ManageEngine
EventLog Analyzer

Atividade de sessão de auditoria em redes

www.manageengine.com/br/eventlog/

Atividade de sessão de auditoria em redes

O monitoramento de atividades da sessão é uma das formas mais básicas, porém importantes, pelas quais os administradores analisam a atividade da rede. Os detalhes da sessão mostram quando os usuários estão conectados à rede, bem como um detalhamento das atividades de rede específicas dos usuários durante cada uma. Tudo isso ajuda a estabelecer uma linha de base sólida para explicar as interações dos usuários com a rede.

Usos das informações da sessão

As informações da sessão ajudam os administradores a entender os seguintes aspectos de sua rede:

> **Quem está usando a rede:** Saiba quais usuários estão usando ativamente a rede para que seja mais fácil identificar usuários que não deveriam estar logados.

> **Como eles fazem login:** Diferencie entre usuários que efetuam login diretamente em uma máquina e aqueles que efetuam login por meio de uma área de trabalho remota ou conexão de serviços de terminal.

> **De onde eles fazem login:** Identifique quais máquinas estão sendo usadas para estabelecer conexões remotas.

> **Em qual sistema eles fazem login:** Descubra quais dispositivos são usados com mais frequência na rede.

> **Quando eles fazem login e logoff:** Analise a duração de várias sessões e identifique as que estão ociosas, assim como as que não foram logadas. Observar essas estatísticas para um dispositivo específico pode fornecer uma ideia do seu nível de envolvimento.

A necessidade de uma ferramenta de auditoria

Dispositivos individuais geram logs de login e logoff, que fornecem informações de sessão; no entanto, eles não oferecem relatórios nativos e capacidades de análise de forma holística. O uso de uma ferramenta de auditoria resoluta e centralizada resolve este problema e oferece os seguintes benefícios:

> Uma visão geral abrangente da rede: reúna as informações da sessão de vários dispositivos da rede e apresente-as de maneira unificada.

> Padrões de login: identifique hosts e usuários com o maior número de logins na rede.

> Anomalias: identifique todas as sessões estranhas, como logins fora do horário comercial, logins de usuários sem permissões suficientes e afins.

Monitoramento de atividade de sessão com o EventLog Analyzer

Com o EventLog Analyzer, rastrear a atividade da sessão em uma rede é rápido e fácil. A solução fornece relatórios predefinidos que rastreiam sessões inteiras do usuário do início ao fim, incluindo detalhes de sua atividade durante a sessão.

Onde acesso esses relatórios?

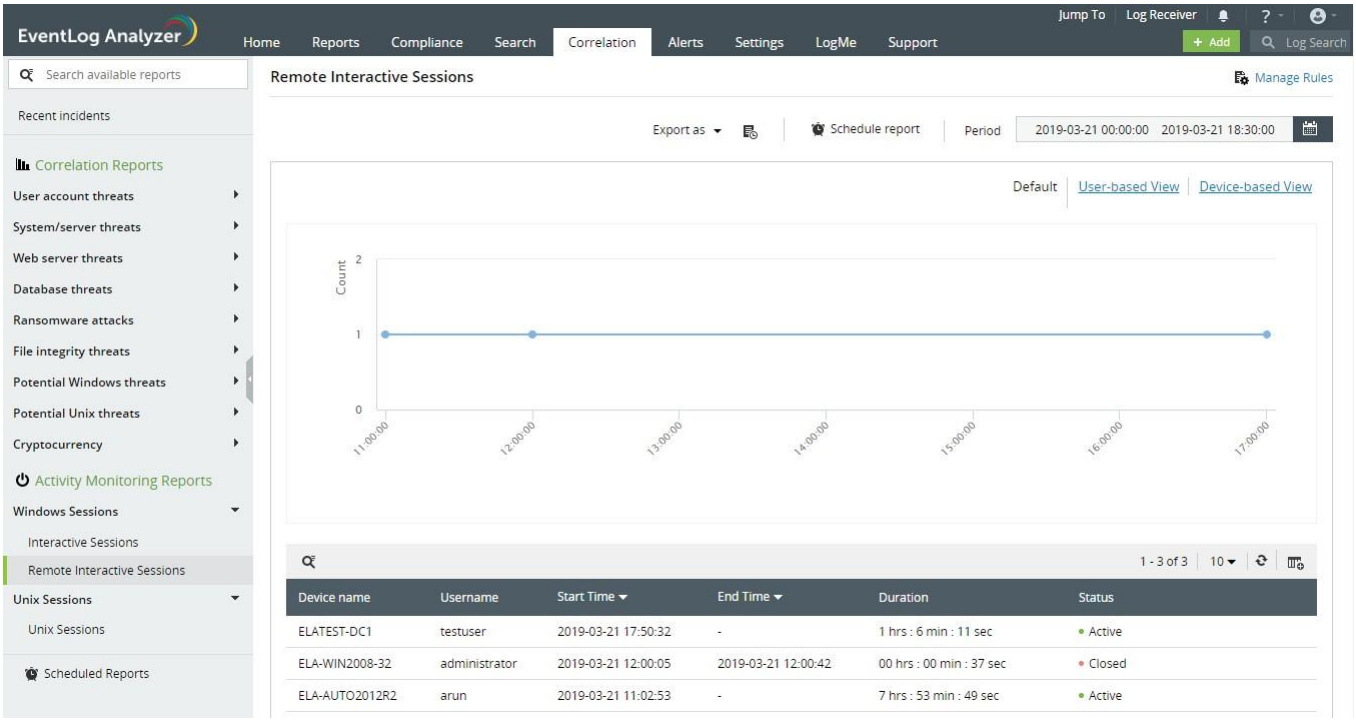
Acesse os relatórios de atividade da sessão indo para a guia Correlação e clicando no relatório desejado em Relatórios de Monitoramento de Atividade no painel esquerdo.

Sobre o que esses relatórios fornecem informações?

Atualmente, os relatórios fornecidos cobrem os seguintes tipos de sessões:

- Sessões interativas do Windows
- Sessões interativas remotas do Windows
- Sessões do Windows Password Manager Pro
- Sessões Unix

Trabalhando com relatórios de atividade de sessão



Os relatórios de atividade da sessão ajudam a:

- Identificar, em um piscar de olhos, quem está ativo na rede em um determinado momento.
- Escolher sessões encerradas incorretamente.
- Analisar quantas sessões ocorrem em vários momentos e identificar períodos anormalmente ativos ou ociosos.
- Aprofundar-se nas sessões de interesse e analisar exatamente o que ocorreu durante cada sessão.
- Identificar os usuários mais ativos e os dispositivos que eles usam. Da mesma forma, você também pode identificar dispositivos usados com frequência na rede e os usuários que estão ativos neles.

A exibição padrão de um relatório de atividade da sessão fornece as seguintes informações:

- O gráfico mostra o número de sessões iniciadas em vários intervalos durante a janela de tempo selecionada.
- A tabela lista cada sessão e especifica detalhes como nomes de usuários e dispositivos, horários de início e término, duração e status da sessão (ativa ou finalizada).
- Para sessões que terminaram, também é dado o motivo pelo qual terminaram; por exemplo, se a sessão foi desconectada ou o dispositivo foi desligado. Para sessões em andamento, a coluna de duração exibe um cronômetro ao vivo para mostrar quanto tempo o usuário está ativo.
- Para rastrear a atividade de um usuário durante uma sessão, você pode clicar em Exibir Histórico na entrada da respectiva sessão na tabela. A página que se abre apresenta uma linha do tempo, que lista as diversas ações do usuário em ordem cronológica.

Você também pode alternar o relatório para uma exibição com base em usuário ou dispositivo. Você pode fazer isso selecionando os links de exibição com base em usuário ou exibição com base em dispositivo que aparecem quando você passa o mouse sobre o gráfico.

> **Visualização baseada em usuário:** informa o número de sessões iniciadas por cada usuário durante a janela de tempo selecionada e os dispositivos nos quais elas estavam ativas.

> **Visualização baseada em dispositivo:** informa o número de sessões iniciadas em cada dispositivo durante a janela de tempo selecionada e os usuários ativos nesses dispositivos.

Para visualizar as sessões de um determinado usuário ou dispositivo, você pode:

- Usar a barra de pesquisa em qualquer um dos relatórios.
- Navegar até a visualização baseada em usuário ou dispositivo e clicar no respectivo nome de usuário/dispositivo.

Regras de sessão definidas pelo usuário

Normalmente, uma sessão começa quando um usuário faz login em um dispositivo e termina quando ele faz logoff ou o dispositivo é desligado. Os relatórios de atividade de sessão predefinidos descritos acima fornecem informações com base nesta definição. No entanto, as sessões típicas duram várias horas e, se você estiver interessado em uma específica, ainda poderá ter muitas informações para analisar.

O EventLog Analyzer leva você além do modelo simples de login/logoff de uma sessão e permite que você defina as condições iniciais e finais de uma sessão — ou regras de atividade. Essas regras de atividade consistem em uma sequência de eventos de rede. Dessa forma, quando ocorrerem os eventos descritos por essas regras, você poderá acompanhar todas as atividades que ocorrerem entre elas.

Por exemplo, você pode querer monitorar a atividade em um de seus servidores de arquivos críticos. Você deseja monitorar os usuários que efetuam login remotamente no servidor de arquivos e acessam um arquivo após várias tentativas malsucedidas. Você também está interessado em rastrear como eles obtiveram esse acesso. Para monitorar isso, você pode criar uma regra de atividade da seguinte maneira:

> **Regra de início da atividade:** login remoto no servidor de arquivos, seguido por algumas tentativas malsucedidas de acessar um arquivo.

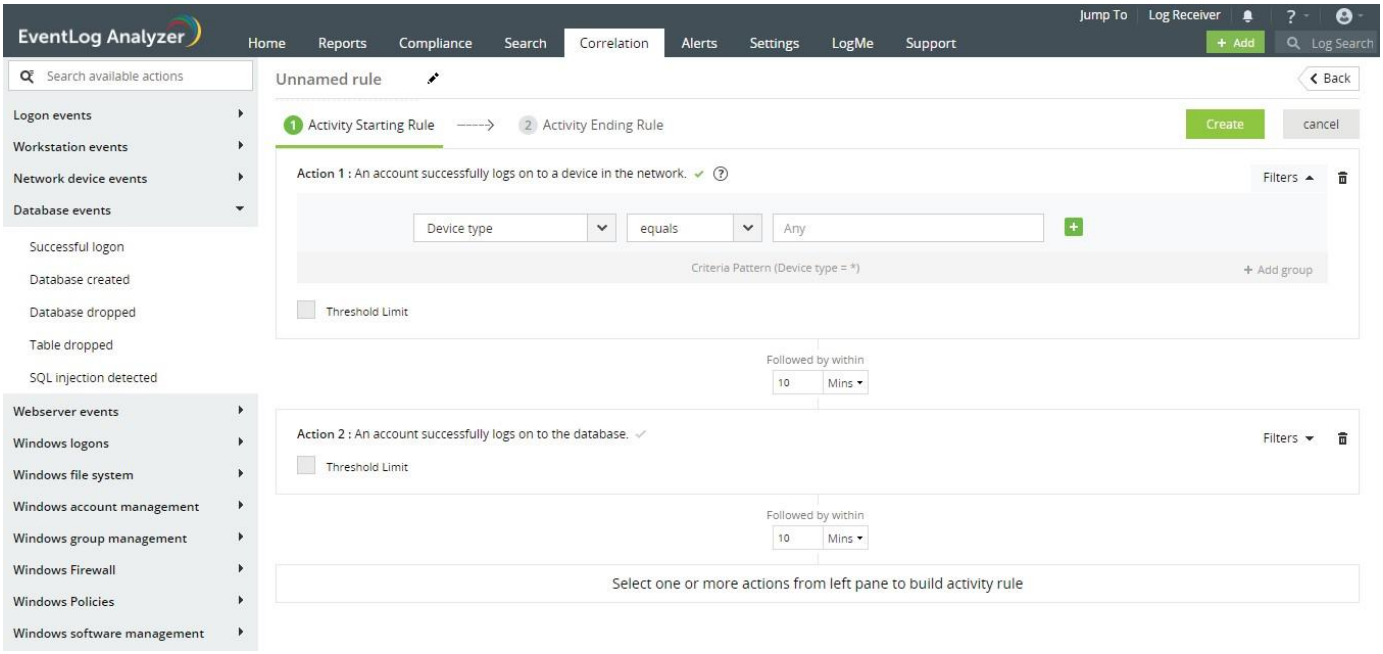
> **Regra de finalização da atividade:** acesso bem-sucedido ao arquivo.

Ao criar uma regra de atividade de sessão dessa maneira, você não apenas monitora o acesso não autorizado a arquivos confidenciais, mas também identifica brechas de segurança em seu servidor de arquivos que permitem esses acessos.

Como criar regras de atividade

Os relatórios de atividade da sessão podem ser encontrados na guia Correlação. Crie uma regra de atividade recente acessando:

Correlação > Gerenciar Regras > Regras de Atividade > +Criar Regra de Atividade



A interface do construtor de regras é igual à do construtor de regras de correlação. Você pode aprender como usá-lo neste vídeo. As regras de atividade de sessão são como as de correlação e as únicas diferenças são:

> **As regras de atividade da sessão são divididas em duas sub-regras:** a regra de início e a de término da atividade definem como uma sessão começa e termina, respectivamente.

> **O uso de uma ação primária:** cada sub-regra de uma regra de atividade tem uma ação principal. Por padrão, é a primeira ação de cada sub-regra, mas você pode designar qualquer uma como principal selecionando a marca de seleção verde ao lado da ação necessária. Você pode comparar os campos das ações primárias de ambas as regras usando o link para o filtro.

Conclusão

O EventLog Analyzer é extremamente eficaz na auditoria de sessões de usuários na rede de uma organização. Os relatórios fornecem informações granulares sobre a atividade do usuário e permanecem atualizados com todas as atividades em sua rede. Essas regras permitem que você monitore sessões definidas de forma personalizada e rastreie a atividade do usuário com relatórios simples e diretos. Com a interface fácil de usar do EventLog Analyzer e os relatórios intuitivos, é fácil visualizar todas as informações de sessão necessárias e identificar rapidamente padrões ou anomalias.

ManageEngine
EventLog Analyzer

O EventLog Analyzer é uma solução de gerenciamento de logs e conformidade de TI baseada na web, em tempo real, que combate ataques de segurança de rede. Com capacidades abrangentes de gerenciamento de logs, o EventLog Analyzer ajuda as organizações a atenderem às diversas necessidades de auditoria. Também oferece relatórios e alertas de conformidade prontos para uso, que facilmente atendem aos rigorosos requisitos normativos da TI.

Obter orçamento Download

Ligação gratuita
+1 844 649 7766

Número de Discagem Direta
EUA: +1-408-352-9254

eventlog-support@manageengine.com

www.manageengine.com/br/eventlog/