IBM Security QRadar
Versão 7.2.2

Notificações do Sistema de Resolução de Problemas

SC43-4521-00

Observação

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 35.

Índice

Capítulo 1. Introdução às notificações do sistema

O Guia de Notificações do Sistema de Resolução de Problemas do IBM Security QRadar fornece informações sobre como resolver problemas e notificações do sistema que são exibidas no Console do QRadar. As notificações do sistema que são exibidas no Console podem aplicar-se a qualquer dispositivo ou produto do QRadar em sua implementação. O Guia de Notificações do Sistema de Resolução de Problemas *IBM Security QRadar* fornece informações sobre como resolver problemas e notificações do sistema que são exibidas no Console do QRadar. As notificações do sistema que são exibidas no Console podem aplicar-se a qualquer dispositivo ou produto do QRadar em sua implementação.

A menos que observado o contrário, todas as referências para o QRadar se referem aos produtos a seguir:

- IBM® Security QRadar SIEM
- IBM Security QRadar Log Manager
- IBM Security QRadar Network Anomaly Detection

Público alvo

Os administradores da rede responsáveis pela instalação e configuração dos sistemas do QRadar devem estar familiarizados com os conceitos de segurança da rede e com o sistema operacional Linux.

Documentação técnica

Para localizar a documentação do produto IBM Security QRadar na web, inclusive toda a documentação traduzida, acesse o IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Para obter informações sobre como acessar mais documentação técnica na biblioteca de produtos QRadar, consulte Acessando o IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Entrando em contato com o suporte ao cliente

Para obter informações sobre como entrar em contato com o suporte ao cliente, consulte a Nota Técnica de Suporte e Download (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Declaração de boas práticas de segurança

A segurança do sistema de TI envolve a proteção de sistemas e as informações através da prevenção, detecção e resposta para acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mau uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança individual pode ser completamente eficaz na prevenção do acesso ou uso impróprio. Os sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança abrangente, que envolverá necessariamente procedimentos operacionais adicionais e podem

requerer que outros sistemas, produtos ou serviços sejam mais efetivos. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU TORNAM A SUA EMPRESA IMUNE CONTRA CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PESSOA.

Capítulo 2. Resolução de problemas de notificações do sistema do QRadar

Use as notificações do sistema que são geradas pelo IBM Security QRadar para monitorar o status e o funcionamento do seu sistema. Os processos e ferramentas de software e hardware monitoram continuamente os dispositivos do QRadar e fornecem informações, avisos e mensagens de erro para usuários e administradores.

Conceitos relacionados:

Capítulo 3, "Notificações de erro para dispositivos do QRadar", na página 5
As notificações de erro nos produtos do IBM Security QRadar requerem uma resposta do usuário ou administrador.

Capítulo 4, "Notificações de aviso para dispositivos do QRadar", na página 15
As notificações de funcionamento do sistema do IBM Security QRadar são mensagens proativas de falhas reais ou iminentes de software ou hardware.

Capítulo 5, "Notificações de informação para dispositivos do QRadar", na página 31
O IBM Security QRadar fornece mensagens de informação sobre o status ou resultado de um processo ou ação

Capítulo 3. Notificações de erro para dispositivos do QRadar

As notificações de erro nos produtos do IBM Security QRadar requerem uma resposta do usuário ou administrador.

Erro de falta de memória

`O aplicativo ficou sem memória.`

Explicação

Quando o sistema detectar que nenhuma memória ou espaço de troca estiver disponível, o aplicativo ou o serviço poderá parar de funcionar. Problemas de falta de memória são causados pelo software, ou por consultas e operações definidas pelo usuário que esgotam a memória disponível.

Resposta do Usuário

Revise a mensagem de erro gravada no arquivo `/var/log/qradar.log`. O reinício de um serviço pode parar o aplicativo ofensivo ou o serviço e redistribuir os recursos.

Se você usar Java™ Database Connectivity (JDBC) ou o protocolo de arquivo de log para importar vários registros a partir de uma origem de log, o sistema poderá usar recursos. Se diversas importações de dados grandes ocorrerem simultaneamente, será possível escalonar os intervalos de horário de início.

O Acumulador Não Pode Ler a Definição de Visualização para Dados Agregados

`Acumulador: não é possível ler a definição de visualização de dados agregados para evitar um problema de dessincronização. As visualizações de dados agregados não podem mais ser criadas ou carregadas. Os gráficos de série temporal não funcionarão mais, bem como o relatório.`

Explicação

Ocorreu um problema de sincronização. A configuração de visualização de dados agregados que está na memória gravou dados errados no banco de dados.

Para evitar distorção de dados, o sistema desativa as visualizações de dados agregados. Quando as visualizações de dados agregados forem desativadas, os gráficos de série temporal, as procuras salvas e os relatórios planejados exibirão gráficos vazios.

Resposta do Usuário

Entre em contato com o suporte ao cliente.

Erro de Atualização Automática

`As atualizações automáticas não puderam concluir a instalação. Consulte o Log de Atualização Automática para obter detalhes.`

Explicação

O processo de atualização encontrou um erro ou não pode se conectar a um servidor de atualização. O sistema não está atualizado.

Resposta do Usuário

Selecione uma das opções a seguir:

- Verificar o histórico de atualização automática para determinar a causa do erro de instalação.

  Na guia **Admin**, clique no ícone **Atualização Automática** e selecione **Visualizar Log**.
- Verificar se o console pode se conectar ao servidor de atualização.

  Na janela Atualizações, selecione **Alterar Configurações** e, em seguida, clique na guia **Avançado** para visualizar a configuração de atualização automática. Verifique o endereço no campo **Servidor da Web** para assegurar que o servidor de atualização automática está acessível.

O CRE Falhou ao Ler as Regras

`A última tentativa de ler regras (geralmente devido a uma mudança de regra) falhou. Consulte os detalhes da mensagem e o log de erro para obter informações sobre como resolver isso.`

Explicação

O Custom Rules Engine (CRE) em um Processador de Evento não pode ler uma regra para correlacionar um evento recebido. A notificação pode conter uma das mensagens a seguir:

- Se o CRE não puder ler uma única regra, na maioria dos casos, uma mudança recente na regra será a causa. A carga útil da mensagem de notificação exibe a regra ou a regra da cadeia de regras que é responsável.
- Em raras circunstâncias, a distorção de dados pode causar uma falha completa do conjunto de regras. Um erro de aplicativo é exibido e a interface do editor de regras pode se tornar irresponsivo ou gerar mais erros.

Resposta do Usuário

Para um único erro de leitura de regra, revise as opções a seguir:

- Para localizar a regra que está causando a notificação, desative temporariamente a regra.
- Edite a regra para reverter as mudanças recentes.
- Exclua e recrie a regra que está causando o erro.

Para erros de aplicativos em que o CRE falhou ao ler regras, entre em contato com o suporte ao cliente.

Backup Incapaz de Concluir uma Solicitação

`Backup: não é possível executar a Solicitação de Backup.`

Explicação

Um backup poderá falhar pelos motivos a seguir:

- O sistema não pode limpar a tabela de sincronização de replicação de backup.
- O sistema não pode excluir uma solicitação.
- O sistema não pode sincronizar o backup usando os arquivos no disco.
- O diretório de backup montado de NFS não está disponível ou possui opções incorretas de exportação de NFS (`no_root_squash`).
- Não é possível inicializar o backup on demand.
- Não é possível recuperar a configuração para o tipo de backup selecionado.
- Não é possível inicializar um backup planejado.

Resposta do Usuário

Inicie manualmente um backup para determinar se a falha ocorre novamente.

O Aplicativo do Monitor de Processo Falhou ao Ser Iniciado Diversas Vezes

`Monitor de Processo: o aplicativo falhou ao ser inicializado diversas vezes.`

Explicação

O sistema não pode iniciar um aplicativo ou um processo em seu sistema.

Resposta do Usuário

Revise as fontes de fluxo para determinar se um dispositivo foi interrompido ao enviar dados de fluxo ou se os usuários excluíram uma fonte de fluxo.

Remova o processo de fluxo usando o editor de implementação ou designe uma fonte de fluxo para os dados de fluxo. Na guia **Admin**, clique em **Fontes de Fluxo**.

O Monitor de Processo Deve Reduzir o Uso de Disco

`Monitor de Processo: o uso de disco deve ser reduzido.`

Explicação

O monitor de processo não pode iniciar processos devido a uma falta de recursos do sistema. Provavelmente, a partição de armazenamento no sistema está 95% ou mais cheia.

Resposta do Usuário

Libere algum espaço em disco, excluindo manualmente os arquivos ou alterando as políticas de retenção de dados de fluxo ou de evento. O sistema reiniciará automaticamente os processos do sistema quando o espaço em disco usado ficar abaixo de um limite de 92% de capacidade.

O Pipeline do Evento Descartou os Eventos

`Os Eventos/Fluxos foram descartados pelo pipeline do evento.`

Explicação

Se houver um problema com o pipeline do evento ou você exceder seu limite de licença, um evento ou fluxo poderá ser descartado.

Eventos e fluxos descartados não podem ser recuperados.

Resposta do Usuário

Revise as opções a seguir:

- Verifique as taxas de evento e de fluxo recebidos em seu sistema. Se o pipeline do evento estiver descartando eventos, expanda sua licença para manipular mais dados.
- Revise as mudanças recentes nas regras ou nas propriedades customizadas. As mudanças na regra ou na propriedade customizada podem causar mudanças nas taxas de evento ou de fluxo e podem afetar o desempenho do sistema.
- Determine se o problema está relacionado às notificações SAR. As notificações SAR podem indicar que há eventos e fluxos enfileirados no pipeline do evento. Normalmente, o sistema roteia eventos para armazenamento, em vez de descartar os eventos.
- Ajuste o sistema para reduzir o volume de eventos e de fluxos que inserem o pipeline do evento.

O Pipeline do Evento Descartou as Conexões

`As conexões foram descartadas pelo pipeline do evento.`

Explicação

Um protocolo baseado em TCP descartou uma conexão estabelecida com o sistema.

O número de conexões que podem ser estabelecidas por protocolos baseados em TCP é limitado para assegurar que as conexões sejam estabelecidas e os eventos sejam encaminhados. O Event Collection System (ECS) permite no máximo 15.000 manipulações de arquivos e cada conexão TCP usa três manipulações de arquivos.

Os protocolos TCP que fornecem notificações de conexão descartada incluem os protocolos a seguir:

- protocolo syslog TCP
- protocolo syslog TLS
- protocolo multilinhas TCP

Resposta do Usuário

Revise as opções a seguir:

- Distribua eventos para mais dispositivos. As conexões com outros processadores de eventos e fluxos distribuem a carga de trabalho a partir do console.
- Configure eventos de fonte de log TCP de prioridade baixa para usar o protocolo de rede UDP.

- Ajuste o sistema para reduzir o volume de eventos e de fluxos que inserem o pipeline do evento.

Atualização Automática Instalada com Erros

`Atualizações automáticas instaladas com erros. Consulte o Log de Atualização Automática para obter detalhes.`

Explicação

O motivo mais comum para erros de atualização automática é uma dependência do software ausente para um DSM, protocolo ou atualização do scanner.

Resposta do Usuário

Selecione uma das opções a seguir:

- Na guia **Admin**, clique no ícone **Atualização Automática** e selecione **Visualizar Histórico da Atualização** para determinar a causa do erro de instalação. É possível visualizar, selecionar e, em seguida, reinstalar um RPM com falha.
- Se não for possível reinstalar uma atualização automática através da interface com o usuário, faça download e instale manualmente a dependência ausente no console. O console replica o arquivo instalado para todos os hosts gerenciados.

Falha do Sistema HA de Espera

`Falha do Sistema HA de Espera.`

Explicação

O status do dispositivo secundário é alternado para `com falha` e o sistema não tem proteção de HA.

Resposta do Usuário

Revise as resoluções a seguir:

- Restaure o sistema secundário.

  Clique na guia **Admin**, clique em **Gerenciamento de Sistema e de Licença** e, em seguida, em **Restaurar Sistema**.
- Inspecione o dispositivo HA secundário para determinar se ele está desligado ou teve uma falha de hardware.
- Utilize o comando **`ping`** para verificar a comunicação entre o sistema primário e de espera.
- Verifique o comutador que conecta os dispositivos HA primário e secundário.

  Verifique os IPtables nos dispositivos primário e secundário.
- Revise o arquivo `/var/log/qradar.log` no dispositivo de espera para determinar a causa da falha.

Falha do Sistema High Availability (HA) Primário

`Falha do Sistema HA Primário.`

Explicação

O sistema primário não pode se comunicar com o sistema de espera porque o sistema primário não responde ou está com falha. O sistema secundário assumirá as operações a partir do sistema primário com falha.

Resposta do Usuário

Revise as resoluções a seguir:

- Inspecione o dispositivo HA primário para determinar se ele está desligado ou teve uma falha de hardware.
- Restaure o sistema primário.

  Clique na guia **Admin** e clique em **Gerenciamento de Sistema e de Licença**. No menu **Alta Disponibilidade**, selecione a opção **Restaurar Sistema**.
- Revise o arquivo `/var/log/qradar.log` no dispositivo de espera para determinar a causa da falha.
- Use o comando **`ping`** para verificar a comunicação entre os sistemas primário e de espera.
- Verifique o comutador que conecta os dispositivos HA primário e secundário.

  Verifique os IPtables nos dispositivos primário e secundário.

Falha ao Instalar a Alta Disponibilidade

`Ocorreu um problema ao instalar a Alta Disponibilidade no cluster.`

Explicação

Ao instalar um dispositivo de alta disponibilidade (HA), o processo de instalação vincula os dispositivos primário e secundário. O processo de configuração e instalação contém um intervalo de tempo para determinar quando uma instalação requer atenção. A instalação de alta disponibilidade excedeu o limite de tempo de seis horas.

Nenhuma proteção de HA estará disponível até que o problema seja resolvido.

Resposta do Usuário

Entre em contato com o suporte ao cliente.

Falha ao Desinstalar um Dispositivo HA

`Ocorreu um problema durante a remoção de High Availability no cluster.`

Explicação

Ao remover um dispositivo de alta disponibilidade (HA), o processo de instalação remove as conexões e os processos de replicação de dados entre os dispositivos primário e secundário. Se o processo de instalação não puder remover corretamente o dispositivo HA do cluster, o sistema primário continuará a funcionar normalmente.

Resposta do Usuário

Tente remover o dispositivo de alta disponibilidade uma segunda vez.

Erro de Inicialização de Scanner

`A inicialização de um scanner falhou.`

Explicação

Uma varredura de vulnerabilidade planejada não pôde se conectar a um scanner externo ao iniciar o processo de importação de varredura.

Os problemas de inicialização de varredura são causados tipicamente por problemas de credenciais ou de conectividade com o scanner remoto. Scanners que falham ao ser inicializados exibem mensagens de erro detalhadas no texto de ajuda instantânea de uma varredura planejada com um status com falha.

Resposta do Usuário

Siga estas etapas:

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. Clique no ícone **Planejar Scanners VA**.
4. Na lista de scanners, passe o cursor na coluna **Status** de qualquer scanner para exibir uma mensagem detalhada de êxito ou de falha.

Inicialização de Filtro com Falha

`A inicialização do filtro de análise de tráfego falhou.`

Explicação

Se uma configuração não for salva corretamente, ou se um arquivo de configuração estiver corrompido, o Event Collection Service (ECS) poderá falhar ao ser inicializado. Se o processo de análise de tráfego não for iniciado, novas fontes de logs não serão descobertas automaticamente.

Resposta do Usuário

Selecione uma das opções a seguir:

- Criar manualmente fontes de logs para os novos dispositivos ou origens de eventos até que o processo de análise de tráfego esteja funcionando.

  Todas as origens de eventos novas são classificadas como SIM Genérico, até que sejam mapeadas para uma fonte de log.
- Se você obtiver um erro de atualização automática, revise o log de atualização automática para determinar se ocorreu um erro quando um DSM ou um protocolo foi instalado.

Armazenamento em Disco Indisponível

`O Vigilante de Disco detectou que uma ou mais partições de armazenamento não são acessíveis.`

Explicação

O sinalizador de disco não recebeu uma resposta em 30 segundos. Um problema de partição de armazenamento pode existir, ou o sistema pode estar sob carga

pesada e não conseguir responder dentro do limite de 30 segundos.

Resposta do Usuário

Selecione uma das opções a seguir:

- Verificar o status da partição `/store` usando o comando **`touch`**.

Se o sistema responder ao comando **`touch`**, a indisponibilidade do armazenamento em disco será provavelmente devido ao carregamento do sistema.

- Determinar se a notificação corresponde aos eventos descartados.

Se os eventos foram descartados e o armazenamento em disco estiver indisponível, as filas de eventos e de fluxos poderão ficar cheias. Investigue o status de partições de armazenamento.

Espaço Insuficiente em Disco para Exportar Dados

`Espaço insuficiente em disco para concluir a solicitação de exportação de dados.`

Explicação

Se o diretório de exportação não contiver espaço suficiente, a exportação de evento, fluxo e dados da ofensa será cancelada.

Resposta do Usuário

Selecione uma das opções a seguir:

- Liberar algum espaço em disco no diretório `/store/exports`.
- Configurar a propriedade **Diretório de Exportação** na janela Configurações do Sistema a ser usada para uma partição que possui espaço suficiente em disco.
- Configurar um dispositivo de armazenamento não integrado.

O Acumulador Descartou os Registros

`Fluxos/Eventos foram descartados pelo Acumulador.`

Explicação

O sistema pode descartar um intervalo de acumulação a partir de um conjunto de dados, se houver muitos dados a serem processados para a visualização de dados agregados. Os intervalos de acumulação descartada também ocorrerão, se o carregamento do sistema impedir que a acumulação seja concluída dentro do limite definido.

O conjunto de dados para o relatório, procura ou gráfico não é exibido. Não há perda de dados porque as acumulações são conjuntos de dados gerados a partir dos dados armazenados.

Resposta do Usuário

Para ajudar a diagnosticar a causa, revise os detalhes a seguir:

- Se a acumulação descartada ocorrer com notificações SAR Sentinel, provavelmente, o problema será devido ao carregamento do sistema.

- Revise os relatórios incluídos recentemente ou as procuras de série temporal para grandes números de valores exclusivos.
- Reduza o escopo dos dados de procura.

Falha da Ferramenta de Varredura

`Uma varredura foi interrompida inesperadamente, em alguns casos, isso pode fazer com que a varredura seja interrompida.`

Explicação

O sistema não pode inicializar uma varredura de vulnerabilidade, e os resultados da varredura de ativo não podem ser importados a partir de scanners externos. Se as ferramentas de varredura pararem inesperadamente, o sistema não poderá se comunicar com um scanner externo. O sistema tenta a conexão com o scanner externo cinco vezes em intervalos de 30 segundos.

Em casos raros, as ferramentas de descoberta encontram um host não testado ou uma configuração de rede.

Resposta do Usuário

Selecione uma das opções a seguir:

- Revisar a configuração para scanners externos no editor de implementação para assegurar que o endereço IP do gateway esteja correto.
- Assegurar que o scanner externo possa se comunicar através do endereço IP configurado.
- Assegurar que as regras de firewall para o DMZ não estejam bloqueando a comunicação entre o dispositivo e os ativos que você deseja varrer.

Falha de Gateway de Varredura Externa

`Um endereço IP do gateway inválido/desconhecido foi fornecido para o scanner hospedado da IBM externo, a varredura foi interrompida.`

Explicação

Quando um scanner externo for incluído, um endereço IP do gateway será necessário. Se o endereço que está configurado para o scanner no editor de implementação estiver incorreto, o scanner não poderá acessar a rede externa.

Resposta do Usuário

Selecione uma das opções a seguir:

- Revisar a configuração para os scanners externos que são configurados no editor de implementação para assegurar que o endereço IP do gateway esteja correto.
- Assegurar que o scanner externo possa se comunicar através do endereço IP configurado.
- Assegurar que as regras de firewall para o DMZ não estejam bloqueando a comunicação entre o dispositivo e os ativos que você deseja varrer.

Falha de Disco

`Falha de Disco: o Monitoramento de Hardware determinou que um disco está no estado com falha.`

Explicação

As ferramentas do sistema integrado detectaram que um disco falhou. A mensagem de notificação fornece informações sobre o disco com falha e o local da falha do slot ou do compartimento.

Resposta do Usuário

Se a notificação persistir, entre em contato com o suporte ao cliente ou substitua as peças.

Falha de Disco Preditiva

`Falha de Disco Preditiva: o Monitoramento de Hardware determinou que um disco está no estado com falha preditivo.`

Explicação

O sistema monitora o status do hardware de hora em hora para determinar quando o suporte de hardware é necessário no dispositivo.

As ferramentas do sistema integrado detectaram que um disco está prestes a falhar ou terminar sua vida útil. O local do slot ou do compartimento da falha foi identificado.

Resposta do Usuário

Planeje a manutenção para o disco que está em um estado com falha preditivo.

Capítulo 4. Notificações de aviso para dispositivos do QRadar

As notificações de funcionamento do sistema do IBM Security QRadar são mensagens proativas de falhas reais ou iminentes de software ou hardware.

Não É Possível Determinar a Fonte de Log Associada

`Não é possível detectar automaticamente a fonte de log associada para o endereço IP <endereço IP>.`

Explicação

No mínimo, 25 eventos são necessários para identificar uma fonte de log. Se a fonte de log não for identificada após 1.000 eventos, o sistema abandonará o processo de descoberta automática.

Quando o processo de análise de tráfego exceder o limite máximo para a descoberta automática, o sistema categorizará a fonte de log como `SIM Genérico` e rotulará os eventos como `Unknown Event Log`.

Ação do usuário

Revise as opções a seguir:

- Revisar o endereço IP para identificar a fonte de log.
- Revisar as fontes de logs que encaminham eventos em uma taxa baixa. As fontes de logs que possuem taxas de eventos baixas, geralmente, causam essa notificação.
- Para analisar corretamente os eventos para o sistema, assegure-se de que a atualização automática faça download dos DSMs mais recentes.
- Revisar as fontes de logs que fornecem eventos através de um servidor de log central. As fontes de logs que são fornecidas a partir de servidores de log centrais ou de consoles de gerenciamento podem requerer que você crie manualmente suas fontes de logs.
- Revise a guia **Atividade de Log** para determinar o tipo de dispositivo a partir do endereço IP na mensagem de notificação e, em seguida, crie manualmente uma fonte de log.
- Verifique se a fonte de log é suportada oficialmente. Se o dispositivo for suportado, crie manualmente uma fonte de log para os eventos.
- Se o dispositivo não for suportado oficialmente, crie um DSM universal para identificar e categorizar os eventos.

Localizado um Processo Não Gerenciado que Está Causando uma Transação Longa

`Sinalizador de Transação: Localizado um processo não gerenciado que causa extraordinariamente uma transação longa que provoca efeitos negativos na estabilidade do sistema.`

Explicação

O sinalizador de transação determina que um processo externo, como um problema de replicação de banco de dados, script de manutenção, atualização automática ou processo da linha de comandos ou uma transação está causando um bloqueio do banco de dados.

Resposta do Usuário

Selecione uma das opções a seguir:

- Revisar o arquivo `/var/log/qradar.log` para a palavra `TxSentry` para determinar o identificador de processo que está causando problemas de transação.
- Aguardar para ver se o processo conclui a transação e libera o bloqueio do banco de dados.
- Liberar manualmente o bloqueio do banco de dados.

Sincronização de Tempo com Falha

`A sincronização de tempo com o primário ou com o console falhou.`

Explicação

O host gerenciado não pode se sincronizar com o console ou o dispositivo de HA secundário não pode se sincronizar com o dispositivo primário.

Os administradores devem permitir a comunicação **`rdate`** na porta 37. Quando a sincronização de tempo estiver incorreta, os dados poderão não ser relatados corretamente para o console. Quanto mais tempo os sistemas ficarem sem sincronização, maior será o risco de que uma procura de dados, relatório ou ofensa possa retornar um resultado incorreto. A sincronização de tempo é crítica para solicitações bem-sucedidas a partir de host gerenciado e dispositivos

Resposta do Usuário

Entre em contato com o suporte ao cliente.

Funcionamento do Sistema Restaurado Cancelando Transações Interrompidas

`Sinalizador de Transação: funcionamento do sistema restaurado cancelando transações interrompidas ou conflitos.`

Explicação

O sinalizador de transação restaurou o sistema para o funcionamento normal do sistema cancelando transações do banco de dados suspensas ou remover bloqueios do banco de dados. Para determinar o processo que causou o erro, revise o arquivo `qradar.log` para a palavra `TxSentry`.

Resposta do Usuário

Nenhuma ação é necessária.

Máximo de Ofensas Ativas Atingidas

`MPC: não é possível criar nova ofensa. O número máximo de ofensas ativas foi atingida.`

Explicação

O sistema não pode criar ofensas ou alterar uma ofensa inativa para uma ofensa ativa. O número padrão de ofensas ativas que podem ser abertos em seu sistema é limitado a 2500. Uma ofensa ativa é qualquer ofensa que continua recebendo contagens de eventos atualizadas nos últimos cinco dias ou menos.

Resposta do Usuário

Selecione uma das opções a seguir:

- Altere ofensas de baixa segurança de abertas (ativas) para encerradas ou protegidas encerradas.
- Ajustar o sistema para reduzir o número de eventos que geram ofensas.

  Para impedir que uma ofensa encerrada seja removida pela política de retenção de dados, proteja a ofensa encerrada.

Total Máximo de Ofensas Atingidos

`MPC: não é possível processar a ofensa. O número máximo de ofensas foi atingido.`

Explicação

Por padrão, o limite de processo é de 2500 ofensas ativas e 100.000 ofensas gerais.

Se uma ofensa ativa não receber uma atualização de evento em 30 minutos, o status da ofensa será alterado para inativo. Se uma atualização do evento ocorrer, uma ofensa inativo poderá ser alterado para ativo. Após cinco dias, as ofensas inativas que não possuem atualizações de evento são alteradas para inativas.

Resposta do Usuário

Selecione uma das opções a seguir:

- Ajustar o sistema para reduzir o número de eventos que geram ofensas.
- Ajustar a política de retenção de ofensa para um intervalo no qual a retenção de dados pode remover Ofensas Inativas.

  Para impedir que uma ofensa encerrada seja removida pela política de retenção de dados, proteja a ofensa encerrada.
- Para liberar espaço em disco para ofensas ativas importantes, altere as ofensas de ativas para inativas.

Relatórios de Execução Longa Interrompidos

`Finalizando um relatório que estava sendo executado por mais tempo do que o limite máximo configurado.`

Explicação

O sistema cancela o relatório que excedeu o limite de tempo. Os relatórios que são executados por mais tempo do que os seguintes limites de tempo padrão são cancelados.

Tabela 1. Limites de Tempo Padrão por Frequência de Relatório

Frequência de relatório	Limites de tempo padrão (horas)
De Hora em Hora	2
Diário	12
Manual	12
Semanal	24
Mensal	24

Usuário Necessário

Selecione uma das opções a seguir:

- Reduzir o período de tempo para o relatório, mas planejar o relatório para ser executado com mais frequência.
- Editar relatórios manuais a serem gerados em um planejamento.

  Um relatório manual pode contar com dados brutos, mas não possui acesso aos dados acumulados. Edite o relatório manual e altere o relatório para usar um planejamento de hora em hora, diário, mensal ou semanal.

Transações Longas para um Processo Gerenciado

`Sinalizador de Transação: Localizado o processo gerenciado que causa extraordinariamente uma transação longa que provoca efeitos negativos na estabilidade do sistema.`

Explicação

O sinalizador de transação determina que um processo gerenciado, como o Tomcat ou o Event Collection Service (ECS) é a causa de um bloqueio do banco de dados.

Um processo gerenciado é forçado a ser reiniciado.

Resposta do Usuário

Para determinar o processo que causou o erro, revise o `qradar.log` para a palavra `TxSentry`.

Configuração Incorreta da Origem de Protocolo

`Uma configuração da origem de protocolo pode estar impedindo que os eventos sejam coletados.`

Explicação

O sistema detectou uma configuração incorreta de protocolo para uma fonte de log. As fontes de logs, que usam protocolos para recuperar os eventos a partir das origens remotas, podem gerar um erro de inicialização quando um problema de configuração no protocolo for detectado.

Resposta do Usuário

Para resolver problemas de configuração de protocolo:

- Revise a fonte de log para assegurar que a configuração de protocolo está correta.

  Verifique os campos de autenticação, caminhos do arquivo, nomes do banco de dados para JDBC, e assegure-se de que o sistema possa se comunicar com servidores remotos. Passe o ponteiro do mouse sobre uma fonte de log para visualizar mais informações de erro.
- Revise o arquivo `/var/log/qradar.log` para obter mais informações sobre o erro de configuração de protocolo.

MPC: Processo não Encerrado de Forma Clara

`MPC: o servidor não foi encerrado de forma clara. As ofensas estão sendo encerrados para serem ressincronizados e assegurarem a estabilidade do sistema.`

Explicação

O processo de funcionário público encontrou um erro. As ofensas ativas são encerrados, os serviços são reiniciados e, se necessário, as tabelas de banco de dados são verificadas e reconstruídas.

O sistema é sincronizado para evitar distorção de dados. Se o componente de funcionário público detectar um estado corrompido, em seguida, as tabelas de banco de dados e os arquivos serão reconstruídos.

Resposta do Usuário

O componente de funcionário público é capaz se reparar por conta própria. Se o erro continuar, entre em contato com o suporte ao cliente.

O Último Backup Excedeu o Limite de Tempo Permitido

`Backup: O último backup planejado excedeu o limite de execução.`

Explicação

O limite de tempo é determinado pela prioridade de backup que você designa durante a configuração.

Resposta do Usuário

Selecione uma das opções a seguir:

- Editar a configuração de backup para aumentar o limite de tempo que é configurado para concluir o backup. Não estenda para mais de 24 horas.
- Editar o backup com falha e alterar o nível de prioridade para uma prioridade mais alta. Os níveis de prioridade mais alta alocam mais recursos do sistema para concluir o backup.

Limite de Licença de Fonte de Log

`O número de Fontes de Logs configuradas está se aproximando ou atingiu o limite licenciado.`

Explicação

Cada dispositivo é vendido com uma licença que coleta eventos a partir de um número específico de fontes de logs. Você se aproximou ou excedeu o limite de licenças.

Mais fontes de logs que foram incluídas são desativadas, por padrão. Os eventos não são coletados para fontes de logs desativadas.

Resposta do Usuário

Revise as opções a seguir:

- Na guia **Admin**, clique no ícone **Fontes de Logs** e desative ou exclua as fontes de logs que são de baixa prioridade ou têm uma fonte de eventos inativa. As fontes de logs desativadas não consideram a licença da fonte de log. No entanto, os dados do evento que são coletados pelas fontes de logs desativadas ainda estão disponíveis e são pesquisáveis.
- Assegure-se de que as fontes de logs excluídas não sejam redescobertas automaticamente. Se a fonte de log for redescoberta, será possível desativá-la. A desativação de uma fonte de log impede a descoberta automática.
- Assegure-se de não exceder seu limite de licença ao incluir fontes de logs em massa.

Fonte de Log Criada em um Estado Desativado

`Uma Fonte de Log foi criada no estado desativado, devido aos limites de licença.`

Explicação

A análise de tráfego é um processo que descobre e cria automaticamente fontes de logs a partir de eventos. Se você estiver no limite de licença da fonte de log atual, o processo de análise de tráfego poderá criar a fonte de log no estado desativado. As fontes de logs desativadas não coletam eventos e não são consideradas no limite de origem de dados.

Resposta do Usuário

Revise as opções a seguir:

- Na guia **Admin**, clique no ícone **Fontes de Logs** e desative ou exclua as fontes de logs de baixa prioridade. As fontes de logs desativadas não consideram a licença da fonte de log.
- Assegure-se de que as fontes de logs excluídas não sejam redescobertas automaticamente. É possível desativar a fonte de log para impedir a descoberta automática.
- Assegure-se de não exceder seu limite de licença ao incluir fontes de logs em massa.
- Se você precisar de uma licença estendida para incluir mais fontes de logs, entre em contato com o representante de vendas.

Limite Ultrapassado do SAR Sentinel

`SAR Sentinel: limite ultrapassado.`

Explicação

O utilitário System Activity Reporter (SAR) detectou que o carregamento do sistema está acima do limite. Seu sistema pode ter o desempenho reduzido.

Resposta do Usuário

Revise as opções a seguir:

- Na maioria dos casos, nenhuma resolução será necessária.

  Por exemplo, quando o uso de CPU estiver acima de 90%, o sistema tentará retornar automaticamente à operação normal.
- Se essa notificação for recorrente, aumente o valor padrão do SAR Sentinel.

  Clique na guia **Admin** e, em seguida, clique em **Notificações do Sistema Global**. Aumente o limite de notificação.
- Para notificações de carregamento do sistema, reduza o número de processos que são executados simultaneamente.

  Escalone o horário de início para relatórios, varreduras de vulnerabilidade ou importações de dados para as fontes de logs. Planeje backups e processos do sistema para serem iniciados em horários diferentes para reduzir o carregamento do sistema.

O Usuário não Existe ou É Indefinido

`O usuário não existe ou tem uma função indefinida.`

Explicação

O sistema tentou atualizar uma conta do usuário com mais permissões, mas a conta do usuário ou função de usuário não existe.

Resposta do Usuário

Na guia **Admin**, clique em **Implementar Mudanças**. As atualizações nas contas ou funções do usuário requerem que você implemente a mudança.

Aviso sobre o Uso de Disco

`Sinalizador de Disco: O Uso de disco excedeu o limite de aviso.`

Explicação

O sinalizador de disco detectou que o uso de disco no sistema é maior que 90%.

Quando o espaço em disco no sistema atingir 90%, o sistema começará a desativar os processos para impedir a distorção de dados.

Resposta do Usuário

Você deve liberar algum espaço em disco excluindo arquivos ou alterando as políticas de retenção de dados. O sistema pode reiniciar processos

automaticamente, após o uso de espaço em disco ficar abaixo de um limite de 92% de capacidade.

Eventos Roteados Diretamente para Armazenamento

`Foi detectada a degradação de desempenho no pipeline do evento. 0(s) evento(s) foi(foram) roteado(s) diretamente para o armazenamento.`

Explicação

Para evitar que as filas sejam preenchidas, e para evitar que o sistema descarte os eventos, o Event Collection System (ECS) roteará os dados para o armazenamento. Os eventos e os fluxos recebidos não são categorizados. No entanto, os dados de evento e de fluxo brutos são coletados e são pesquisáveis.

Resposta do Usuário

Revise as opções a seguir:

- Verifique as taxas de evento e de fluxo recebidos. Se o pipeline do evento estiver enfileirando eventos, expanda sua licença para reter mais dados.
- Revise as mudanças recentes nas regras ou nas propriedades customizadas. As mudanças na regra ou na propriedade customizada podem causar mudanças repentinas nas taxas de evento ou de fluxo. As mudanças podem afetar o desempenho ou fazer com que o sistema roteie eventos para armazenamento.
- Problemas de análise de DSM podem fazer com que os dados do evento sejam roteados para armazenamento. Verifique se a fonte de log é suportada oficialmente.
- As notificações de SAR podem indicar que os eventos e fluxos enfileirados estão no pipeline do evento.
- Ajuste o sistema para reduzir o volume de eventos e de fluxos que inserem o pipeline do evento.

Propriedade Customizada Desativada

`Uma propriedade customizada foi desativada.`

Explicação

Uma propriedade customizada foi desativada devido a problemas ao processá-la. Regras, relatórios ou procuras que usam a propriedade customizada desativada param de funcionar corretamente.

Resposta do Usuário

Selecione uma das opções a seguir:

- Revisar a propriedade customizada desativada para corrigir os padrões regex. Não reative as propriedades customizadas desativadas sem revisar e otimizar primeiro o padrão regex ou o cálculo.
- Se a propriedade customizada for usada para regras customizadas ou relatórios, assegure-se de que a caixa de seleção **Otimizar análise para regras, relatórios e procuras** esteja selecionada.

Falha de Backup de Dispositivo

`Ocorreu uma falha ao tentar fazer backup de um dispositivo ou o backup foi cancelado.`

Explicação

Normalmente, o erro é causado por erros de configuração no Configuration Source Management (CSM) ou se um backup for cancelado por um usuário.

Resposta do Usuário

Selecione uma das opções a seguir:

- Revisar as credenciais e os conjuntos de endereços no CSM para assegurar que o dispositivo possa efetuar login.
- Verificar se o protocolo configurado para se conectar ao dispositivo de rede é válido.
- Assegurar que o dispositivo de rede e a versão sejam suportados.
- Verificar se há conectividade entre o dispositivo de rede e o dispositivo.
- Verificar se os adaptadores mais atuais estão instalados.

Dados de Evento ou de Fluxo Não Indexados

`Dados do Evento/Fluxo não indexados para o intervalo.`

Explicação

Se muitos índices forem ativados ou o sistema estiver sobrecarregado, o sistema poderá eliminar o evento ou fluxo a partir da parte do índice.

Resposta do Usuário

Selecione uma das opções a seguir:

- Se o intervalo de índice descartado ocorrer com notificações do SAR Sentinel, provavelmente, o problema será devido ao carregamento do sistema ou ao espaço insuficiente em disco.
- Para desativar temporariamente alguns índices para reduzir o carregamento do sistema, na guia **Admin**, clique no ícone **Gerenciamento de Índice**.

Limite Atingido para Ações de Resposta

`Ação de Resposta: limite atingido.`

Explicação

O Custom Rules Engine (CRE) não pode responder a uma regra porque o limite de resposta está cheio.

As regras genéricas ou um sistema ajustado pode gerar muitas ações de resposta, especialmente os sistemas com a opção **IF-MAP** ativada. As ações de resposta são enfileiradas. As ações de resposta poderão ser descartadas se a fila exceder 2000 no Event Collection System (ECS) ou 1000 ações de resposta no Tomcat.

Resposta do Usuário

- Se a opção **IF-MAP** for ativada, verifique se a conexão com o servidor **IF-MAP** existe e se um problema de largura da banda não está fazendo com que a resposta da regra seja enfileirada no Tomcat.
- Ajuste o sistema para reduzir o número de regras que está sendo acionado.

Atraso da Replicação de Disco

`DRBD Sentinel: a replicação de disco está atrasando. Consulte o log para obter detalhes.`

Explicação

Se a fila de replicação for preenchida no dispositivo primário, o carregamento do sistema no primário poderá ser aumentado. Normalmente, os problemas de replicação são causados por problemas de desempenho no sistema primário, ou problemas de armazenamento no sistema secundário, ou problemas de largura da banda entre os dispositivos.

Resposta do Usuário

Selecione uma das opções a seguir:

- Revisar a atividade da largura da banda carregando uma procura salva **MGMT: Gerenciador de Largura da Banda** na guia **Atividade de Log**. Essa procura exibe o uso de largura da banda entre o console e os hosts.
- Se as notificações do sentinela SAR forem recorrentes no dispositivo primário, as filas do Distributed Replicated Block Device deverão estar completas no sistema primário.
- Use SSH e o comando `cat /proc/drbd` para monitorar o status do Distributed Replicated Block Device dos hosts primários e secundários.

Regra Customizada Cara Localizada

`Regras Customizadas Caras Localizadas no CRE: foi detectada a degradação de desempenho no pipeline do evento. Regras customizadas caras localizadas no CRE.`

Explicação

O Custom Rules Engine (CRE) é um processo que é validado, se um evento corresponder a um conjunto de regras e, em seguida, acionar alertas, ofensas ou notificações.

Quando um usuário criar uma regra customizada que possui um escopo grande ou usar um padrão regex que não está otimizado, a regra customizada poderá afetar o desempenho.

Resposta do Usuário

Revise as opções a seguir:

- Na guia **Ofensas**, clique em **Regras** e use a janela de procura para localizar e editar ou desativar a regra cara.
- Se as notificações do SAR Sentinel forem recorrentes com a notificação de regra cara, investigue a regra.

A Acumulação Está Desativada para o Mecanismo de Detecção de Anomalias

`Acumulação desativada para o Mecanismo de Detecção de Anomalias.`

Explicação

A visualização de dados agregados está desativada ou indisponível, ou uma nova regra requer dados que estão indisponíveis.

Uma acumulação descartada não indica perda de dados de anomalias. Os dados de anomalias originais são mantidos, porque as acumulações são conjuntos de dados gerados a partir de dados armazenados. A notificação fornece mais detalhes sobre o intervalo de acumulação descartada.

O mecanismo de detecção de anomalias não pode revisar esse intervalo dos dados de anomalias para a acumulação.

Resposta do Usuário

Atualize as regras de anomalias para usar um conjunto de dados menor.

Se a notificação for um erro recorrente de SAR Sentinel, o desempenho do sistema poderá ser a causa do problema.

O Processo Excede o Tempo de Execução Permitido

`O processo leva muito tempo para ser executado. O tempo padrão máximo é 3600 segundos.`

Explicação

O limite de tempo padrão de uma hora para que um processo individual conclua uma tarefa foi excedido.

Resposta do Usuário

Revise o processo em execução para determinar se a tarefa é um processo que pode continuar a ser executado ou deve ser interrompido.

Disco Cheio de Fila de Persistências de Ativo

`Disco Cheio de Fila de Persistências de Ativo.`

Explicação

O sistema detectou que o espaço em disco excedente, que é designado à fila de persistências do ativo, está cheio. As atualizações de persistência do ativo estarão bloqueadas até que o espaço em disco esteja disponível. As informações não são descartadas.

Resposta do Usuário

Reduza o tamanho da varredura. Uma redução no tamanho da varredura pode evitar que as filas de persistências do ativo sejam excedidas.

Disco Cheio da Fila do Resolvedor de Atualização de Ativo

`Disco Cheio da Fila do Resolvedor de Atualização de Ativo.`

Explicação

O sistema detectou que o espaço em disco excedente, que é designado à fila do resolvedor de ativo, está cheio.

O sistema grava continuamente os dados no disco para evitar qualquer perda de dados. No entanto, se o sistema não tiver espaço em disco, ele descartará os dados de varredura. O sistema não pode manipular dados de varredura de ativos recebidos até que o espaço em disco esteja disponível.

Resposta do Usuário

Revise as opções a seguir:

- Assegure-se de que o sistema tenha espaço livre em disco. A notificação pode acompanhar as notificações do SAR Sentinel para notificá-lo de problemas potenciais de espaço em disco.
- Reduzir o tamanho das varreduras.
- Diminuir a frequência da varredura.

Disco Cheio para a Fila de Mudança de Ativo

`Disco Cheio da Fila do Listener de Mudança de Ativo.`

Explicação

O gerenciador de perfil do ativo inclui um processo, um listener de mudança, que calcula estatísticas para atualizar a pontuação de CVSS de um ativo. O sistema grava os dados no disco, o que evita perda de dados de estatísticas de ativos pendentes. No entanto, se o espaço em disco estiver cheio, o sistema descartará os dados de varredura.

O sistema não pode processar dados de varredura de ativo recebido até que o espaço em disco esteja disponível.

Resposta do Usuário

Selecione uma das opções a seguir:

- Assegurar que o sistema tenha espaço livre suficiente em disco.
- Reduzir o tamanho das varreduras.
- Diminuir a frequência da varredura.

Mudança no Ativo Descartada

`Mudanças no Ativo Interrompidas.`

Explicação

Uma mudança no ativo excedeu o limite de mudança e o gerenciador de perfil do ativo ignorou a solicitação de mudança no ativo.

O gerenciador de perfil do ativo inclui um processo, persistência do ativo, que atualiza as informações de perfil para ativos. O processo coleta dados do ativo novo e, em seguida, enfileira as informações antes que o modelo de ativo seja atualizado. Quando um usuário tentar incluir ou editar um ativo, os dados serão armazenados no armazenamento temporário e incluídos no final da fila de mudanças. Se a fila de mudanças for grande, a mudança no ativo poderá atingir o tempo limite e o armazenamento temporário será excluído.

Resposta do Usuário

Selecione uma das opções a seguir:

- Incluir ou editar o ativo uma segunda vez.
- Ajustar ou escalonar o horário de início para varreduras de vulnerabilidades ou reduzir o tamanho das varreduras.

Cadeia Detectada de Dependência de Regra Customizada Cíclica

`Localizada cadeia de dependência cíclica de regras customizadas.`

Explicação

Uma regra única referida a si mesma diretamente ou a si mesma através de uma série de outras regras ou de blocos de construção. O erro ocorre ao implementar uma configuração integral. O conjunto de regras não é carregado.

Resposta do Usuário

Edite as regras que criaram a dependência cíclica. A cadeia de regras deve ser quebrada para evitar uma notificação do sistema recorrente. Após a cadeia de regras ser corrigida, um salvamento recarrega automaticamente as regras e resolve o problema.

Máximo de Dispositivos de Sensor Monitorados

`A análise de tráfego já está monitorando o número máximo de fontes de logs.`

Explicação

O sistema contém um limite para o número de fontes de logs que podem ser enfileiradas para a descoberta automática por análise de tráfego. Se o número máximo de fontes de logs na fila for atingido, novas fontes de logs não poderão ser incluídas.

Os eventos para a fonte de log são categorizados como `SIM Genérico` e rotulados como `Log de Evento Desconhecido`.

Resposta do Usuário

Selecione uma das opções a seguir:

- Revisar as fontes de logs do SIM Genérico na guia **Atividade de Log** para determinar o tipo de dispositivo a partir da carga útil do evento.
- Assegurar que as atualizações automáticas possam fazer download das atualizações mais recentes de DSM para identificar e analisar corretamente os eventos de fontes de logs.
- Verifique se a fonte de log é suportada oficialmente.

Se o dispositivo for suportado, crie manualmente uma fonte de log para os eventos que não foram descobertos automaticamente.

- Se o dispositivo não for suportado oficialmente, crie um DSM universal para identificar e categorizar os eventos.
- Aguardar até que o dispositivo forneça 1.000 eventos.

  Se o sistema não puder descobrir automaticamente a fonte de log após 1.000 eventos, ele será removido da fila de análise de tráfego. O espaço se torna disponível para que outra fonte de log seja descoberta automaticamente.

O Coletor de Fluxo Não Pode Estabelecer Sincronização de Tempo Inicial

`O coletor de fluxo não pôde estabelecer sincronização de tempo inicial.`

Explicação

O processo QFlow contém uma função avançada para configurar um endereço IP do servidor para sincronização de tempo. Na maioria dos casos, não configure um valor. Se for configurado, o processo QFlow tentará sincronizar o tempo a cada hora com o servidor de horário de endereço IP.

Resposta do Usuário

No editor de implementação, selecione o processo QFlow. Clique em **Ações** > **Configurar** e clique em **Avançado**. No campo **Endereço IP do Servidor de Sincronização de Tempo**, limpe o valor e clique em **Salvar**.

Licença expirada

`Uma licença alocada expirou e não é mais válida.`

Explicação

Quando uma licença expirar no console, uma nova licença deverá ser aplicada. Quando uma licença expirar em um host gerenciado, o contexto do host será desativado no host gerenciado. Quando o contexto do host estiver desativado, o dispositivo com a licença expirada não poderá processar dados de evento ou de fluxo.

Resposta do Usuário

Para determinar o dispositivo com a licença expirada, clique na guia **Admin**, clique em **Gerenciamento de Sistema e de Licença**. Um sistema que possui uma licença expirada exibe um status inválido na coluna **Status da Licença**.

Máximo de Eventos Atingido

`O limite de eventos por intervalo foi excedido na última hora.`

Explicação

Cada dispositivo possui uma licença que processa um volume específico de dados de evento e de fluxo.

Se o limite de licença continuar a ser excedido, o sistema poderá enfileirar eventos e fluxos ou, possivelmente, descartar os dados quando a fila de backups for preenchida.

Resposta do Usuário

Ajuste o sistema para reduzir o volume de eventos e de fluxos que inserem o pipeline do evento.

Licença do Monitor de Processo Expirada ou Inválida

`Monitor de Processo: Não é possível iniciar o processo: licença expirada ou inválida.`

Explicação

A licença foi expirada para um host gerenciado. Todos os processos de coleta de dados param no dispositivo.

Resposta do Usuário

Entre em contato com seu representante de vendas para renovar a licença.

Erro de Falta de Memória e Aplicativo Incorreto Reiniciado

`Falta de Memória: sistema restaurado, o aplicativo incorreto foi reiniciado.`

Explicação

Um aplicativo ou serviço foi executado sem memória e foi reiniciado. Problemas de falta de memória são causados normalmente por problemas de software ou por consultas definidas pelo usuário.

Resposta do Usuário

Revise o arquivo `/var/log/qradar.log` para determinar se um reinício de serviço é necessário.

Determine se grandes varreduras vulnerabilidades ou a importação de grandes volumes de dados é responsável pelo erro. Por exemplo, compare quando o sistema importa dados de evento ou de vulnerabilidade em seu sistema com o registro de data e hora da notificação. Se necessário, escalone os intervalos de tempo para as importações de dados.

Implementação de uma Atualização Automática

`Atualizações automáticas instaladas com êxito. Na guia Administração, clique em Implementar Mudanças.`

Explicação

Uma atualização automática, como uma atualização de RPM, foi transferida por download e requer que a mudança seja implementada para concluir o processo de instalação.

Resposta do Usuário

Na guia **Admin**, clique em **Implementar Mudanças**.

Licença expirada

`Uma licença alocada expirou e não é mais válida.`

Explicação

Quando uma licença expirar no console, uma nova licença deverá ser aplicada. Quando uma licença expirar em um host gerenciado, o contexto do host será desativado no host gerenciado. Quando o contexto do host estiver desativado, o dispositivo com a licença expirada não poderá processar dados de evento ou de fluxo.

Resposta do Usuário

Para determinar o dispositivo com a licença expirada, clique na guia **Admin**, clique em **Gerenciamento de Sistema e de Licença**. Um sistema que possui uma licença expirada exibe um status inválido na coluna **Status da Licença**.

Varredura Externa de um Endereço IP ou Intervalo Desautorizado

`Uma execução de varredura externa tentou varrer um endereço IP ou intervalo de endereço desautorizado.`

Explicação

Quando um perfil de varredura incluir um intervalo do CIDR ou endereço IP fora da lista de ativos definida, a varredura continuará. No entanto, os intervalos do CIDR ou endereços IP para ativos que não estão dentro da lista de scanners externos são ignorados.

Resposta do Usuário

Atualize a lista de intervalos do CIDR autorizados ou o endereço IP para ativos que são varridos pelo scanner externo. Revise os perfis de varredura para assegurar que a varredura esteja configurada para ativos que são incluídos na lista de redes externas.

O Componente de Infraestrutura Está Corrompido ou Não Foi Iniciado

`Componente de infraestrutura corrompido.`

Explicação

Quando não for possível iniciar ou reconstruir o serviço de mensagem (IMQ) ou o banco de dados PostgreSQL, o host gerenciado não poderá operar corretamente ou se comunicar com o console.

Resposta do Usuário

Entre em contato com o suporte ao cliente.

Capítulo 5. Notificações de informação para dispositivos do QRadar

O IBM Security QRadar fornece mensagens de informação sobre o status ou resultado de um processo ou ação

Armazenamento em Disco Disponível

`Uma ou mais partições que estavam inacessíveis anteriormente estão agora acessíveis.`

Explicação

O sinalizador de disco detectou que a partição de armazenamento está disponível.

Resposta do Usuário

Nenhuma ação é necessária.

Atualizações Automáticas Transferidas por Download com Êxito

`Atualizações automáticas transferidas por download com êxito. Consulte o log Atualizações Automáticas para obter detalhes.`

Explicação

As atualizações de software foram transferidas por download automaticamente.

Resposta do Usuário

Clique no link na notificação para determinar se as atualizações transferidas por download requerem instalação.

Atualização Automática Bem-Sucedida

`Atualizações automáticas concluídas com êxito.`

Explicação

As atualizações de software automáticas foram transferidas por download e instaladas com êxito.

Resposta do Usuário

Nenhuma ação é necessária.

Restauração da Operação de SAR Sentinel

`SAR Sentinel: operação normal restaurada.`

Explicação

O utilitário System Activity Reporter (SAR) detectou que o carregamento do sistema foi retornado para níveis aceitáveis.

Resposta do Usuário

Nenhuma ação é necessária.

Uso de Disco Retornado para o Normal

`Sinalizador de Disco: O Uso de Disco do Sistema Voltou para Níveis Normais.`

Explicação

O sinalizador de disco detectou que o uso de disco está abaixo de 90% da capacidade geral.

Resposta do Usuário

Nenhuma ação é necessária.

Um Componente de Infraestrutura Foi Reparado

`Componente de infraestrutura corrompido reparado.`

Explicação

Um componente corrompido, que é responsável por serviços de host em um host gerenciado, foi reparado.

Resposta do Usuário

Nenhuma ação é necessária.

Licença Próxima da Expiração

`Uma licença está próxima da expiração. É necessário substituí-la em breve.`

Explicação

O sistema detectou que uma licença para um dispositivo está dentro do prazo de 35 dias da expiração.

Resposta do Usuário

Nenhuma ação é necessária.

Limite de Período de Carência de Alocação de Licença

`Um período de carência de licença alocada está quase terminado e será alocado para o local brevemente.`

Explicação

O sistema detectou que uma mudança de licença para um dispositivo está dentro do período de carência de licença.

Um administrador pode mover licenças desbloqueadas ou aplicar evento não utilizado ou licenças de fluxo a outros dispositivos na implementação. Ao alocar uma licença para um host, um período de carência de 14 dias para a licença é iniciado. Após a expiração do período de carência, a licença não poderá ser movida.

Resposta do Usuário

Nenhuma ação é necessária.

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre os produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento deste documento não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licenças devem ser enviados, por escrito, para:

Gerência de Relações Industriais e Comerciais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições estejam inconsistentes com a lei local:

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

Estas informações podem incluir imprecisões técnicas ou erros tipográficos. Periodicamente, são feitas alterações nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-14
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença de Programa Internacional IBM ou de qualquer outro contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais poderão variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais poderão variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não-IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não-IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a mudança ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Todos os preços IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso prévio. Os preços dos revendedores podem variar.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

Se você estiver visualizando essas informações em cópia eletrônica, as fotografias e as ilustrações coloridas poderão não aparecer.

Marcas Comerciais

IBM, o logotipo IBM e ibm.com são marcas ou marcas comerciais da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca registrada da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca registrada (® ou ™), estes símbolos indicarão marcas registradas dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações forem publicadas. Estas marcas comerciais também podem ser marcas registradas ou marcas comerciais de direito consuetudinário em outros países. Uma lista atual de marcas registradas da IBM está disponível na web em Informações de copyright e de marca registrada (www.ibm.com/legal/copytrade.shtml).

Considerações de Política de Privacidade

Os produtos de Software IBM, incluindo soluções de software como serviço, ("Ofertas de Software") podem usar cookies ou outras tecnologias para coletar informações de uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar interações com o usuário final ou para outros propósitos. Em muitos casos nenhuma informação identificável pessoalmente é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem permitir que você colete as informações pessoais identificáveis. Se esta Oferta de Software usar cookies para coletar informações pessoais identificáveis, informações específicas sobre o uso de cookies dessa oferta serão apresentadas a seguir.

Dependendo das configurações implementadas, essa Oferta de Software pode usar cookies de sessão que coletam o ID de sessão de cada usuário para propósitos de autenticação e gerenciamento de sessões. Estes cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade que eles ativam.

Se as configurações implementadas para esta Oferta de Software permitirem que você, como cliente, colete informações de identificação pessoal de usuários finais por meio de cookies e outras tecnologias, você deverá consultar seu conselho jurídico sobre as leis aplicáveis a essa coleta de dados, incluindo requisitos para aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para tais propósitos, consulte a Política de Privacidade da IBM em http://www.ibm.com/privacy e a Declaração de Privacidade On-line da IBM em http://www.ibm.com/privacy/details, a seção intitulada "Cookies, Web Beacons and Other Technologies" e "IBM Software Products and Software-as-a-Service Privacy Statement" em http://www.ibm.com/software/info/product-privacy.

Índice Remissivo

R

S

V