidos nestes logs no banco de dados do servidor da Kaseya, o **Monitoramento de logs** utiliza conjuntos de analisadores e definições de analisadores para analisar cada arquivo de log e selecionar somente os dados nos quais você está interessado. Mensagens analisadas são exibidas em Monitoramento de logs, que pode ser acessado na guia Logs do agente de Live Connect > Dados do agente ou na página Resumo da máquina, ou gerando um relatório na página Agente > Logs - Monitoramento de logs. Opcionalmente, os usuários podem acionar alertas quando um registro do **Monitoramento de Registros** é gerado, conforme definido usando Atribuir Conjuntos de Analisadores ou Resumo do Analisador.

Definições dos analisadores e Conjuntos de analisadores

Ao configurar o Monitoramento de Registros é útil distinguir entre dois tipos de registros de configuração: **definições de analisadores** e **conjuntos de analisadores**.

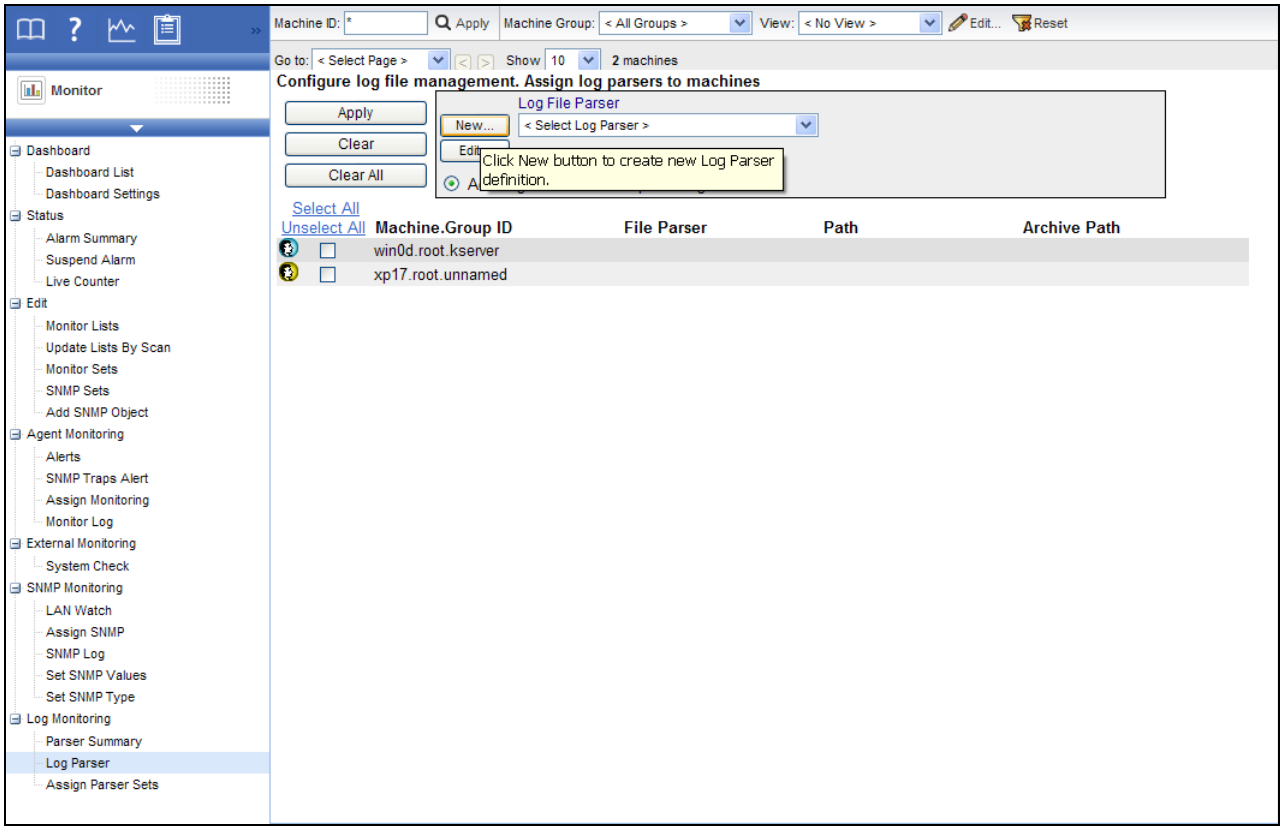
Uma **definição de analisador** é usada para:

- Localizar o arquivo de registro que está sendo analisado.
- Selecionar os dados de registro de acordo com o *formato*, conforme especificado por um modelo.
- Preencher os parâmetros com valores dos dados do registro.
- Opcionalmente, formate a entrada do registro em **Monitoramento de Registros**.

Um **conjunto de analisadores** *filtrará* posteriormente os dados selecionados. De acordo com os *valores* dos parâmetros preenchidos e com os critérios definidos, um conjunto de analisadores pode gerar entradas de monitoramento dos registros e, opcionalmente, acionar alertas.

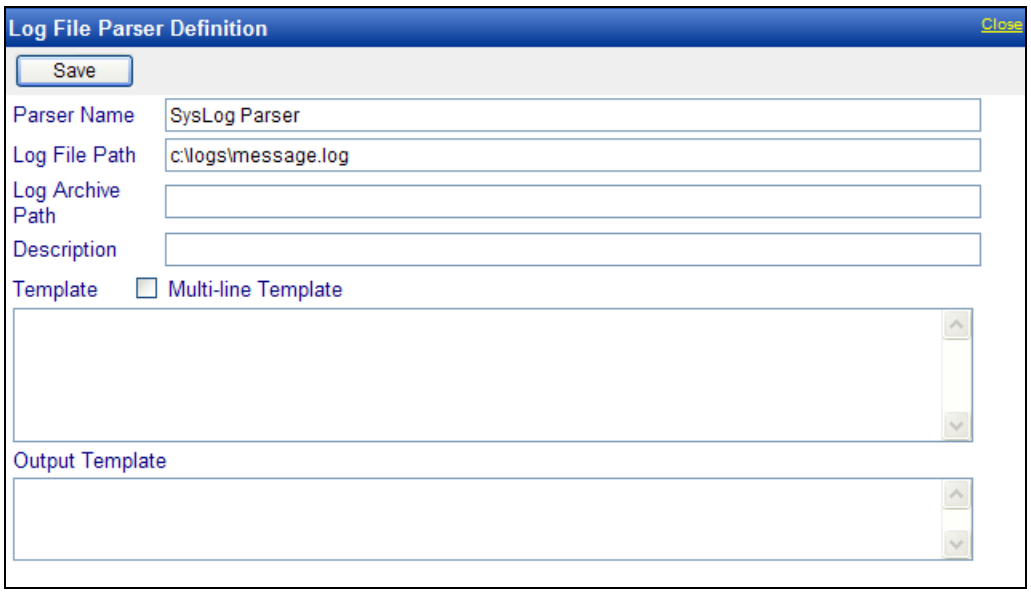
Sem a filtragem realizada pelo conjunto de analisadores, o banco de dados do servidor da Kaseya se expandiria rapidamente. Por exemplo, um parâmetro de arquivo de registro denominado $FileServerCapacity$ pode ser repetidamente atualizado com o último percentual de espaço disponível em um servidor de arquivos. Até que o espaço disponível seja inferior a 20%, pode não ser necessário fazer um registro no 20% **Monitoramento de Registros**, nem acionar um alerta com base nesse limite. Todos os conjuntos de analisadores se aplicam apenas à definição do analisador de filtro para que foram criados. Vários conjuntos de analisadores podem ser criados para cada definição de analisadores. Cada conjunto de analisadores pode acionar um alerta separado em cada ID de máquina ID à qual está atribuído.

Etapa 1: Criar uma nova definição de analisador de registro



Acesse a guia **Monitor** no VSA. Selecione **Analisador de registro** sob **Monitoramento de registro**. Clique no botão **Nova** para criar uma nova definição de analisador de registro.

Etapa 2: Insira o Nome do analisador, Caminho do arquivo de registro



Insira o seguinte:

Nome do analisador - O nome desta definição de analisador de registro.

Caminho do arquivo de registro - O caminho completo do arquivo de registro a ser processado. O caminho precisa ser acessível pelo agente. O arquivo de registro deveria conter entradas de registro formatadas. Os arquivos Unicode não são ainda suportados. Exemplo: `c:\logs\message.log`.

> **Nota:** O caractere curinga de asterisco (*) pode ser usado no nome do arquivo. O arquivo mais recente será processado neste caso. Exemplo: `c:\logs\message*.log`.

Clique no botão **Salvar** após inserir o nome do analisador e o caminho do arquivo de registro. A janela é expandida para incluir as definições de parâmetro.

Informações opcionais

Caminho do arquivo de registro - O analisador do registro altera periodicamente o arquivo de registro alvo. As entradas do registro podem ser arquivadas em diferentes arquivos antes que o analisador possa processar estas entradas. Portanto, você pode especificar o caminho do arquivo de registro no Caminho do arquivo de registro. Exemplo: Se `message.log` for salvo diariamente em um arquivo no formato `messageYYYYMMDD.log`, você poderá especificar `c:\logs\message*.log` para o **Caminho do arquivo de log**. O **Analisador de registro** é capaz de localizar o arquivo por último processado já que mantém um bookmark para o arquivo de registro.

Descrição - A descrição detalhada do analisador do registro.

Etapa 3: Especificar modelos e definir parâmetros

Template

O modelo é usado para comparação com a entrada no arquivo de registro para extrair os dados requeridos aos parâmetros. Os parâmetros são incluídos com o caractere $ no modelo. É importante que você precisa ter texto entre parênteses para que os parâmetros possam ser claramente distinguidos. Os caracteres na entrada são comparados sensível a maiúsculas e minúsculas contra o modelo.

Modelo de linha única para a entrada do registro de linha única do analisador - O modelo somente contém uma linha de entrada e o arquivo de registro é processado linha a linha.

Modelo de múltiplas linhas para a entrada de múltiplas linhas do analisador - O modelo contém entradas de múltiplas linhas e o arquivo de registro é processado por blocos de linhas delimitados por um limite de linha.

> **Nota:** A sequência de caracteres `{tab}` pode ser usada como caractere de tabulação, enquanto `{nl}` pode ser usada como uma quebra de nova linha. `{nl}` não pode ser usada em um modelo de linha única. `%` pode ser usado como caractere curinga.

Dica: Ele é mais fácil copiar e colar a entrada do registro na caixa de edição **Modelo** e substitua os dados necessários com nomes parâmetros, ao invés de tentar criar um modelo de entrada de registro ao digitar tudo.

Template de Saída

Este é um campo opcional. Isso pode ser usado para formatar a mensagem quando a entrada de registro é salvo no banco de dados, caso contrário, a entrada do registro é salvo como uma mensagem no banco e dados.

Parâmetros do Arquivo de Log

Quando o modelo estiver criado, será necessário definir a lista de parâmetros usados. Todos os parâmetros no modelo têm de ser definidos, caso contrário o analisador retornará um erro. Os parâmetros disponíveis são *integer, unsigned integer, long, unsigned long, float, double, datetime, string.* O nome do parâmetro é limitado a 32 caracteres.

Sequência do formato de data hora

Uma sequência de modelo pode conter um formato de data e hora é usado para analisar as informações de data e hora de entradas do registro. Exemplo: AAAA-MM-DD hh:mm:ss

Formatos:

- `yy, yyyy, YY, YYYY`: ano de dois ou quatro dígitos
- `M`: mês de um ou dois dígitos
- `MM`: mês de dois dígitos
- `MMM`: abreviação do nome do mês, ex. " Jan"
- `MMMM`: nome completo do mês, ex. "Janeiro"
- `D`, `d`: dia de um ou dois dígitos
- `DD`, `dd`: dia de dois dígitos
- `DDD`, `ddd`: nome abreviado do dia da semana, Ex." Seg"
- `DDDD`, `dddd`: nome completo do dia da semana, ex. "Segunda-feira"
- `H`, `h`: hora de um ou dois dígitos
- `HH`, `hh`: hora de dois dígitos

- `m`: minuto de um ou dois dígitos
- `mm`: minuto de dois dígitos
- `s`: segundo de um ou dois dígitos
- `ss`: segundo de dois dígitos
- `f`: fração de segundo de um ou mais dígitos
- `ff` - fffffffff: dois a nove dígitos
- `t`: marca de hora de um caractere, ex. "a"
- `tt`: marca de hora de dois caracteres, ex. "am"

Nota: Cada parâmetro de data e hora deve conter pelo menos os dados de mês, dia, hora e segundo. O valor do parâmetro `$Time$` é usado como a hora do evento, se especificada. Caso contrário, a hora em que a entrada foi processada é usada como a hora do vento no banco de dados.

Exemplo 1 - Entrada de linha única do registro

Inicie com uma entrada típica do registro do arquivo de registro que deseja monitorar:

```
<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]
```

Identifique as partes da entrada do registro com a qual deseja preencher parâmetros:

```
<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]
```

No modelo, substitua o texto sublinhado por parâmetros:

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

Parâmetros do Arquivo de Log

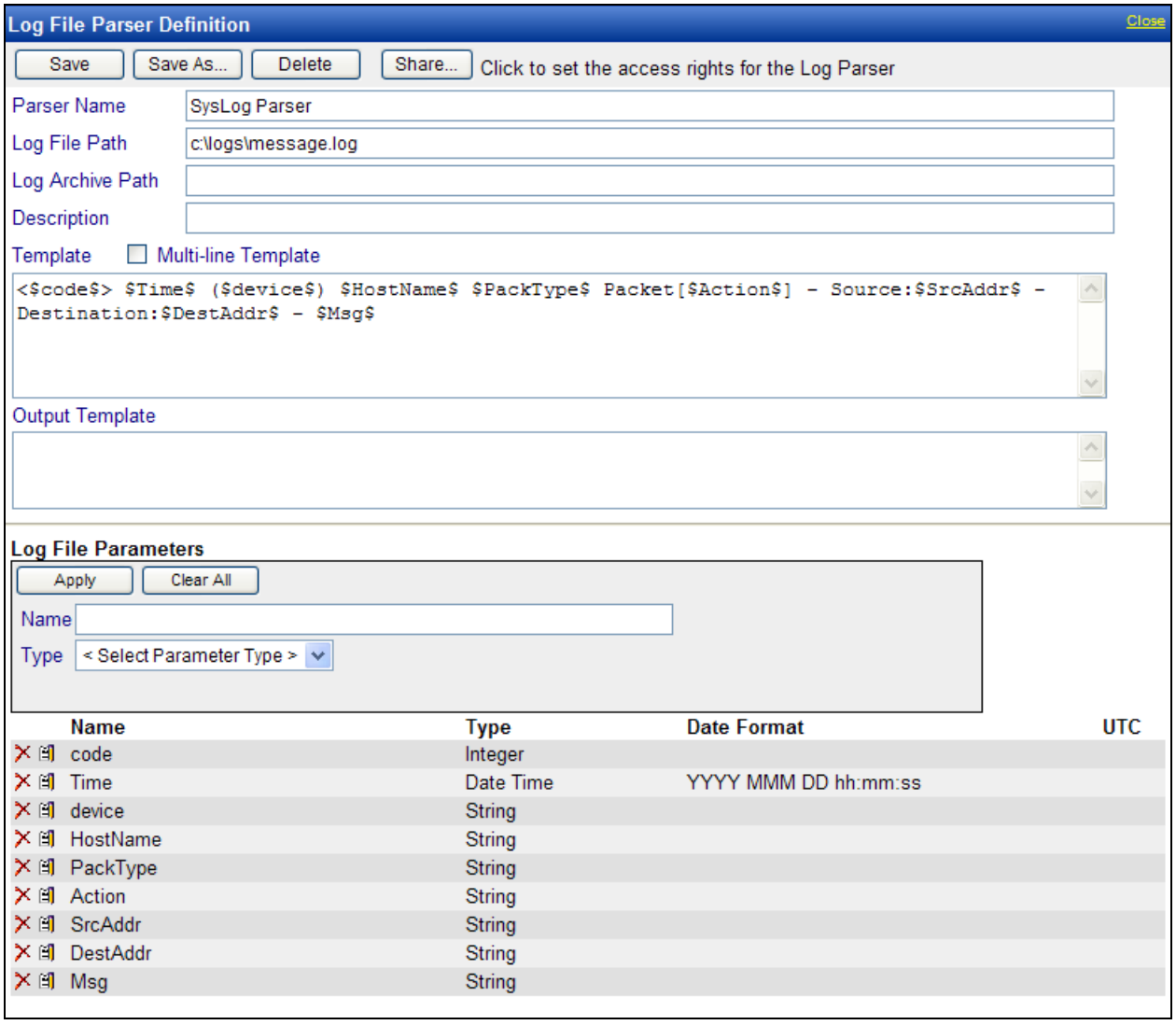
Nota: Clique no botão **Salvar** pelo menos uma vez para exibir a seção **Parâmetros do arquivo de log** da caixa de diálogo.

O texto que não é usado para preencher parâmetros precisa coincidir com o texto na entrada do registro. Por exemplo: a sequência '`] - Source:`' precisa corresponder ao texto na entrada do log, incluindo o caractere de espaço logo antes do hífen.

Defina os parâmetros:

Nome do parâmetro	Tipo de parâmetro	ResultadoAnalisado
código	Inteiro	189
Hora	datahora no formato "AAAA MMM DD hh:mm:ss", não UTC	2006-11-08 11:57:48
Dispositivo	Seqüência	FVS114-ba-b3-d2
NomeHost	Seqüência	71.121.128.42
TipoPacote	Seqüência	ICMP
Ação	Seqüência	Destino inalcançável
EndOrig	Seqüência	192.168.0.186
EndDest	Seqüência	192.168.0.1
Mens	Seqüência	[Receber]

Etapa 3: Especificar modelos e definir parâmetros



Exemplo 2 – Incluindo o símbolo % (cartão coringa)

Inicie com uma entrada típica do registro do arquivo de registro que deseja monitorar:

```
<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]
```

Identifique o texto desnecessário no arquivo de registro que deseja monitorar:

```
<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]
```

No modelo, substitua o texto traçado desnecessário acima com um cartão coringa de sinal percentual (%). Substituir outro texto com parâmetros:

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

Defina os parâmetros:

Nome do parâmetro	Tipo de parâmetro	ResultadoAnalisado
código	Inteiro	`189`
Hora	data e hora no formato `YYYY MMM DD hh:mm:ss`	`2006-11-08 11:57:48`
NomeHost	Seqüência	`71.121.128.42`
TipoPacote	Seqüência	`ICMP`
EndOrig	Seqüência	`192.168.0.186`
EndDest	Seqüência	`192.168.0.1`

Exemplo 3 - Entrada de múltiplas linhas do registro

Inicie com uma entrada de múltiplas linhas típicas do registro do arquivo de registro que deseja monitorar:

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

Identifique o texto a ser ignorado e o texto a ser preenchido por parâmetros.

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

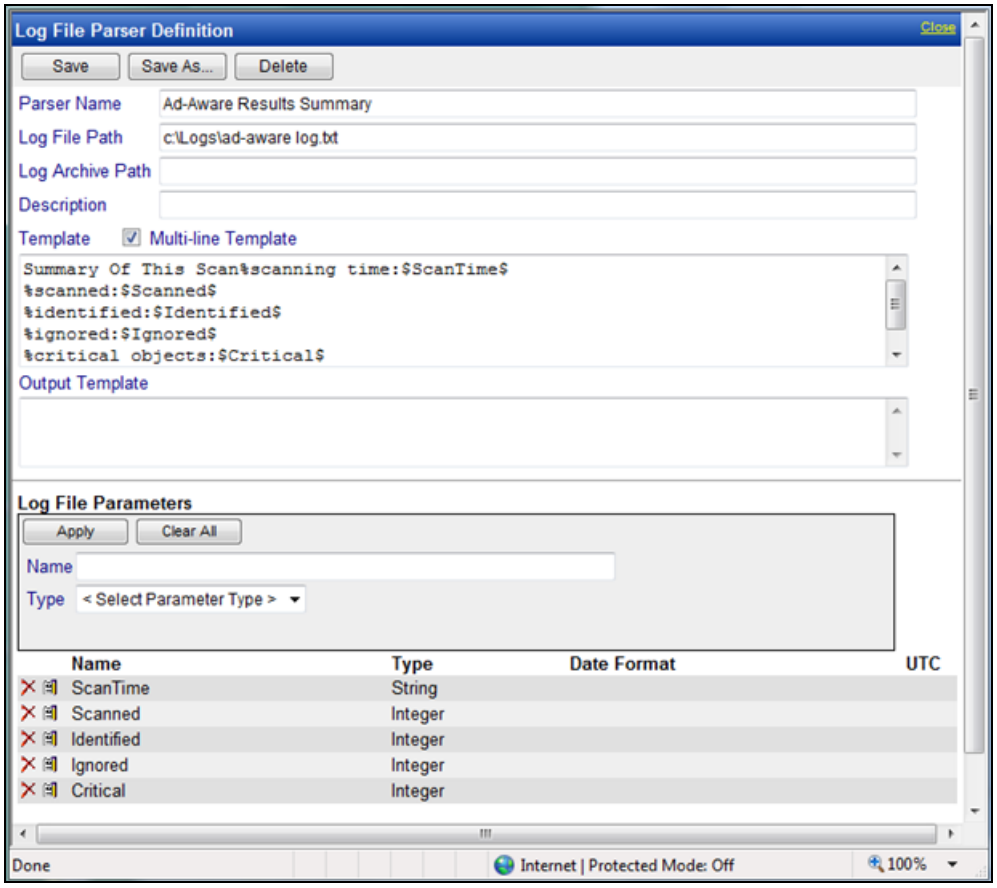
No modelo, substitua o texto traçado desnecessário com um cartão coringa de sinal percentual (%). Substitua o texto sublinhado com parâmetros.

```
Summary Of This Scan
%scanning time:$ScanTime$
%scanned:$Scanned$
%identified:$Identified$
%ignored:$Ignored$
%critical objects:$Critical$
```

Defina os parâmetros:

Nome do parâmetro	Tipo de parâmetro	ResultadoAnalisado
HoraVarredura	Seqüência	00:02:32.765
Varrido	Inteiro	91445
Identificado	Inteiro	0
Ignorado	Inteiro	0
Crítico	Inteiro	0

Etapa 3: Especificar modelos e definir parâmetros

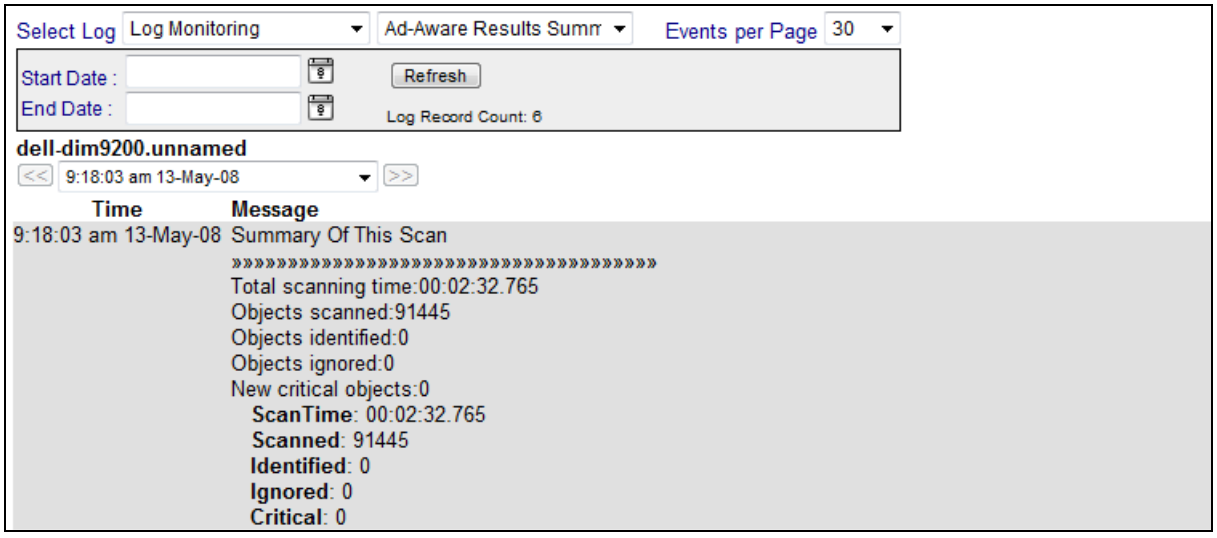


Exemplo 4 – Modelo de saída

Inicie com uma entrada de múltiplas linhas típicas do registro do arquivo de registro que deseja recuperar:

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

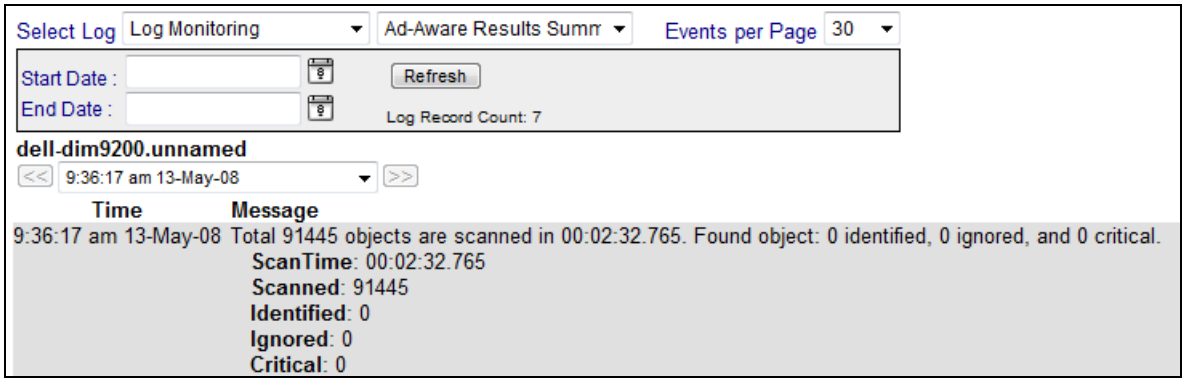
Todos os dados acima serão registrados como o corpo da mensagem no registro do monitor se uma modelo de saída não for especificado. Aqui está um exemplo da saída no monitoramento do registro sem especificar um modelo de saída:



No modelo de saída, especifique um modelo ao usar parâmetros definidos:

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

Aqui está um exemplo da saída no monitoramento do registro após especificar um modelo de saída:

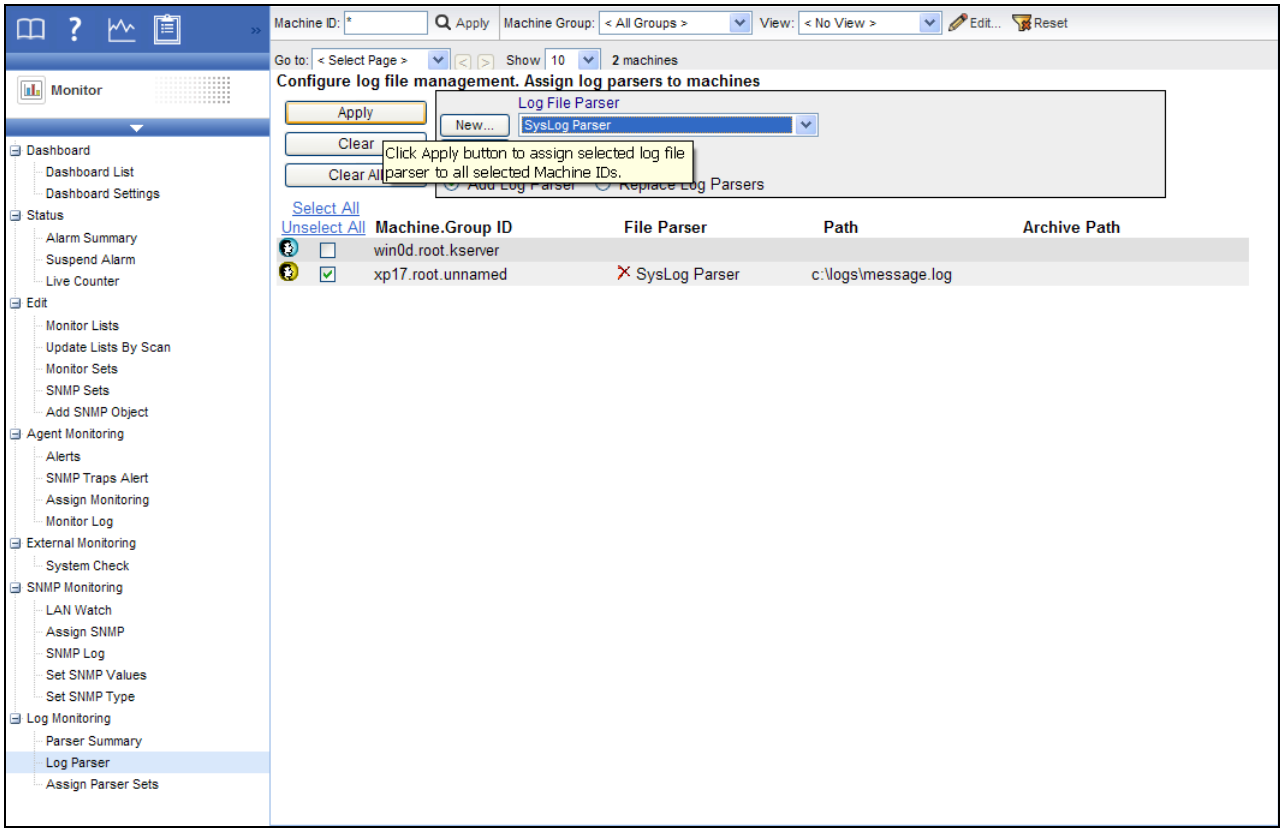


Etapa 4: Atribuir a definição do analisador do registro

Um definição completa do analisador de registro precisa ser atribuída à uma ou mais IDs de máquina usando a função **Analisador do registro**. Selecione as IDs de máquina nas quais aplicar a definição e clique no botão **Aplicar**. Isso significa que a definição do analisador pode ser usada pelas máquinas selecionadas, mas a análise não ocorre até que você selecione o critério de filtro para os dados de

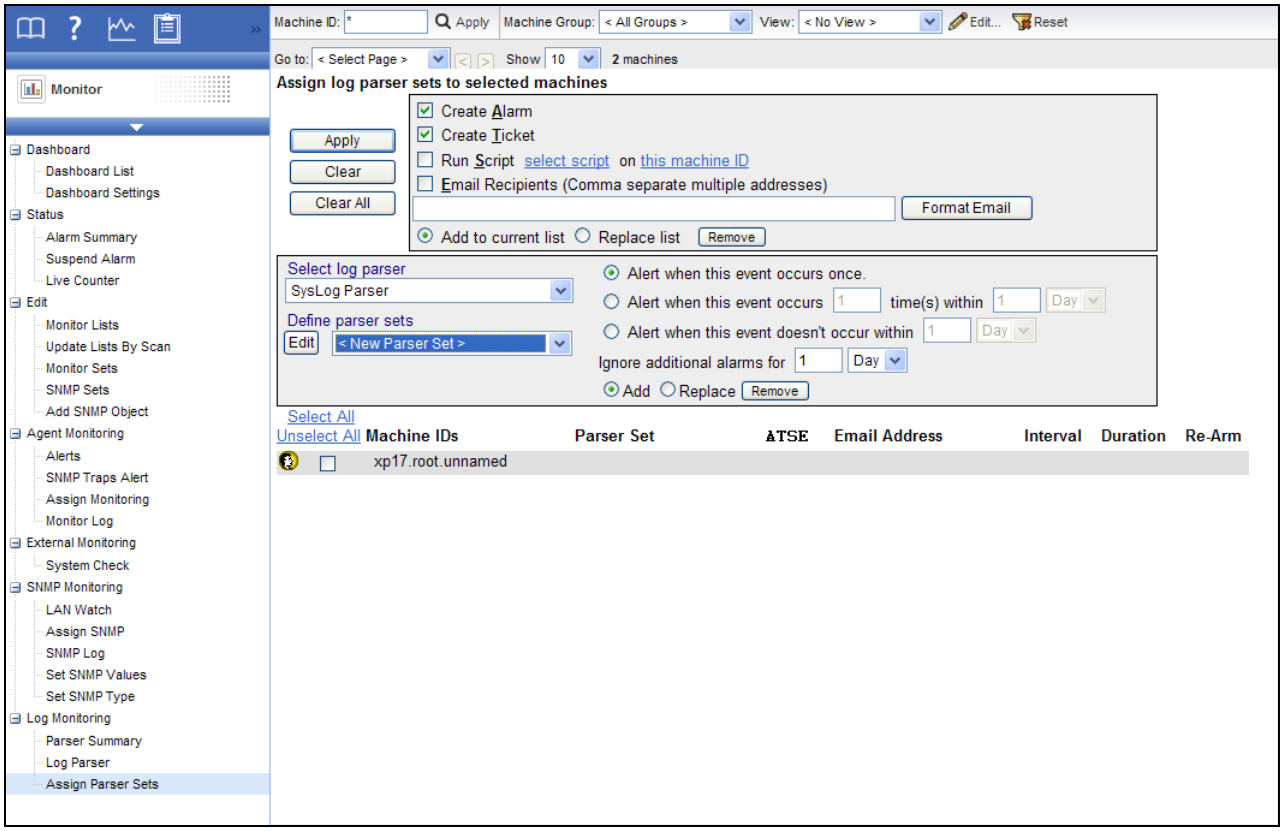
Etapa 4: Atribuir a definição do analisador do registro

registro sendo coletados e após atribuir as condições de alerta, como descrito nas Etapas 5 e 6.

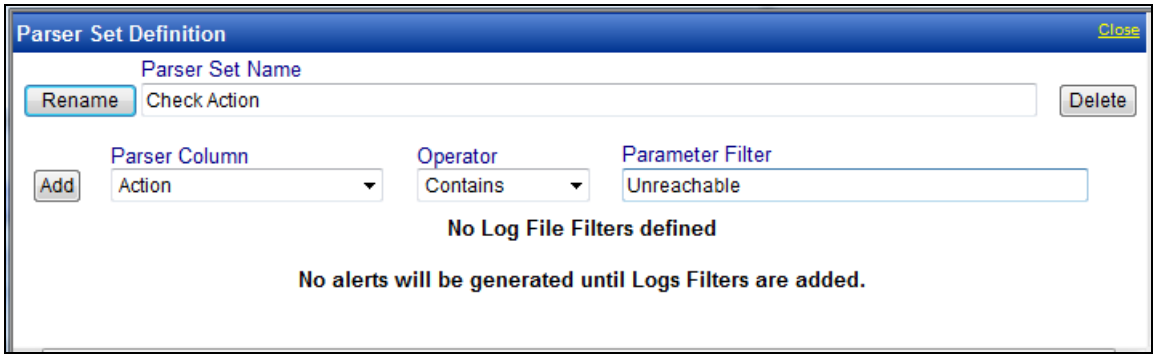


Etapa 5: Definir a coleção e as condições do alerta

Clique em **Atribuir conjuntos do analisador** sob **Monitoramento do registro** na lista de funções. Selecione uma definição do analisador do registro na lista suspensa **Selecionar analisador do registro**. Em seguida, selecione `<New Parser Sets>` na lista suspensa **Definir conjuntos de analisadores**. *Um conjunto de analisadores de logs é um conjunto de condições que devem ser verdadeiras sobre a análise de uma entrada do log para que esta seja incluída no log de "monitoramento de logs" e, opcionalmente, para criar uma alerta para a mesma.* Isso garante que somente as entradas relevantes do log sejam lançadas no log de "monitoramento de logs". Observe que um conjunto de analisador do registro é específico de um analisador do registro. Você pode definir múltiplos conjuntos do analisador para o mesmo analisador do registro e acionar um conjunto diferente de alertas para cada conjunto de analisador do registro.



Defina as condições do alerta. No exemplo a seguir, uma entrada é criada no log de "monitoramento de logs" quando uma entrada do log é analisada de tal forma que o parâmetro `Action` contenha o texto `Unreachable`.



Operadores para parâmetros

- **Sequência**: `begins with, does not begin with, contains, does not contain, ends with, does not end with, equals, does not equal`
- **Numérica**: `equal, not equal, over, under`
- **Hora**: `equal, not equal, over, under`

O **Filtro de parâmetro** para **Hora** pode estar em um dos seguintes formatos. Uma sequência de filtro que termina com `Z` indica uma hora UTC.

- `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`

Exemplo: `2008-04-01 15:30:00.00`

Conjuntos e condições do analisador

As condições são definidas em um conjunto do analisador. Você atribui múltiplas condições para um conjunto do analisador. Você também pode atribuir múltiplos conjuntos do analisador para um analisador do registro. Um entrada do registro precisa atender todas as condições dentro de um conjunto do analisador para poder acionar a coleta de dados e/ou o alerta. Observe que este comportamento é diferente dos alertas do registro de eventos e outros conjuntos de monitores. Por exemplo:

Conteúdo do registro:

```
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"
```

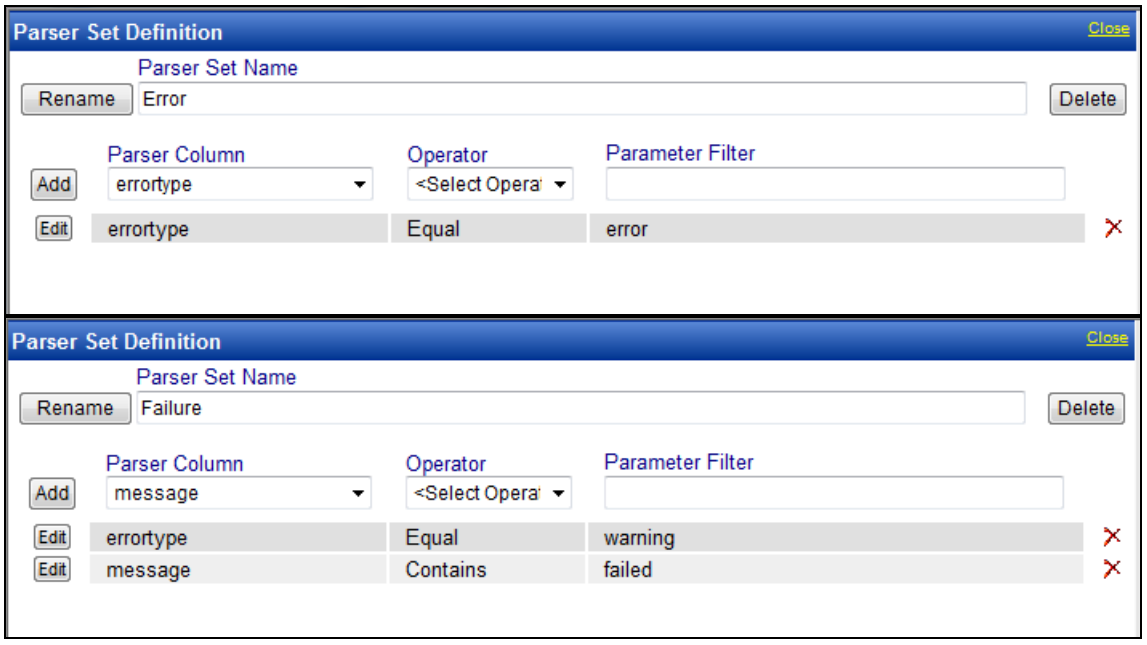
Modelo de linha única:

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

Para coletar entradas que atendem uma das seguintes condições, é preciso definir dois conjuntos do analisador do registro e atribuir ambos ao analisador do registro:

```
$errortype$ is "error"
$errortype$ is "warning" AND $message$ contains "failed"
```

Aqui estão as capturas de tela correspondentes para estes dois conjuntos do analisador:

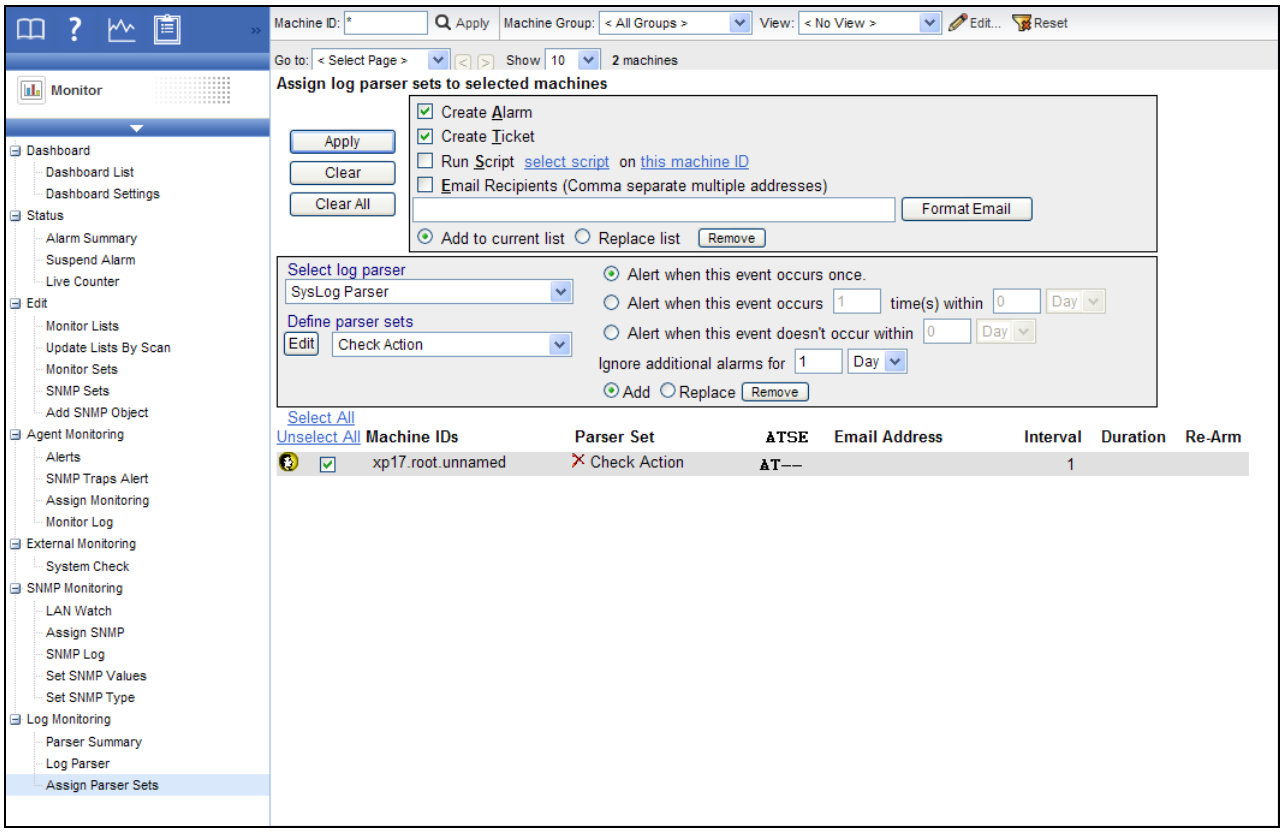


Etapa 6: Atribuir conjunto do analisador

Selecione a ID de máquina, as opções de alarme e tipos de alertas, e a seguir clique no botão **Aplicar** para atribuir o conjunto do analisador do registro para uma ID de máquina. Após a ID de máquina receber a configuração do analisador do registro, o agente na máquina gerenciada irá começar a analisar o arquivo de registro *, sempre que o arquivo de registro é atualizado.*

Notificação

O agente coleta entradas de logs e cria uma entrada no log "monitoramento de logs" com base nos critérios definidos pelo conjunto de analisadores, *independentemente de os métodos de notificação estarem marcados ou não.* Não é necessário ser notificado cada vez que uma nova entrada do monitoramento do registro for criada. Você pode simplesmente revisar o log "Monitoramento de logs" periodicamente, à sua conveniência.

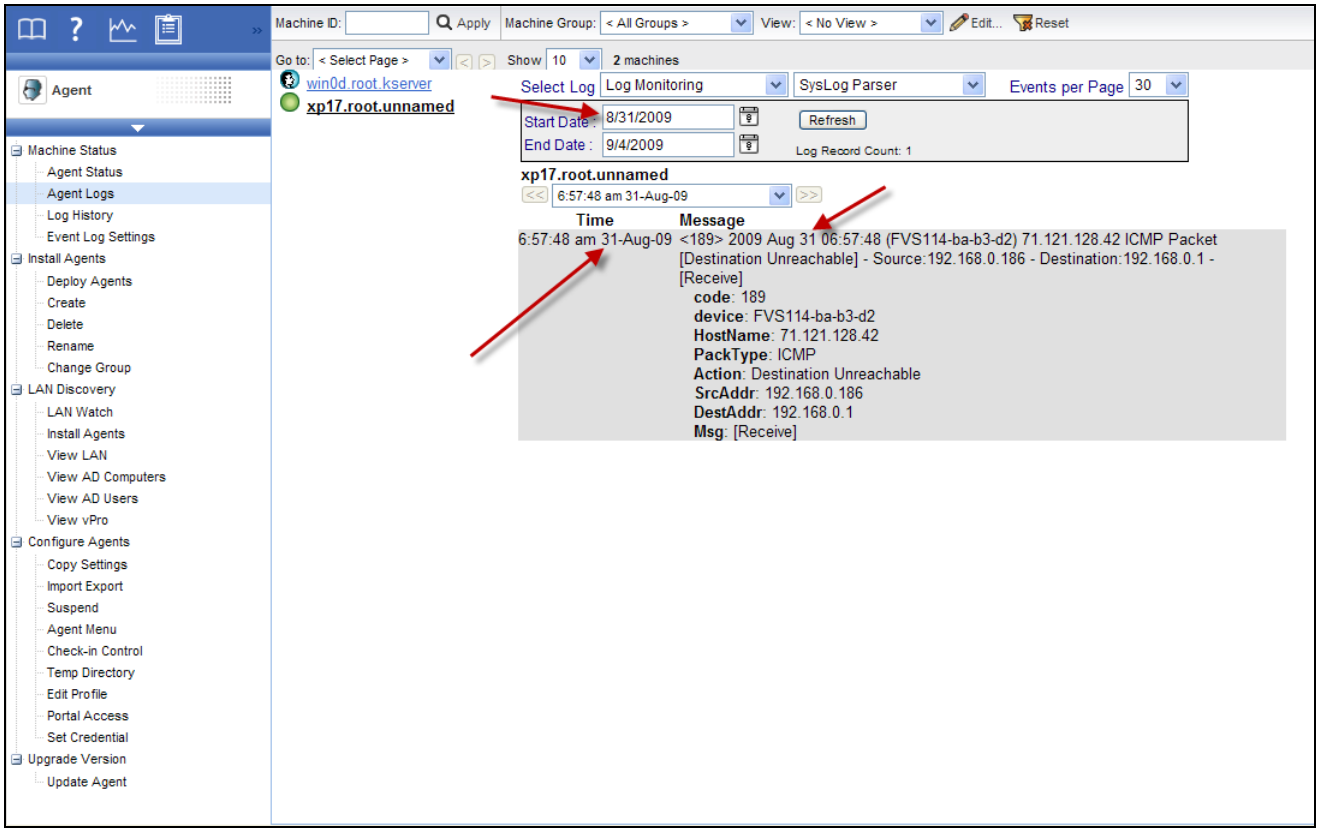


Etapa 7: Analisar o log de "monitoramento de logs"

As entradas do Monitoramento de Registros são exibidas em **Monitoramento de Registros**, que pode ser acessado usando:

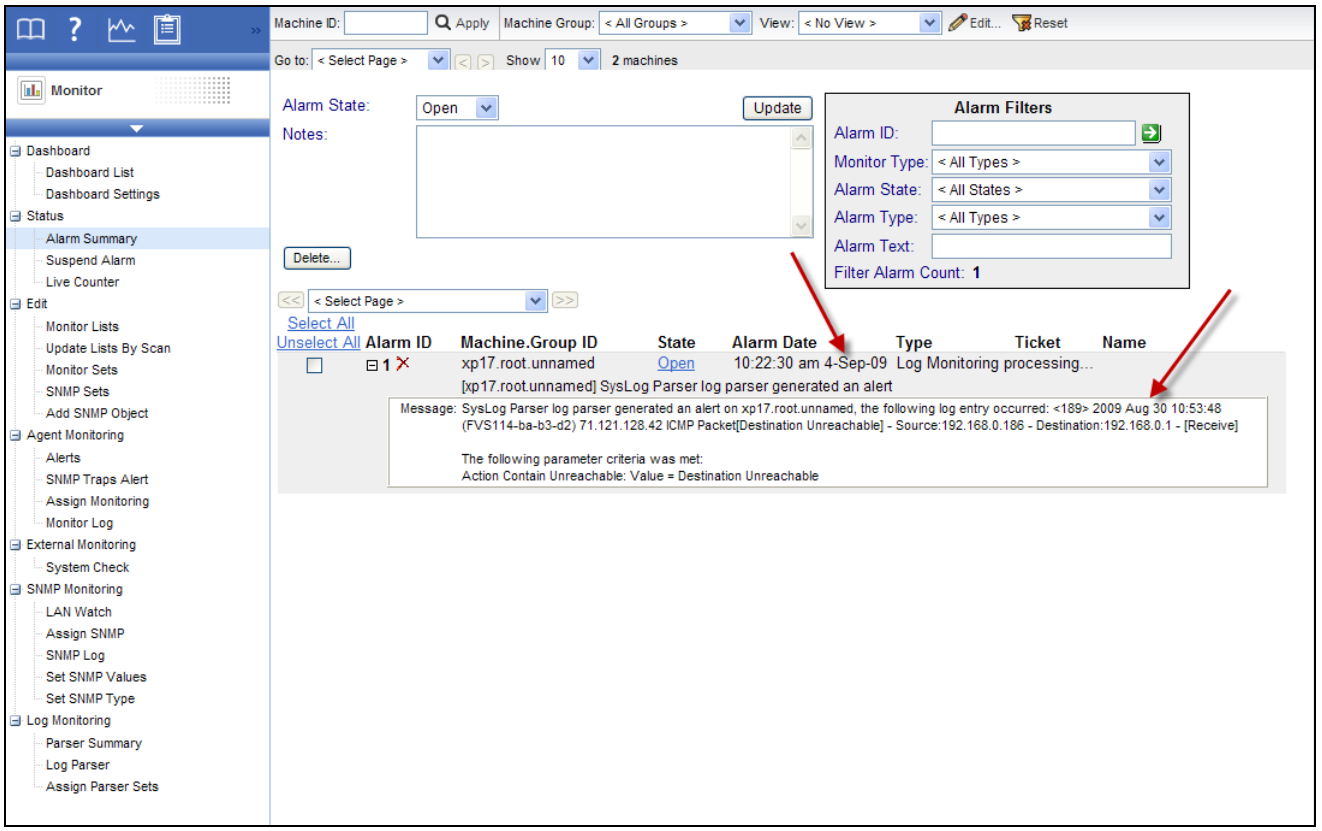
- Agentes > Logs do agente > Monitoramento de logs > (definição do analisador)
- Live Connect > Dados do agente > Logs do agente > Monitoramento de logs > (definição do analisador). O Live Connect é exibido clicando no ícone de status de entrada de uma ID de máquina selecionada.
- Auditoria > Resumo da máquina guia > Logs do agente > Monitoramento de logs > (definição do analisador). A página Resumo das Máquinas também pode ser exibida *pressionando Alt e clicando* no ícone de status de entrada de uma ID de máquina selecionada.
- O Centro de informações > Emissão de relatórios > Relatórios > Monitor - Logs > relatório de Monitoramento de logs

Estas imagens de amostra mostram o parâmetro $Time$ sendo usado para as entradas do monitoramento do registro. *Data e hora de filtragem em exibições e relatórios são baseadas na hora da entrada no registro.* Se você incluir um parâmetro de `$Time$` utilizando o tipo de dados de `Date Time` em seu modelo, o **Monitoramento de logs** utilizará o tempo armazenado no parâmetro de `$Time$` conforme o tempo de entrada do log. Se um parâmetro de `$Time$` *não* estiver incluído no seu modelo, o tempo que foi adicionado na entrada para **Monitoramento de logs** servirá como o tempo de entrada do log. Assegure-se em selecionar uma faixa de datas que exiba as datas da entrada do registro.



Etapa 7: Analisar o log de "monitoramento de logs"

Em contraste, as datas de alarmes têm como base a data em que o alarme foi criado, não a data das entradas no log de "monitoramento de logs".



Índice

E

I