Kaseya 2

Analizadores de registros

Guía del usuario

Versión R8

Español

Outubre 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."

Contenido

Introducción

El VSA es capaz de supervisar datos obtenidos de muchos archivos de registro estándar. **Monitoreo de registro** extiende esa capacidad extrayendo datos del resultado de cualquier archivo de registro basado en texto. Los ejemplos incluyen archivos de registro de aplicaciones y archivos de syslog creados para los sistemas operativos Unix, Linux y Apple, y dispositivos de red, como los enrutadores Cisco. Para evitar cargar todos los datos contenidos en estos registros en la base de datos del servidor Kaseya Server, la función **Supervisión de registros** usa definiciones de analizadores y conjuntos de analizadores para analizar cada archivo de registro y seleccionar sólo los datos en los que está interesado. Los mensajes analizados se muestran en Supervisión de registros, función a la que puede accederse mediante la pestaña Registros de agente de Live Connect > Datos de agente; por medio de la página Resumen de máquina; o generando un informe en la página Registros -Supervisión de registros de Agente. Opcionalmente, los usuarios pueden activar alertas cuando se genera un registro de **Monitoreo de registro**, tal lo definido utilizando Asignar conjuntos de analizador o Resumen de analizador.

Definiciones de analizador versus conjuntos de analizador

Al configurar Monitoreo de registros resulta útil distinguir entre las dos clases de registros de configuración: **definiciones de analizador** y **conjuntos de analizador**.

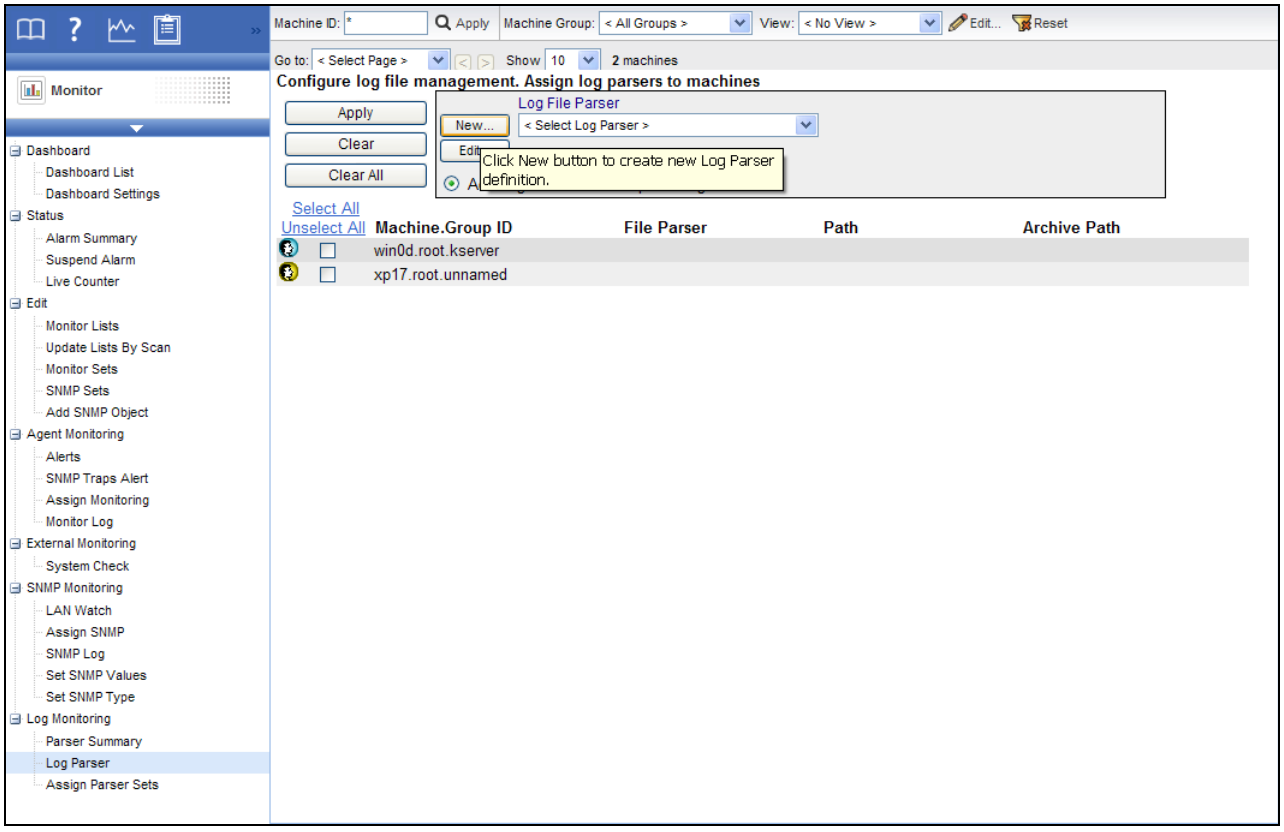
Una **definición de analizador** se usa para:

- Ubicar el archivo de registro que se está analizando.
- Seleccionar datos de registro en base al *formato* de los datos de registro, según se especifica en una plantilla.
- Poblar parámetros con valores de datos de registro.
- Opcionalmente formatear la entrada de registro en **Monitoreo de registro**.

Posteriormente un **conjunto de analizador** *filtra* los datos seleccionados. En base a los *valores* de parámetros poblados y a los criterios que define, un conjunto de analizador puede generar entradas de monitoreo de registro y opcionalmente activar alertas.

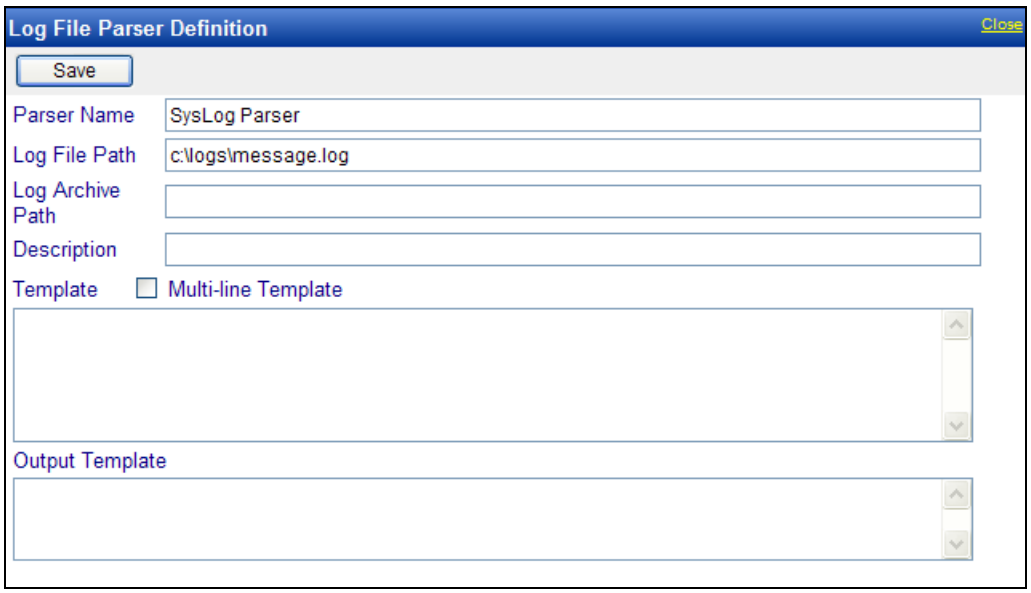
Sin el filtrado realizado por el conjunto de analizadores, la base de datos del servidor Kaseya Server se expandiría a gran velocidad. Por ejemplo, el parámetro de un archivo de registro llamado $FileServerCapacity$ podría actualizarse repetidas veces con el último porcentaje de espacio libre en un servidor de archivos. Hasta que el espacio libre sea menor al 20% posiblemente no sea necesario hacer un registro en el **Monitoreo de registro**, ni activar una alerta en base a este umbral. Cada conjunto de analizador se aplica sólo a la definición de analizador para la que fue creado para filtrar. Los conjuntos de analizador múltiples pueden crearse para cada definición de analizador. Cada conjunto de analizador puede activar una alerta separada en cada ID de máquina a la que está asignado.

Paso 1: Crear una nueva definición de analizador de registro



Diríjase a la pestaña **Monitor** en el VSA. Seleccione **Analizador de registro** debajo de **Monitoreo de registro**. Haga clic en el botón **Nuevo** para crear una nueva definición de analizador de registro.

Paso 2: Ingrese Nombre de analizador, Ruta de archivo de registro



Ingrese lo siguiente:

Nombre de analizador: el nombre de esta definición de analizador de registro.

Ruta de archivo de registro: la ruta completa del archivo de registro a procesar. El agente debe poder acceder a esta ruta. El archivo de registro debe contener entradas de registro formateadas. Aún no es posible aceptar archivos Unicode. Ejemplo: `c:\logs\message.log`.

> **Nota:** El carácter comodín de asterisco (*) puede usarse en el nombre de archivo. En este caso se procesará el archivo más reciente. Ejemplo: `c:\logs\message*.log`.

Haga clic en el botón **Guardar** después de ingresar el nombre de analizador y la ruta del archivo de registro. La ventana se expande para incluir las definiciones de parámetros.

Información opcional

Ruta de archivo de registro - El analizador de registro verifica los cambios del archivo de registro de destino en forma periódica. Las entradas de registro pueden archivarse en diferentes archivos antes de que el analizador de registro pueda procesar esas entradas. Así puede especificar la ruta del archivo en el campo de la Ruta de archivo de registro. Ejemplo: Si `message.log` se archiva a diario en un archivo en formato `messageYYYYMMDD.log`, puede especificar `c:\logs\message*.log` para la **Ruta de archivo de registro**. **Analizador de registro** puede localizar el último archivo que procesó ya que guarda ese archivo de registro como favorito.

Descripción - La descripción detallada del analizador de registro.

Paso 3: Especifique las plantillas y defina los parámetros.

Plantilla

La plantilla se usa para comparar con la entrada de registro en el archivo de registro para extraer los datos necesarios en los parámetros. Los parámetros están encerrados con el carácter $ en la plantilla. Es importante que tenga textos alrededor de los parámetros de manera que los parámetros puedan distinguirse claramente. Los caracteres en la entrada de registro se comparan contra la plantilla distinguiendo entre mayúsculas y minúsculas.

Plantilla de una línea a entrada de registro de analizador de una línea: la plantilla sólo contiene una entrada de una línea y el archivo de registro se procesa línea por línea.

Plantilla de múltiples líneas a entradas de registro de analizador de múltiples líneas: la plantilla contiene entradas de líneas múltiples y el archivo de registro se procesa por bloque de líneas limitado por un delimitador de línea.

> **Nota:** La cadena de caracteres `{tab}` puede usarse como un carácter de tabulación y `{nl}` puede usarse como un nuevo salto de línea. `{nl}` no puede usarse en una plantilla de una sola línea, y `%` puede usarse como carácter comodín.

Ayuda: Es más fácil copiar y pegar la entrada de registro en la casilla de edición de la **Plantilla** y reemplazar los datos necesarios con nombres de parámetros, en lugar de crear una plantilla de entrada de registro y tipear todos los datos.

Plantilla de salida

Este campo es opcional. Puede usarse para formatear el mensaje cuando la entrada de registro se guarda en la base de datos; de lo contrario, la entrada de registro se guarda como el mensaje en la base de datos.

Parámetros de archivo de registro

Una vez que se ha creado la plantilla, es necesario definir la lista de parámetros utilizados por la plantilla. Todos los parámetros en la plantilla tienen que estar definidos, de lo contrario el análisis devuelve un error. Los parámetros disponibles son *entero, entero no firmado, largo, largo no firmado, flotante, doble, DateTime, cadena* El largo del nombre de parámetro está limitado a 32 caracteres.

Cadena de formato Fecha y Hora

Una cadena de plantilla puede contener un formato de fecha y hora que se usa para analizar la información de fecha y hora de las entradas de registro. Ejemplo: AAAA-MM-DD hh:mm:ss

Formatos:

- `yy, yyyy, YY, YYYY`: año de dos o de cuatro dígitos
- `M`: mes de uno o de dos dígitos
- `MM`: mes de dos dígitos
- `MMM`: nombre abreviado del mes, p. ej., “ Ene"
- `MMMM`: nombre completo del mes, p. ej., "Enero"
- `D`, `d`: día de uno o de dos dígitos
- `DD`, `dd`: día de dos dígitos
- `DDD`, `ddd`: nombre abreviado del día de la semana, p. ej., “ Lun"
- `DDDD`, `dddd`: nombre completo del día de la semana, p. ej., "Lunes"
- `H`, `h`: hora de uno o de dos dígitos
- `HH`; `hh`: hora de dos dígitos

- `m`: minutos de uno o de dos dígitos
- `mm`: minutos de dos dígitos
- `s`: segundos de uno o de dos dígitos
- `ss`: segundos de dos dígitos
- `f`: fracción de segundos de uno o de más dígitos
- `ff`-fffffffff: de dos a nueve dígitos
- `t`: marca de tiempo de un carácter, p. ej., "a"
- `tt`: marca de tiempo de dos caracteres, p. ej., "am"

> **Nota:** Cada parámetro de fecha y hora debe contener, como mínimo, los datos de mes, día, hora y segundo. El valor del parámetro `$Time$` se usa como hora del evento si se especifica. De lo contrario, la hora en la que se procesa la entrada se usa como hora del evento en la base de datos.

Ejemplo 1: entrada de registro de una línea

Comience con una entrada de registro típica desde el archivo de registro que desea monitorear:

```
<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 las partes de la entrada de registro con la que desea completar los parámetros:

```
<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]
```

En la plantilla, reemplace el texto subrayado con los parámetros:

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

Parámetros de archivo de registro

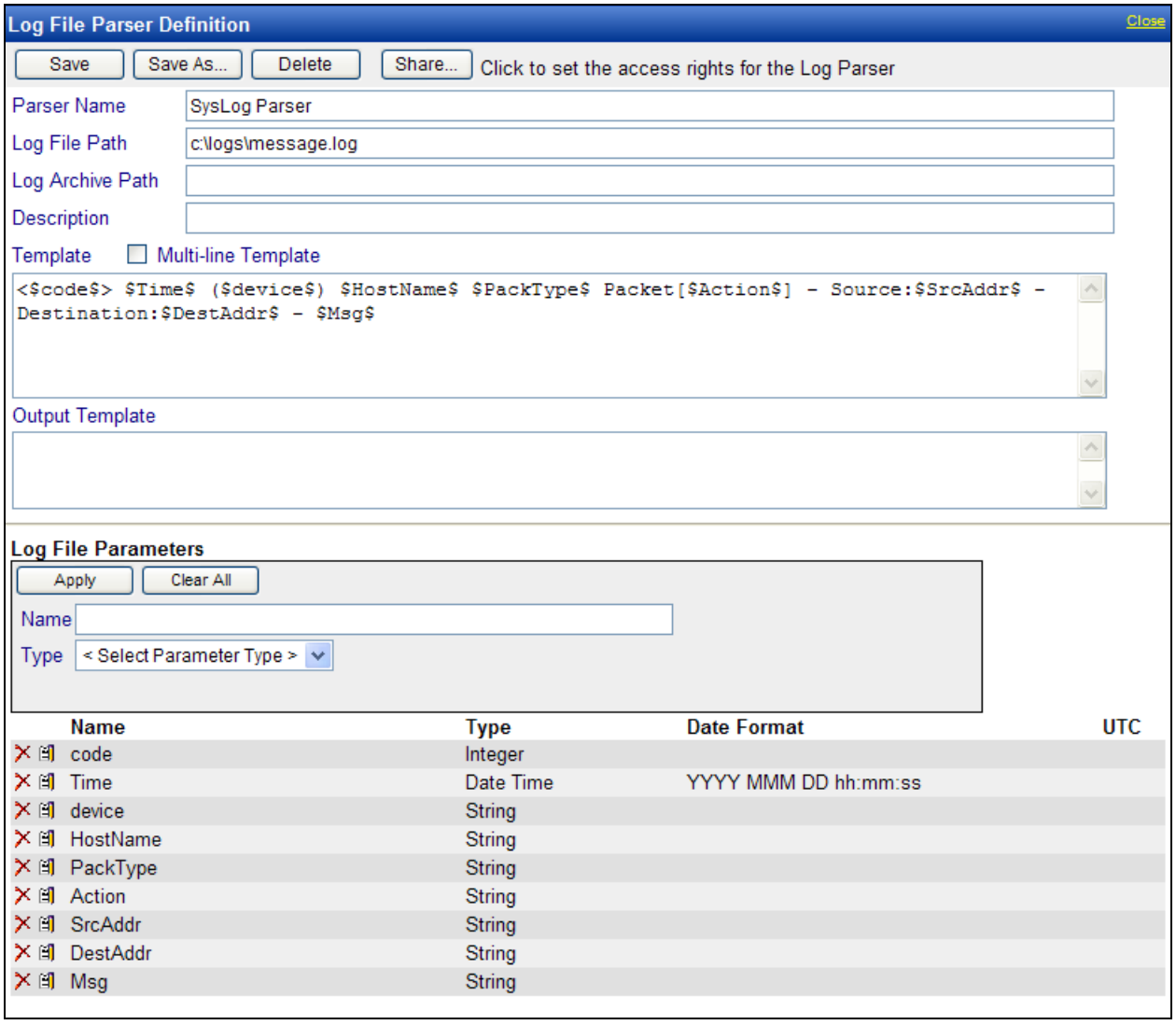
> **Nota:** Haga clic en el botón **Guardar** al menos una vez para ver la sección **Parámetros de archivo de registro** del cuadro de diálogo.

El texto no usado para completar parámetros debe coincidir con el texto en la entrada de registro. Por ejemplo: la cadena "`] - Source:`" debe coincidir con el texto de la entrada del registro, incluido el carácter de espacio antes del guión.

Defina los parámetros:

Nombre de parámetro	**Tipo de parámetro**	**ParsedResult**
código	Entero	189
Hora	datetime en formato "AAAA MMM DD hh:mm:ss" , no UTC	2006-11-08 11:57:48
Dispositivo	Cadena	FVS114-ba-b3-d2
HostName	Cadena	71.121.128.42
PackType	Cadena	ICMP
Acción	Cadena	Destino inalcanzable
SrcAddr	Cadena	192.168.0.186
DestAddr	Cadena	192.168.0.1
Msj	Cadena	[Recibir]

Paso 3: Especifique las plantillas y defina los parámetros.



Ejemplo 2 – Incluye el símbolo % (comodín)

Comience con una entrada de registro típica desde el archivo de registro que desea monitorear:

```
<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 el texto innecesario en el archivo de registro que desea monitorear:

```
<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]
```

En la plantilla, reemplace el texto innecesario tachado de arriba con un carácter de comodín de signo de porcentaje (%). Reemplace otro texto con los parámetros:

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

Defina los parámetros:

Nombre de parámetro	Tipo de parámetro	ParsedResult
código	Entero	`189`
Hora	datetime en formato `YYYY MMM DD hh:mm:ss`	`2006-11-08 11:57:48`
HostName	Cadena	`71.121.128.42`
PackType	Cadena	`ICMP`
SrcAddr	Cadena	`192.168.0.186`
DestAddr	Cadena	`192.168.0.1`

Ejemplo 3: entradas de registro de líneas múltiples

Comience con una entrada de registro típica de líneas múltiples desde el archivo de registro que desea monitorear:

```
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 el texto que debe ignorarse y el texto que debe completarse por parámetros.

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

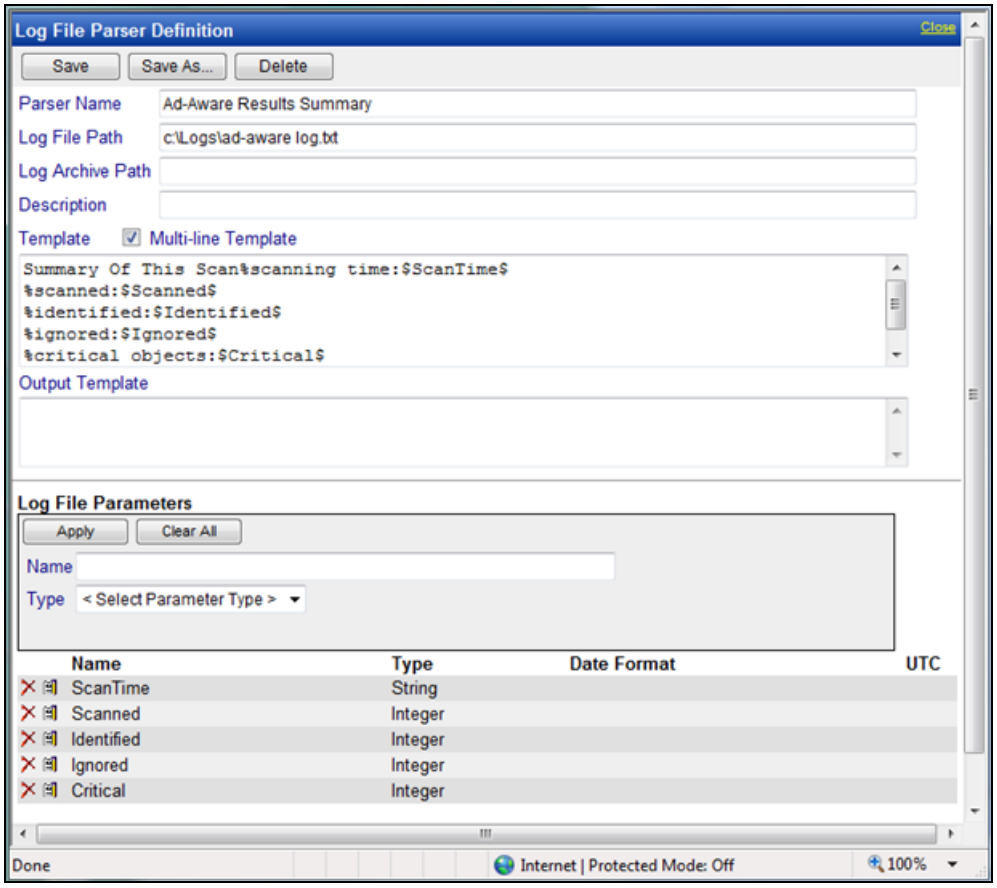
En la plantilla, reemplace el texto tachado con un comodín de signo de porcentaje (%). Reemplace el texto subrayado con parámetros.

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

Defina los parámetros:

Nombre de parámetro	Tipo de parámetro	ParsedResult
ScanTime	Cadena	00:02:32.765
Escaneados	Entero	91445
Identificados	Entero	0
Ignorado	Entero	0
Crítico	Entero	0

Paso 3: Especifique las plantillas y defina los parámetros.

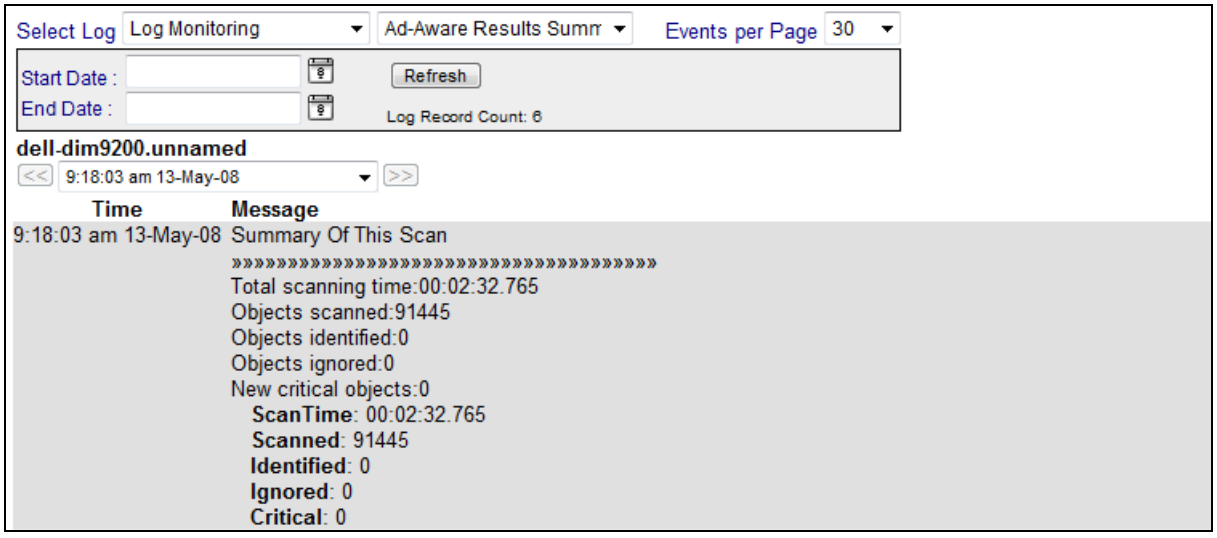


Ejemplo 4: plantilla de salida

Comience con una entrada de registro típica de líneas múltiples desde el archivo de registro que desea 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
```

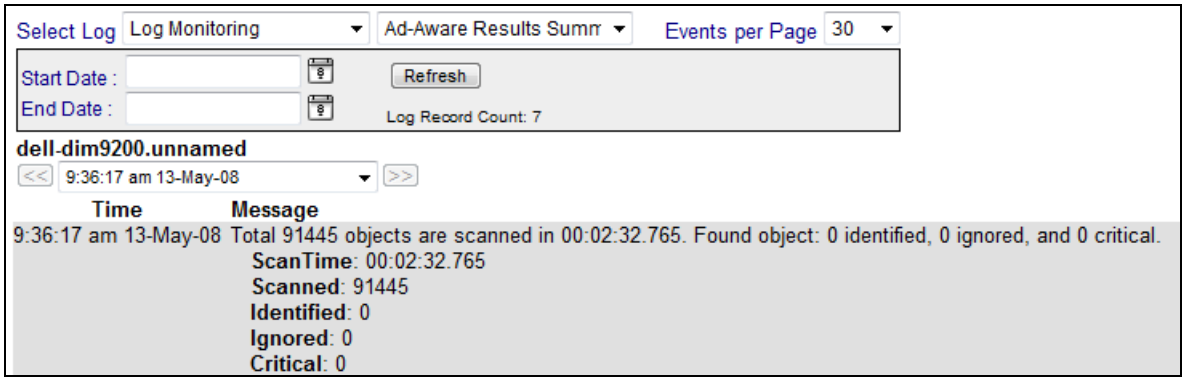
Los datos de arriba se registrarán como el cuerpo del mensaje en el registro de monitoreo si no se especifica una plantilla de salida. El siguiente es un ejemplo de la salida en Monitoreo de registro sin especificar la plantilla de salida:



En la plantilla de salida, especifique una plantilla usando los parámetros definidos:

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

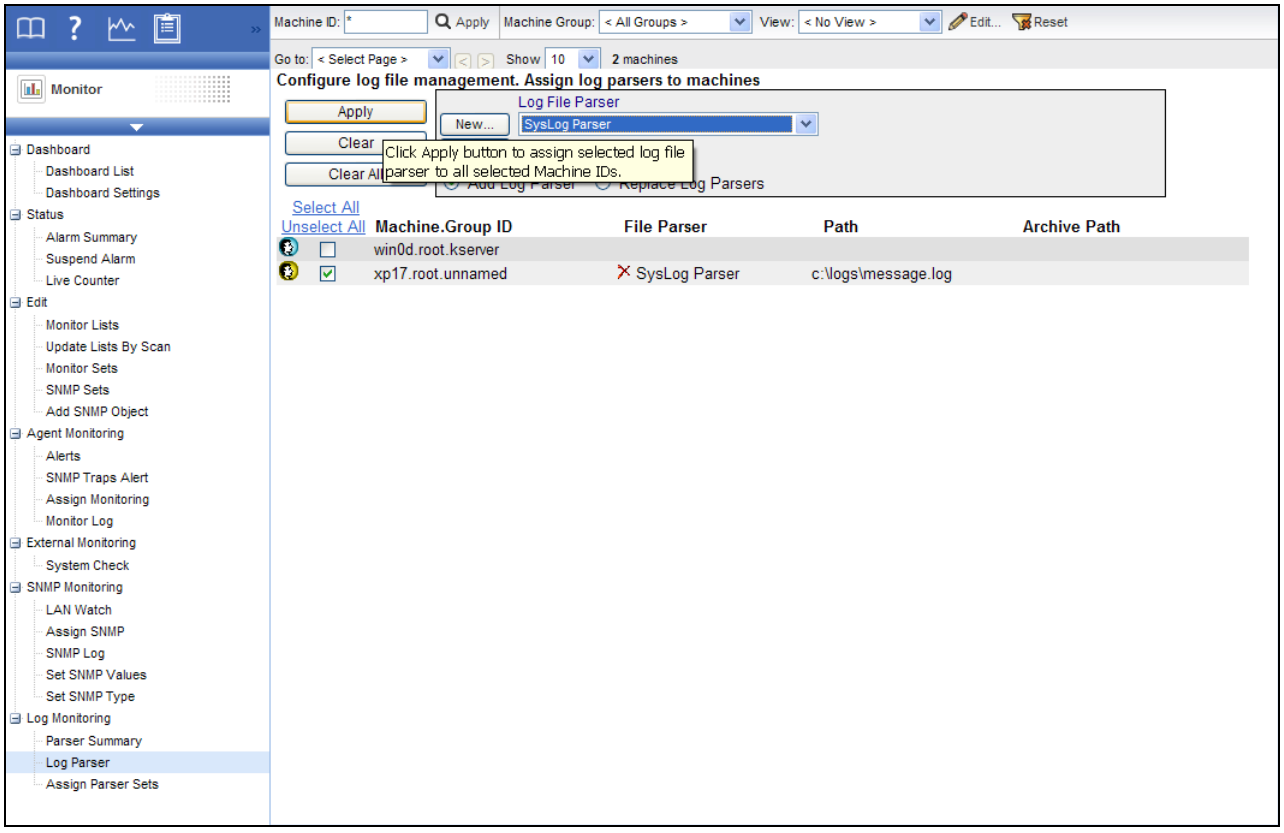
El siguiente es un ejemplo de la salida en Monitoreo de registro después de especificar una plantilla de salida:



Paso 4: Asignar la definición de analizador de registro

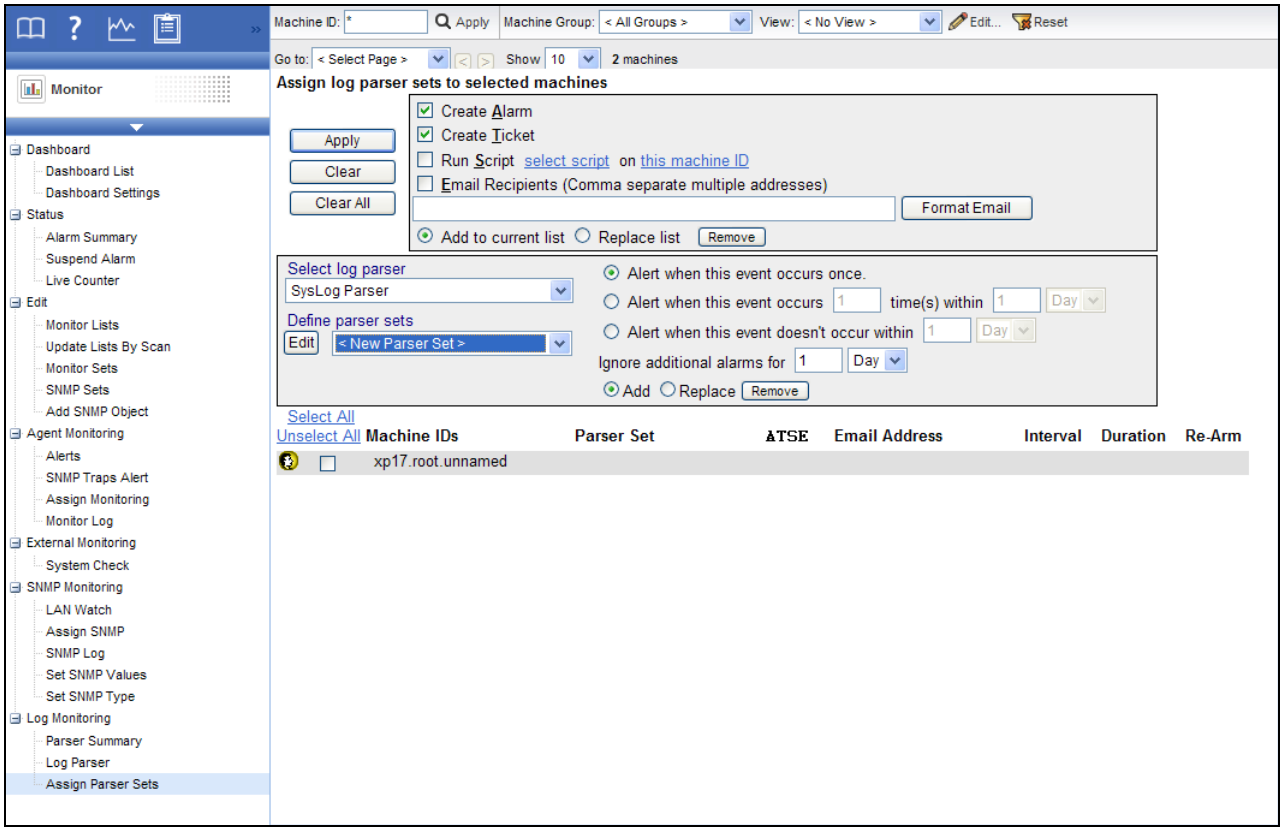
Debe asignarse una definición que se haya completado del analizador de archivo de registro a una o varias ID de máquina usando la función **Analizador de registro**. Seleccione las ID de máquinas a las cuales aplicar la definición y haga clic en el botón **Aplicar**. Esto indica que la definición de analizador

puede ser usada por las máquinas seleccionadas, pero el análisis no se produce hasta que selecciona los criterios de filtro para los datos de registro que se están recopilando y asigna las condiciones de alerta, como se describe en los Pasos 5 y 6.

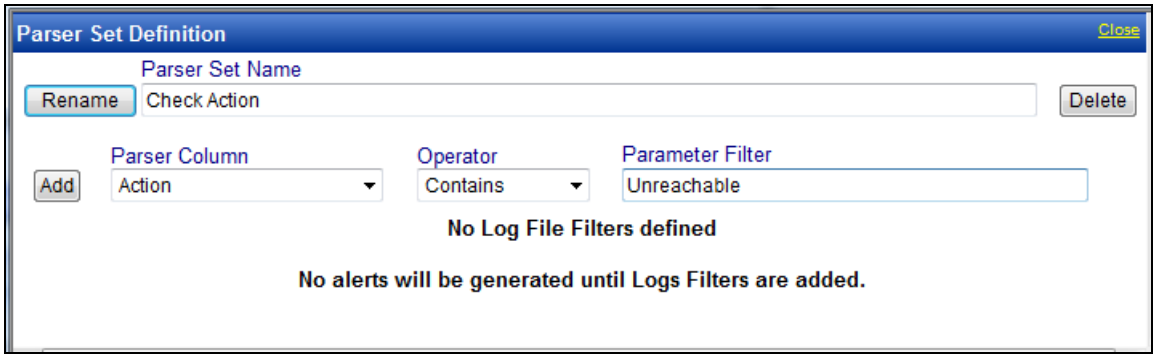


Paso 5: Defina las condiciones de recopilación y alertas

Haga clic en **Asignar conjuntos de analizador** debajo de **Monitoreo de registro** en la lista de funciones. Seleccione la definición del analizador de registro de la lista desplegable **Seleccionar analizador de registro**. A continuación, seleccione `<New Parser Sets>` de la lista desplegable **Definir conjuntos de analizadores**. *Un conjunto de analizadores de registros es un conjunto de condiciones que deben ser verdaderas acerca del análisis de una entrada del registro a fin de incluirlas en el registro de "supervisión de registros" y opcionalmente crear una alerta para ellas.* Esto garantiza que sólo se publiquen las entradas relevantes en el registro de "supervisión de registros". Un conjunto de analizador de registro es específico para un analizador de registro. Puede definir múltiples conjuntos de analizador de registro para el mismo analizador de registro y activar un conjunto de alertas diferente para cada conjunto de analizador de registro.



Defina las condiciones de alerta. En el siguiente ejemplo, se crea una entrada en el registro de "supervisión de registros" si la entrada se analiza de manera tal que el parámetro `Action` contiene el texto `Unreachable`.



Operadores para parámetros

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

El **Filtro de parámetro** para **Hora** puede estar en alguno de los siguientes formatos. Una cadena de filtro que termina con `Z` indica la hora en 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`

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

Conjuntos de analizador y condiciones

Las condiciones están definidas en un conjunto de analizador. Puede asignar múltiples condiciones a un conjunto de analizador. También puede asignar múltiples conjuntos de analizador a un analizador de registro. Una entrada de registro debe cumplir con todas las condiciones dentro de un conjunto de analizador a fin de activar la recopilación de datos y/o el alerta. Tenga en cuenta que este comportamiento es diferente de las alertas de registro de evento y otros conjuntos de monitores. Por ejemplo:

Contenidos de 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"
```

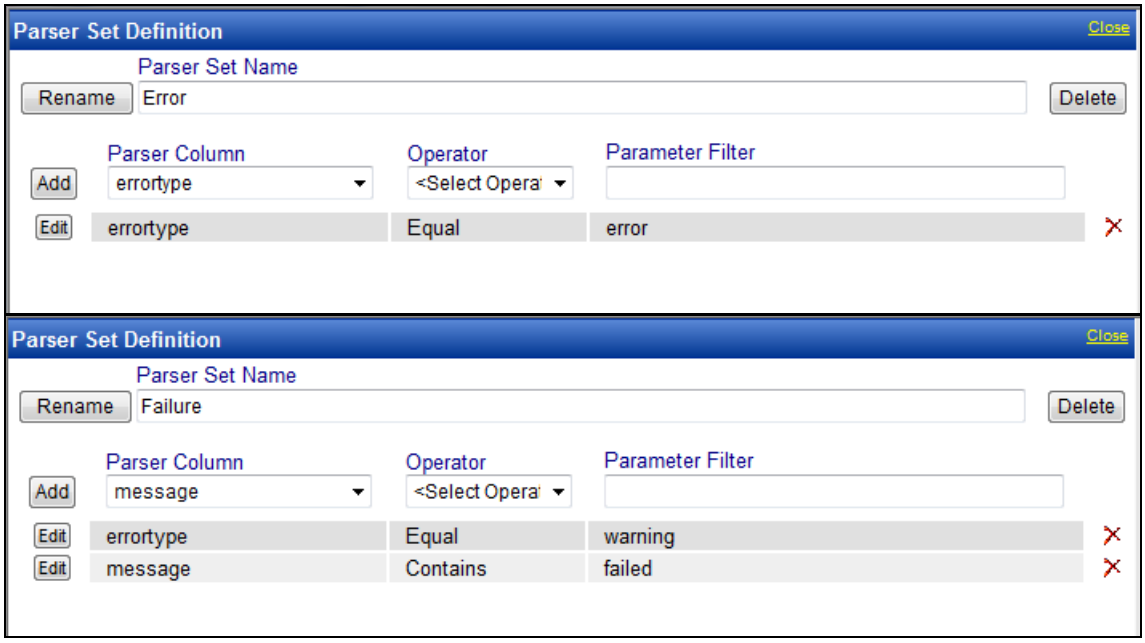
Plantilla de una línea:

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

Para recopilar entradas que cumplan con una de las siguientes condiciones debe definir dos conjuntos de analizador y asignarlos al analizador de registro:

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

A continuación encontrará las correspondientes capturas de pantallas para estos dos conjuntos de analizador:

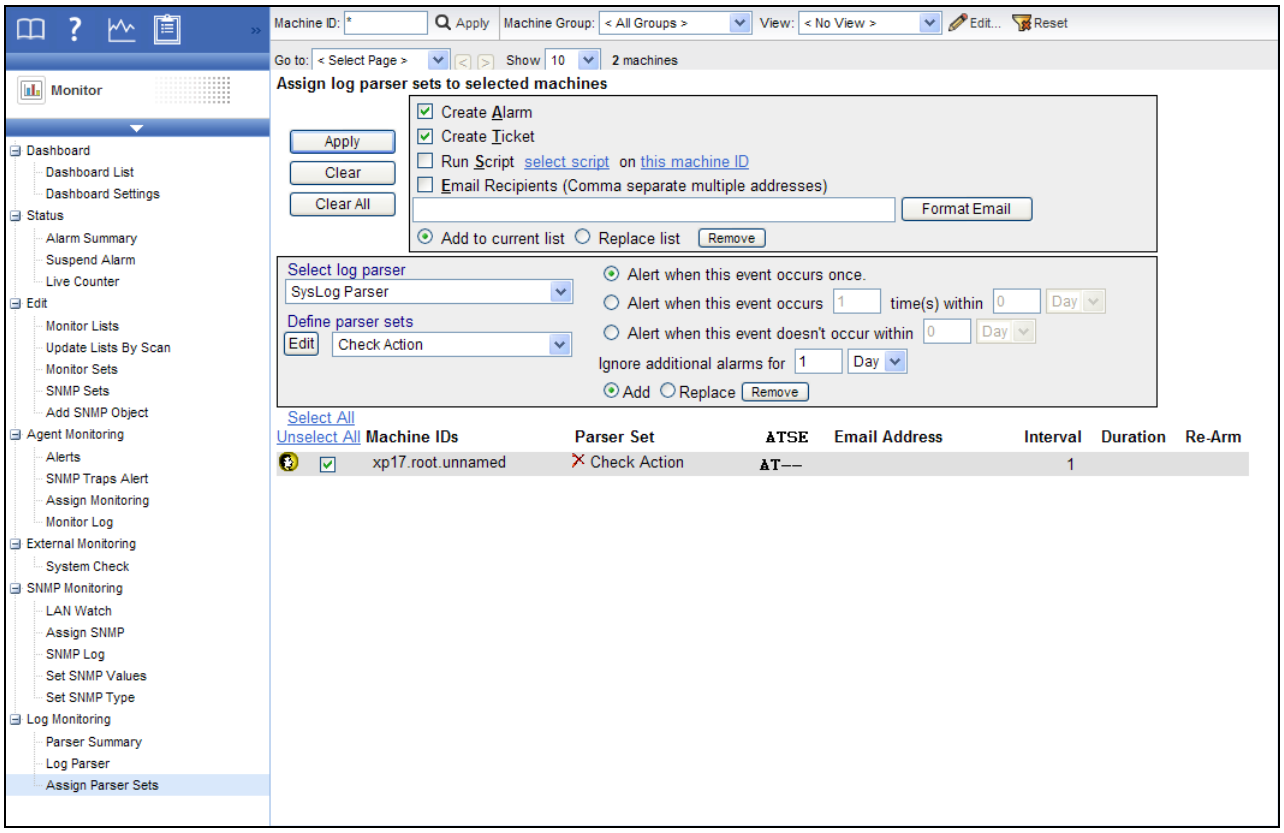


Paso 6: Asignar conjunto de analizador

Seleccione una ID de máquina, opciones de alarma y tipos de alertas y luego haga clic en el botón **Aplicar** para asignar el conjunto de analizador de registro a una ID de máquina. Una vez que la ID de máquina reciba la configuración del analizador de registro, el agente en la máquina administrada comenzará a analizar el archivo de registro *cada vez que se actualice el archivo de registro.*

Notificación

El agente recolecta entradas de registro y crea una entrada en el registro "supervisión de registros" sobre la base de los criterios definidos por el conjunto de analizadores, *independientemente de si alguno de los métodos de notificación está activado.* No es necesario que sea notificado cada vez que se crea una nueva entrada de monitoreo de registros. Simplemente puede revisar el registro de "Supervisión de registros" en forma periódica, según le resulte conveniente.

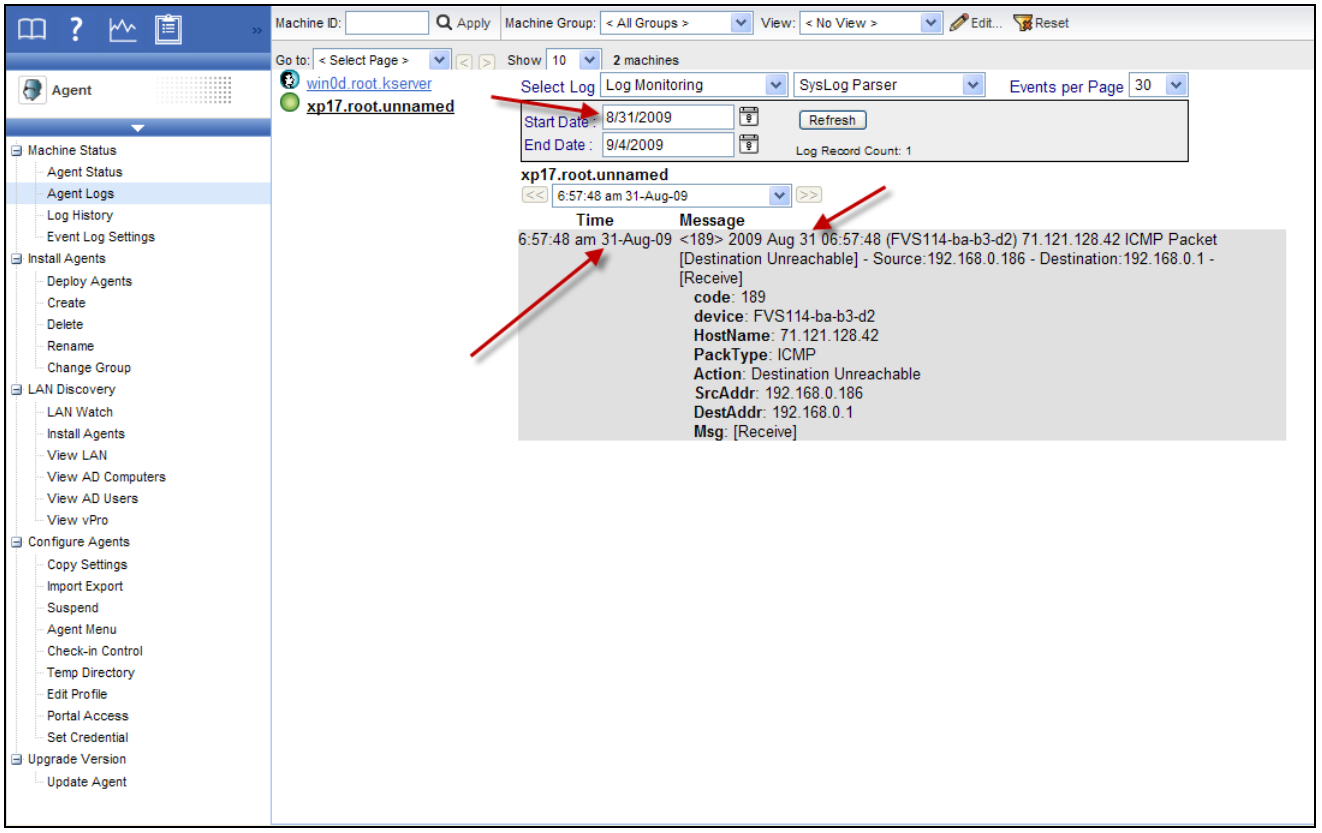


Paso 7: Revise el registro de "Supervisión de registros"

Las entradas de Monitoreo de registro se muestran en **Monitoreo de registro**, al cual puede accederse utilizando:

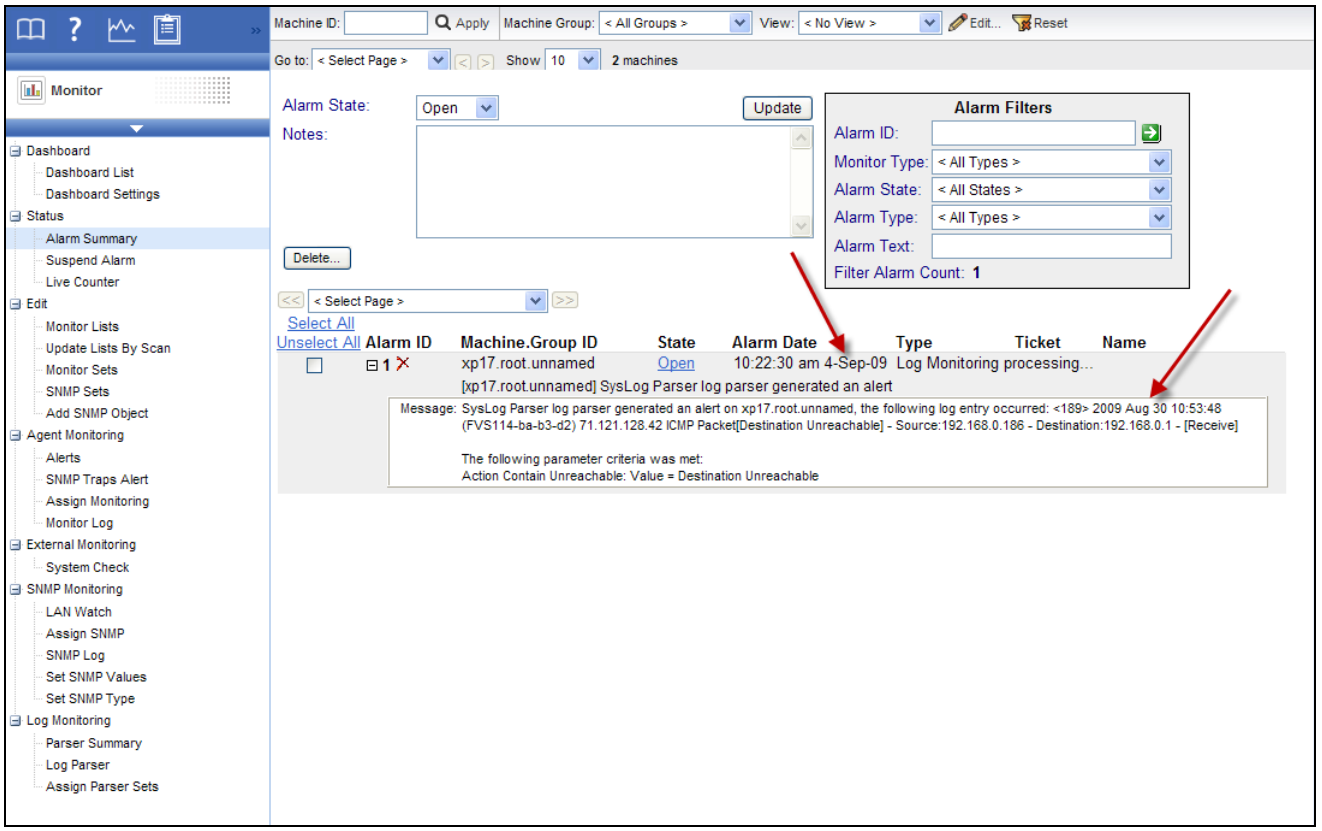
- Agentes > Registros de agente > Supervisión de registros > (definición de analizadores)
- Live Connect > Datos de agente > Registros de agente > Supervisión de registros > (definición de analizadores). Live Connect se muestra al hacer clic en el ícono de estado registrado de una ID de máquina seleccionada.
- Auditoría > Resumen de máquina > pestaña Registros de agente > Supervisión de registros > (definición de analizadores). La página Resumen de máquina también puede mostrarse presionado *Alt y haciendo clic* en el ícono de estado registrado de una ID de máquina seleccionada.
- Info Center > Elaboración de informes > Informes > Monitor - Registros > informe de Supervisión de registros.

Estas imágenes de muestra muestran el parámetro $Time$ que se está usando para las entradas de Monitoreo de registro. *Los filtros de fecha y hora en las vistas y los informes se basan en la hora de la entrada de registros.* Si incluye un parámetro `$Time$` mediante el tipo de datos `Date Time` en su plantilla, **Supervisión de registros** usa la hora almacenada en el parámetro `$Time$` como la hora de entrada del registro. Si *no* se incluye un parámetro `$Time$` en su plantilla, la hora en la que se agregó la entrada a **Supervisión de registros** sirve como la hora de entrada del registro. Asegúrese de seleccionar un rango de fecha que muestre las fechas de entradas de registro.



Paso 7: Revise el registro de "Supervisión de registros"

Por el contrario, las fechas de alarmas se basan en la fecha en que se creó la alarma, no en la fecha de las entradas del registro "Supervisión de registros".



Índice

I

P