Configurar logs de depuração de solicitação no Secure Web Appliance

Contents

Introdução

Este documento descreve as etapas para solicitar logs de depuração no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Acesso administrativo à Interface de Linha de Comando (CLI) do SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Solicitar Logs de Depuração

Os logs de depuração de solicitação no SWA são um tipo de log especializado projetado para capturar informações extremamente detalhadas, de depuração completa e de nível de rastreamento para uma única transação HTTP ou HTTPS específica ou uma máquina cliente. Diferentemente dos logs de proxy padrão que registram eventos resumidos em várias solicitações, os logs de depuração de solicitação agregam a saída de depuração de todos os módulos de proxy da Web envolvidos no processamento de uma determinada solicitação (como autenticação, filtragem de URL, descriptografia, verificação de malware e serviços de reputação) em um fluxo de log correlacionado. Esse tipo de log é destinado exclusivamente a diagnósticos detalhados e só pode ser criado via CLI, não por meio da GUI

Os logs de depuração de solicitação são essenciais ao solucionar problemas de proxy complexos ou intermitentes em que os logs padrão não têm detalhes suficientes. Eles permitem que os administradores e o Cisco TAC rastreiem exatamente como uma única solicitação foi tratada em cada estágio de processamento, tornando possível identificar as causas básicas, como correspondências inesperadas de políticas, atrasos de verificação, falhas de autenticação ou veredictos inconsistentes entre os mecanismos. Como o registro se concentra em uma transação, ele fornece visibilidade máxima sem a sobrecarga operacional e o impacto no desempenho da ativação do registro de depuração em todos os módulos proxy do sistema. Isso torna os logs de depuração de solicitação uma ferramenta de diagnóstico precisa, eficiente e de baixo risco durante investigações avançadas.

Configurando os logs de depuração de solicitação

Etapa 1. Efetue login na CLI, execute logconfig e escolha new.

Etapa 2. Selecione o número associado aos logs de depuração de solicitação e pressione Enter.

Etapa 3. Digite o nome do log.

Etapa 4. Escolha Trace como o nível de log.

Etapa 5. Escolha os módulos onde for solicitado para coletar o log avançado. Várias seleções podem ser feitas na forma de uma lista separada por vírgulas ou de intervalos (como 1,3,4 ou 3-7).

Tip: Se nenhum módulo específico for solicitado pelo TAC, é melhor selecionar todos os módulos (como 1-30).

Etapa 6. Especificar o número de solicitações para as quais o log avançado deve ser ativado. Quando esse número de solicitações for capturado, o registro será automaticamente interrompido.

Note: É importante selecionar um valor razoável com base nas condições de tráfego durante a solução de problemas. Por exemplo, se uma máquina de teste dedicada estiver sendo usada e o tráfego em segundo plano for mínimo, um número menor de solicitações será suficiente. No entanto, em ambientes com maior atividade em segundo plano (como atualizações do sistema operacional, solicitações em segundo plano do navegador ou aplicativos como o Webex), a escolha de um valor mais alto garante que a transação relevante seja capturada.

Etapa 7. Defina os critérios de correspondência de solicitação para o registro em log avançado selecionando o endereço IP do cliente, o endereço IP de destino ou o domínio de destino.

Note: Na maioria dos casos, é recomendável selecionar o endereço IP do cliente, mesmo durante a solução de problemas de acesso a um único site. Essa abordagem garante que todas as solicitações da Web geradas durante o carregamento da página sejam capturadas, incluindo solicitações em segundo plano para URLs adicionais que possivelmente não estejam visíveis imediatamente. No entanto, esse método é mais eficiente ao usar uma máquina de teste dedicada com tráfego de Internet em segundo plano mínimo. Em ambientes onde o cliente gera tráfego adicional significativo (como atualizações do sistema operacional, serviços de segundo plano do navegador ou aplicativos como Webex), é melhor filtrar por domínio de destino ou endereço IP de destino.

Tip: Se o ponto exato da falha for desconhecido, os registros HAR do navegador poderão ser coletados para identificar o URL ou domínio específico que apresenta problemas (por exemplo, falhas de carregamento de página ou alta latência) e esse domínio poderá ser configurado nos critérios de Log de Depuração de Solicitação.

Etapa 8. Escolha o método para recuperar os logs. Se você selecionar FTP Poll, os logs serão armazenados no SWA.

Etapa 9. Defina o nome de arquivo a ser usado para arquivos de log ou pressione Enter para aceitar o nome de arquivo gerado no momento.

Etapa 10. Selecione Não para a rollover de arquivos de log baseados no tempo, já que o log pára

após o número definido de solicitações ter sido atendido.

Etapa 11. Defina o tamanho máximo do arquivo em Bytes ou pressione Enter para aceitar o valor atual.

 Tip: Definir um tamanho maior de arquivo de registro pode dificultar o download e a revisão dos registros. Em vez de aumentar o tamanho dos arquivos de log individuais, é recomendável aumentar o número de arquivos de log (Próxima Etapa). Essa abordagem melhora a capacidade de gerenciamento e garante que todas as informações de depuração necessárias sejam capturadas sem criar arquivos muito grandes.

Etapa 12. Configure o número máximo de arquivos de log com base no número de módulos de proxy selecionados para log na Etapa 5 e nos critérios de correspondência de solicitação definidos na Etapa 7. A seleção de um limite de arquivo razoável é importante para garantir que todas as informações de depuração relevantes sejam capturadas sem interromper prematuramente o log, o que poderia resultar em logs incompletos ou ausentes.

Etapa 13. Selecione No quando solicitado com Deve ser enviado um alerta quando os arquivos são removidos devido ao número máximo de arquivos permitidos? Isso evita alertas desnecessários durante a rotação de log normal, especialmente quando os logs de depuração de solicitação são gerados intencionalmente para fins de solução de problemas.

Etapa 14. Selecione Não quando solicitado com Deseja compactar os logs (sim/não)? Isso mantém os arquivos de log descompactados, facilitando a revisão e a análise durante a solução de problemas.

Etapa 15. Pressione Enter para sair do assistente

Etapa 16. Digite commit e pressione Enter para salvar as alterações

```
SWA_CLI> logconfig

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
55. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
```

```
- HOSTKEYCONFIG - Configure SSH host keys.
- AUDITLOGCONFIG - Adjust settings for audit logging.
[]> new

Choose the log file type for this subscription:
1. ADC Engine Framework Logs
2. ADC Engine Logs
...
[Output removed to simplify readability]
...
53. Request Debug Logs
...
[Output removed to simplify readability]
...
[1]> 53

Please enter the name for the log:
[]> Request_Debug_Logs

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 5

Choose modules where enhanced request logging is to be performed.
Multiple selections can be made in the form of a comma separated or range list (e.g. 1,3,4 or 3-7)
Choosing the Default Proxy will enable enhanced logging across modules:
1. Default Proxy
2. Access Control Engine
3. Proxy Configuration
4. Disk Manager
5. Memory Manager
6. McAfee Integration Framework
7. Sophos Integration Framework
8. Webroot Integration Framework
9. Webcat Integration Framework
10. Connection Management
11. Authentication Framework
12. HTTPS
13. FTP proxy
14. WCCP Module
15. License Module
16. SNMP Module
17. WBRS Integration Framework
18. Logging Framework
19. Data Security Module
20. Miscellaneous Proxy Modules
21. DCA Engine Framework
22. AVC Engine Framework
23. Cloud Connector
24. SOCKS Proxy
25. Advanced Malware Protection
26. ArchiveScan module in proxy
27. Web Traffic Tap module in proxy
28. Bandwidth Control
29. Http2 proxy
30. ADC Engine Framework
[1]> 1-30
```

```
Please enter the number of requests for which to perform enhanced logging:
[1]> 100

Choose the request criteria for logging:
1. Client IP Address
2. Destination Domain
3. Destination IP Address
[1]> 1

Specify source IP address
[]> 10.20.3.15

Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> 1

Filename to use for log files:
[Request_Debug_Logs.text]>

Do you want to configure time-based log files rollover? [N]>

Please enter the maximum file size:
[10485760]>

Please enter the maximum number of files:
[10]> 50

Should an alert be sent when files are removed due to the maximum number of files allowed? [N]>

Do you want to compress logs (yes/no)
[n]>

Currently configured logs:
1. "Request_Debug_Logs" Type: "Request Debug Logs" Retrieval: FTP Poll
2. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
3. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
56. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll


SWA_LIC> commit

Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
```

Informações Relacionadas

- Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance
- Use as práticas recomendadas de dispositivos da Web seguros

- Acessar logs do dispositivo da Web seguro
- Configurar logs de envio de SCP em SWA com o Microsoft Server

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.