AMP para endpoints: Exclusões de processos em MacOS e Linux

Contents

Introduction

Começando com o Connector versão 1.11.0, a AMP para Endpoints está adicionando suporte para exclusões de processos em macOS e Linux. Antigamente, a configuração da AMP para ignorar atividades de um aplicativo macOS ou Linux exigia uma combinação de regras de caminho, extensão de arquivo e/ou exclusão curinga. Como essas regras têm como alvo arquivos e diretórios e não podem ser associadas a um programa ou processo, várias regras eram frequentemente necessárias para cada programa e cada regra pode excluir desnecessariamente atividades de mais de um programa. As exclusões de processos fornecem uma maneira mais direta e precisa de excluir as atividades de um aplicativo. Quando usadas adequadamente, as exclusões de processos podem melhorar significativamente o desempenho da AMP com efeitos adversos mínimos na segurança do sistema.

As regras de exclusão de processos são gerenciadas no console da Web da AMP para endpoints. Cada regra consiste em:

- O caminho completo (absoluto) para o executável do programa,
- O nome de usuário do processo (opcional) e
- Se os processos filho também devem ser excluídos (padrão: não)

Quando uma regra de Exclusão de Processo corresponde a um processo em execução, todas as atividades executadas por esse processo e, opcionalmente, seus processos filho são excluídos da verificação.

Começando com o Connector versão 1.15.2, o caminho de exclusão do processo aceitará curingas ('*'). Um curinga corresponderá a qualquer conjunto de caracteres em um nível de arquivo ou diretório.

> **IMPORTANTE!**
>
> Com a adição da exclusão de processos nos conectores Mac e Linux 1.11.0, a interpretação das regras existentes de caminho, extensão de arquivo e curinga também está mudando. Não há alteração no comportamento dos conectores 1.10.x e anteriores. No entanto, as mesmas regras em 1.11.0 não serão aplicadas de forma tão geral. Consulte *Alterações* da

seção *em Caminho, Extensão de Arquivo e Regras de Exclusão de Curingas* para obter detalhes.

Preparando para exclusões de processos

Há três considerações importantes antes de atualizar seus endpoints macOS e Linux:

1. 1.10.x e conectores mais antigos ignoram as regras de exclusão de processos.
2. 1.11.0 e conectores mais recentes honram as regras de exclusão de processos, mas interpretam as regras de caminho, extensão de arquivo e curinga de forma diferente dos conectores mais antigos. Isso pode afetar adversamente o desempenho do sistema.
3. O Mac Connector 1.10.0 e o Linux Connector 1.11.0 introduziram otimizações genéricas de varredura na execução que reduzem a perda de desempenho da nova interpretação descrita em (2).

Alterações nas regras de caminho, extensão de arquivo e exclusão de curinga

Em versões 1.10.x e mais antigas do Connector: As regras de arquivo, caminho e curinga excluem o arquivo ou diretório de destino da verificação dessas operações de arquivo:

- Criar
- Modificar
- Renomear
- Executar

Em versões 1.11.0 e mais recentes do conector: A interpretação das regras de Caminho, Extensão de Arquivo e Curinga foi alterada de modo que, em uma correspondência, a execução do arquivo acionará uma verificação em vez de ser excluída. A criação, modificação e renomeação do arquivo continuam a ser excluídas. As motivações para essa mudança são:

1. Evita a exclusão indesejada da atividade de execução ao excluir diretórios de arquivos de dados.
2. Ele complementa melhor as regras de Exclusão de Processos, possibilitando a exclusão independente de operações de execução e não execução no mesmo caminho.
3. Ele alinha a interpretação macOS e Linux dessas regras com a AMP no Windows.

Na maioria dos casos, estima-se que o aumento do uso da CPU da AMP seja inferior a 20%. Em alguns casos, o uso da CPU da AMP pode diminuir. Isso é possível se as otimizações genéricas de varredura ao executar da nova versão do Connector forem mais eficazes do que as regras de exclusão em uso.

Orientação para atualização do conector

Para sistemas previamente ajustados usando exclusões, é necessário prestar atenção após atualizar para 1.11.0 (ou mais recente) para garantir que o desempenho do sistema ainda seja satisfatório. As etapas de atualização recomendadas são:

1. Sem fazer nenhuma alteração de exclusão, atualize o conector.
2. Avalie o desempenho do sistema após a atualização.

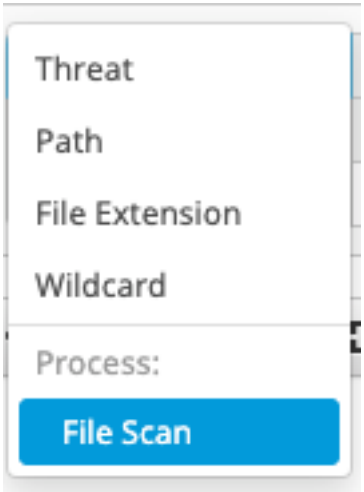
3. Se o desempenho do sistema após a atualização for satisfatório, remova as regras de caminho, extensão de arquivo e exclusão de curinga que direcionam os executáveis do programa em vez dos arquivos de dados. Essas regras já não são necessárias. Novas regras de exclusão de processos podem ser adicionadas para melhorar ainda mais o desempenho quando for conveniente.
4. Se o desempenho do sistema após a atualização não for satisfatório, substitua as regras de caminho, extensão de arquivo e exclusão de curinga que direcionam executáveis do programa pelas regras de exclusão de processo correspondentes. O desempenho do sistema deve melhorar para um nível igual ou melhor do que antes da atualização.

Em implantações maiores em que os conectores são atualizados em fases, recomenda-se adiar a modificação ou a remoção de regras de caminho, extensão de arquivo e exclusão de curinga até que todos os conectores tenham sido atualizados para 1.11.0 ou mais recente. Isso garante que os conectores mais antigos, que dependem das regras de exclusão existentes, não sejam afetados adversamente antes que o endpoint seja atualizado.

Adicionando regras de exclusão de processo

As regras de exclusão de processos podem ser criadas usando o portal da Web AMP para endpoints. O procedimento é:

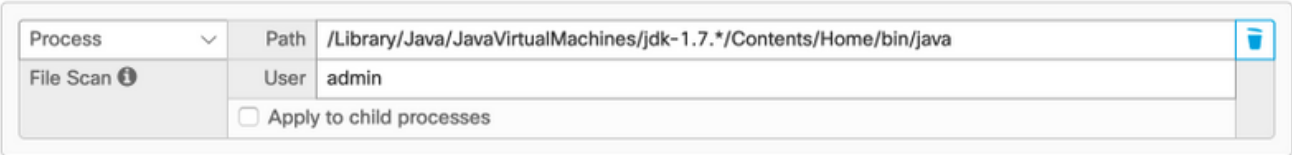
1. Localize o conjunto de exclusões que deseja modificar. Clique em `Adicionar exclusão` e selecione `Processo: File Scan (Verificação de arquivo).



2. Insira o caminho absoluto para o programa ser excluído, a conta de usuário que executará o programa (opcional) e se a exclusão deve ser aplicada a todos os processos filho criados pelo programa.

Começando com o Connector versão 1.15.2, os curingas (*) podem ser usados no caminho para representar qualquer número de caracteres em um único diretório. É recomendável usar o curinga para cobrir o número mínimo de caracteres necessários para fornecer a exclusão necessária. O curinga também pode ser usado juntamente com caracteres em um diretório para restringir ainda mais a

exclusão.



3. Clique em `Adicionar exclusão` para adicionar mais regras (repetindo etapas de 1 a 2) ou clique em `Salvar` para salvar o conjunto de exclusões.

Práticas recomendadas de exclusões de processos

- **Nunca exclua o processo de inicialização:** o processo de inicialização (ou seja, `iniciado' em macOS, `init` ou `systemd` no Linux) é responsável pela criação de todos os outros processos no sistema e está no topo da hierarquia de processos. A exclusão do processo de inicialização e de todos os processos filhos desativaria efetivamente o monitoramento da AMP.
- **Especificar usuário quando possível:** se o campo Usuário for deixado em branco, a exclusão será aplicada a qualquer processo que execute o programa especificado. Embora uma regra que se aplique a qualquer usuário possa ser mais flexível, esse escopo amplo pode excluir involuntariamente atividades que devem ser monitoradas. A especificação do usuário é especialmente importante para regras que se aplicam a programas compartilhados, como motores de tempo de execução (por exemplo, `java') e intérpretes de script (por exemplo, `bash', `python'). Especificar o escopo de limites do usuário e direcionar a AMP para ignorar instâncias específicas ao monitorar outras instâncias.
- **Evite sobreposição entre regras de exclusão de processo e extensão de caminho/arquivo/curinga:** ao excluir a execução de um programa da verificação, uma boa salvaguarda a ser mantida é detectar modificações desse programa confiável e acionar verificações de arquivos. Garantir que o caminho especificado em uma regra de Exclusão de Processo não é coberto por uma regra de Caminho/Extensão de Arquivo/Curinga garante que a modificação do arquivo não seja excluída intencionalmente da verificação.
- **Minimizar o número de regras:** Embora os conectores Mac e Linux não imponham um número máximo de limites de regras de exclusão de processos, mais regras podem incorrer em sobrecarga adicional de avaliação. Escolha o processo pai de nível mais alto que identifica exclusivamente o aplicativo a ser excluído e use a opção Aplicar ao processo filho para minimizar o número de regras.

Diferenças da implementação do Windows

A adição do suporte à exclusão de processos e a redução do escopo de regras de caminho, extensão de arquivo e curinga aproximam as exclusões de macOS e Linux do Windows. No entanto, ainda há diferenças importantes na implementação:

1. as regras de exclusão de processos macOS e Linux aceitam um nome de usuário opcional para acompanhar o caminho completo executável do processo, enquanto o Windows aceita um valor de hash SHA-256 opcional. A exclusão de um processo pelo valor de hash SHA-

256 não é suportada atualmente em macOS e Linux.
2. Os mecanismos de atividade mal-intencionada e processo do sistema são exclusivos do Windows e, portanto, esses tipos de exclusão não estão disponíveis no macOS e no Linux.