SmartEvent em Ambientes Multi Domain

Helio Leite

Security Engineer

Maio - 2024

Este documento criado em Maio de 2024 serve como um guia de implementação e troubleshooting de uma implantação distribuída do SmartEvent não substituindo os guias oficiais para um melhor detalhamento.
Os documentos oficiais são sempre atualizados e podem ser localizados nos links abaixo:

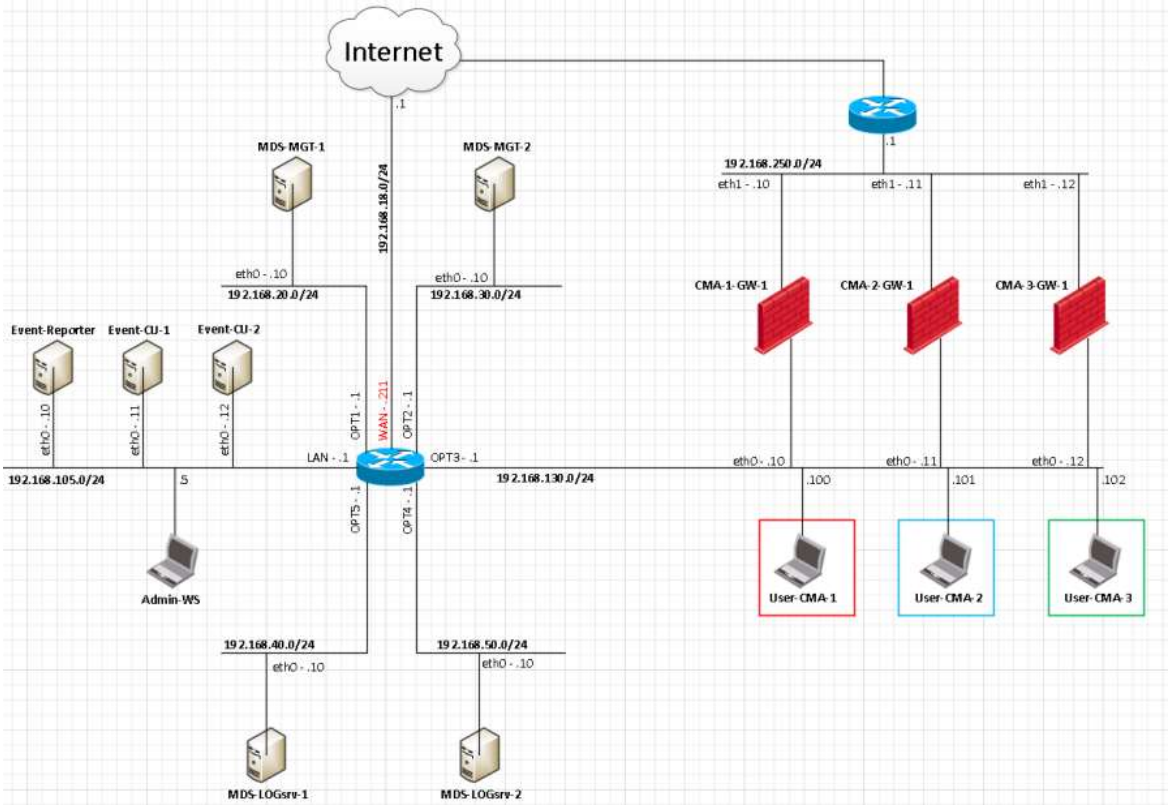
R81.20 Installation and Upgrade Guide
https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_Installation_and_Upgrade_Guide/Content/Topics-IUG/Getting-Started.htm
R81.20 Logging and Monitoring Administration Guide
https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_LoggingAndMonitoring_AdminGuide/Content/Topics-LMG/Deploying-SmartEvent.htm
ATRG: SmartEvent
https://support.checkpoint.com/results/sk/sk93970
Security Management Sizing
https://support.checkpoint.com/results/sk/sk181782
SNMP Best Practices All Versions
https://downloads.checkpoint.com/dc/download.htm?ID=31396
How to analyze logging rate to estimate daily GB ingestion quota required for Smart-1 Cloud or Log Sharing
https://support.checkpoint.com/results/sk/sk181549

Ambiente de laboratório

Foi criado um ambiente de laboratório para demonstrar as etapas de integração detalhadas neste documento.

- Todos os sistemas utilizando a versão R81.20 jumbo take_26
- O Ambiente consiste em:
  - 2 x MDS Management Servers
  - 2 x MDS Log Servers
    - Cada CMA possui 2 Domain Log Servers
  - 3 x CMAs (Não incluindo o Dominio Global)

- 3 x Gateways (1 x Gateway por CMA)
  - CMA-1-GW-1 é gerenciado pela CMA-1
  - CMA-2-GW-1 é gerenciado pela CMA-2
  - CMA-3-GW-1 é gerenciado pela CMA-3
- 3 x Máquinas de Testes (User-CMA-x)
- 1 x SmartEvent Reporter Server
- 2 x SmartEvent Correletion Unit Server



Etapas de preparação antes de configurar o SmartEvent

SIZING

O dimensionamento adequado é essencial para garantir que o(s) servidor(es) do SmartEvent seja(m) capaz(es) de acompanhar o volume de registros e logs que estão analisando.

O subdimensionamento pode levar a um desempenho lento e/ou à incapacidade de executar relatórios ou receber alertas.

NTP

Garantir que todos os sistemas tenham uma hora exata é fundamental por motivos operacionais/segurança.

Certifique-se de que todos os sistemas estejam configurados com servidores NTP e estejam ativamente sincronizados com

esses servidores.

Todos os relógios do sistema Multi-Domain Server devem ser sincronizados em aproximadamente um segundo.

Antes de criar um novo Multi-Domain Server ou Multi-Domain Log Server, você deve

sincronizar seu relógio com outros componentes do sistema.

A sincronização do relógio é importante pelos seguintes motivos:

- A confiança no SIC pode falhar se os dispositivos não estiverem sincronizados corretamente
- A SmartEvent Correlation Unit usa registros de data e hora, que devem ser precisos
- Certifique-se de que as tarefas agendadas sejam executados no horário correto
- A validação do certificado é baseada no horário correto

Se você não se certificar de que todos os sistemas estão configurados com um servidor NTP em funcionamento, poderá ocorrer erros na visualização de registros e a omissão de registros em determinados relatórios.

Padrão de envio e armazenamento de log

Certifique-se de que cada CMA tenha pelo menos dois servidores de logs. Isso é fundamental do ponto de vista da redundância

Idealmente, os GWs devem ser configurados para enviar log somente para servidores dedicados a logs servers ou multi domain log server e não enviar logs para servidores de gerenciamento ou domínios de gerenciamento em nenhuma circunstância.

Certifique-se de que exista um padrão para registro de log bem definido. Por exemplo:

- Padrão 1:
    - Todos os GWs na CMA X devem ser configurados com distribuição dinâmica de logs
    - Nenhum servidor de logs de backup está configurado
- Padrão 2:
    - Todos os GWs na CMA X devem ser configurados para registrar logs em 2 servidores de logs de domínio o tempo todo
    - Nenhum servidor de logs de backup está configurado
- Padrão 3:
    - Todos os GWs na CMA X devem ser configurados para registrar-se em 1 servidor de logs de domínio
    - O outro servidor de logs de domínio está configurado como servidor de backup

Neste laboratório, estamos seguindo o "Padrão 1" acima.
Certifique-se de que todos os GWs em um determinado CMA estejam seguindo o padrão de registro. Para verificar basta analisar a configuração de log de cada objeto de GW.
Essa é uma etapa essencial para garantir a previsibilidade de onde os GWs enviam os logs.
Com essa etapa, a etapa crítica a seguir será decidida, onde o mapeamento de quais Servidores de log de domínio enviam logs para quais unidades de correlação do SmartEvent.
Não ter e/ou não seguir um padrão de registro definido pode levar a muitos problemas, incluindo falsos negativos nos relatórios/alertas do SmartEvent.

SmartEvent Correlation Unit - Mapeamento do servidor de log

Defina o plano de mapeamento de quais servidores SmartEvent Correlation Unit coletarão logs de quais servidores de log de domínio.
Certifique-se de que a coleta esteja configurada de tal forma que:
Supondo que todos os GWs estejam registrando logs de acordo com o padrão definido na etapa anterior, a arquitetura abranje todos os logs gerados por todos os GWs.
Por exemplo, neste laboratório:
Como estamos seguindo o padrão 1 para todos as CMAs, que utiliza o Dynamic Log distribuição dinâmica de logs, os servidores SmartEvent devem ser configurados para coletar logs de todos os servidores Domain Log em cada CMA.
Neste laboratório, o plano de mapeamento é:

CMA	Domain Log Servers	SmartEvent Correlation Unit
CMA-1	CMA_1_LOGsrv-1 CMA_1_LOGsrv-2	**Event-CU-1**
CMA-2	CMA_2_LOGsrv-1 CMA_2_LOGsrv-2	**Event-CU-1**
CMA-3	CMA_3_LOGsrv-1 CMA_3_LOGsrv-2	**Event-CU-2**

A não criação de um plano de mapeamento adequado pode levar a:

- Excesso de utilização de uma determinada unidade de correlação de SmartEvent
- Registros ausentes nos relatórios/alertas do SmartEvent (falsos negativos)

Encaminhamento de logs ativado em todos os GWs

Caso um GW não consiga fazer o registro em pelo menos um dos servidores de log de domínio configurados, ele começará a registrar localmente em seu HDD local.

Recomenda-se ativar o encaminhamento de logs em cada GW em uma programação predefinida (por exemplo todos os dias às 12 horas)

Essa configuração garante que, no caso raro de um GW começar a registrar logs localmente, após restaurar a conectividade com pelo menos um de seus servidores de log de domínio, esses logs locais serão encaminhados para o servidor de registros do domínio.

A não conclusão dessa etapa pode resultar em:

- O disco do GW ficar sem espaço
- Registros ausentes nos relatórios/alertas do SmartEvent (falsos negativos)

Verifique se os gateways estão registrando

Todos os relatórios/alertas do SmartEvent são baseados em registros.

Se os GWs não estiverem registrando corretamente em seus servidores de log configurados, esses registros não serão processados pelo SmartEvent e, portanto, esses dados serão omitidos dos relatórios/alertas do SmartEvent.

Verifique se todos os GWs estão registrando ativamente em seus servidores de log configurados.

Corrija os problemas de registro de qualquer GW na CMA antes de prosseguir.

É altamente recomendável o monitoramento ativo dos GWs para garantir que estejam registrando corretamente. Uma maneira como isso pode ser feito é por meio de SNMP

Logging

Counter	OID	Format	Description
Log Server connectivity	fwLSConnOverall .1.3.6.1.4.1.2620.1.1.30.1	Integer 0-2	Connectivity with log servers: 0=OK, 1=Warning, 2=Error
Log Server connectivity description	fwLSConnOverallDesc .1.3.6.1.4.1.2620.1.1.30.2	String	Description of connectivity status with log servers
Local logging status	fwLocalLoggingStat .1.3.6.1.4.1.2620.1.1.30.5	Integer 0-3	Status of local logging: • 0=to log servers • 1=local configured • 2=local due to connectivity issues • 3=local due to high rate
Local logging status	fwLocalLoggingDesc .1.3.6.1.4.1.2620.1.1.30.4	String	Description of local logging status

A falha no monitoramento do status de registro do GW pode levar a:

- O disco do GW ficar sem espaço
- Registros ausentes nos relatórios/alertas do SmartEvent (falsos negativos)

Ativação e configuração de blades

Certifique-se de que todas as blades Access/Threat aplicáveis estejam ativadas nos GWs relevantes.

Essa etapa é fundamental para o consumidor dos relatórios do SmartEvent. O consumidor do relatório deve entender quais GWs têm quais blades ativados.

Isso define a expectativa de quais tipos de eventos podem ser vistos nos relatórios do SmartEvent.

Configurações de log/rastreamento nas regras de políticas

Histórico:

- Escolha de regras para rastreamento:
- Os registros são úteis se mostrarem os padrões de tráfego nos quais você está interessado.
- Certifique-se de que sua política de segurança rastreie todas as regras necessárias. Quando você ativa o log em várias regras, o arquivo de log se torna maior e requer mais espaço em disco e operações de gerenciamento.
- Para equilibrar esses requisitos, rastreie as regras que podem ajudá-lo a melhorar sua segurança cibernética, que ajudem a entender o comportamento do usuário e que possam ser úteis em relatórios.
- Opções de log/rastreamento:
- **Log** - Essa é a opção de rastreamento padrão. Ela mostra todas as informações que o o Security Gateway usou para fazer a correspondência com a conexão. No mínimo, são a origem, o destino, a porta de origem e a porta de destino. Se houver uma correspondência em uma regra que especifique um aplicativo, um registro de sessão mostra o nome do aplicativo (por exemplo, Dropbox). Se houver uma correspondência em uma regra que especifique um tipo de dados, o registro de sessão mostrará informações sobre os arquivos e o conteúdo dos arquivos.
- **Accounting** - Selecione essa opção para atualizar o registro em intervalos de 10 minutos, para para mostrar a quantidade de dados transmitidos na conexão: Bytes de upload, bytes de download e tempo de navegação.

  - Opções de log/rastreamento avançado:
  - Registro detalhado (Detailed Logs) e Registro estendido (Extended Logs) só estarão disponíveis se uma ou mais das esses Blades estiverem ativados na política:
  - Application Control / URL Filtering
  - Content Awareness
  - Mobile Access

- **Registro detalhado (Detailed Log)** - Equivalente à opção log, mas também mostra o aplicativo aplicativo que correspondeu às conexões, mesmo que a regra não especifique um aplicativo. Prática recomendada - Use para uma regra de limpeza (Any/internet/Accept) de uma layer de política para filtragem de aplicativos e URL que foi atualizada a partir de uma base de regras da versão R77.
- **Extended Log (Registro estendido)**- Equivalente à opção Detalhado, mas também mostra uma lista completa de lista completa de URLs e arquivos na conexão ou na sessão. As URLs e arquivos são exibidos no painel inferior da exibição Logs
- Geração de Logs:
  - **Per Connection (Por conexão)** - Selecione essa opção para mostrar um registro diferente para cada conexão na sessão. Esse é o padrão para regras em uma layer com apenas o Firewall ativado. Esses são os registros básicos do Firewall.
  - **Per Session (Por sessão)** - Selecione essa opção para gerar um único registro para todas as conexões na mesma sessão. Esse é o padrão para as regras em uma layer com URL Filtering, Application Control ou Content Awareness ativados. Esses são logs básicos de controle de aplicativos.
- Recomendações:
- Habilite o registro em log somente para as regras necessárias
- Evite o registro de regras barulhentas que não agregam muito valor (por exemplo, comunicação VOIP, atualizações de NTP, sondagem de SNMP etc.)
- Escolha as opções de registro apropriadas para cada regra em cada pacote de políticas
- A não execução dessa etapa pode fazer com que sejam relatadas menos informações do que o desejado. Por exemplo, se o consumidor do relatório SmartEvent quiser determinar os principais aplicativos por taxa de transferência que passam por um GW, ele precisará se certificar de que as regras aplicáveis na a política tenham a caixa de seleção "Accounting" ativada.

Preparação do sistema operacional do SmartEvent Server

Complete todos os passos abaixo em todos os servidores SmartEvent

- Instalação limpa do Gaia R81.20
- Execute o “First Time Configuration Wizard”
- Durante o FTCW, você deve efetuar as seguintes configurações:
- Na janela descrita “**Installation Type”** selecione **Security Gateway and/or Security Management**
- Na próxima janela **“Products”**
- Na sessão “**Products”** selecione somente “**Security Management”**
- Na sessão “**Clustering”** no campo **“Define Security Management”** selecione **“Log Server / SmartEvent only”**
- Na Janela descrita como **“Security Management Administrator”** selecione uma das opções:
- **“Use Gaia Administrator”**
- **“Define a New Administrator”**
- Na janela **“Security Management GUI Clients”** configure os computadores permitidos ao acesso:
- **Any IP Address** – Permite todos os computadores a conectar
- **This Machine –** Permite somente o computador especificado conectar
- **Network –** Permite todos os computadores na rede especificada conectar.
- **Range of IPv4 address** – Permite todos os computadores no range especificado conectar.
- Em **Secure Internal Communication** entre com a **Activation Key (**Entre 4 e 127 Caracters) para conexão com o MultiDomain
- Atualize o Agente do CPUSE
- Instale o ultimo jumbo hotfix recomendado
- Complete a configuração do Sistema Operacional
- Verifique se todos os Servidores estão ok (EX: NTP, DNS, Rotas, Backups Agendados, etc)

Configuração do SmartEvent

Global Assignment

Um Global Assignment é um objeto do sistema de gerenciamento de segurança de vários domínios que atribui uma configuração global a um domínio específico. Você cria atribuições globais para atribuir diferentes combinações de políticas de controle de acesso global, políticas globais de controle de acesso, políticas globais de prevenção contra ameaças e definições de objetos globais a diferentes domínios.

Quando você cria uma nova atribuição global, ela atribui automaticamente a configuração global especificada ao domínio especificado. Ele também publica a atribuição e
atualiza as políticas locais do domínio.

Depois de adicionar o servidor SmartEvent ao banco de dados global, publique a sessão de domínio global e reatribua a configuração global e após Instale as políticas em cada dominio

- Configuração inicial:
- Conecte-se ao MDS com o SmartConsole
- Vá para: Multi-Domain > Global Assignments
- Clique em: Assign > New Assignment
- Na janela "New Assignment" (Nova atribuição), selecione: 'Local Domain' (Domínio local)
- **Importante** - Você pode criar uma atribuição global que não inclua uma política global de controle de acesso e prevenção de ameaças. Para fazer isso, selecione o valor Nenhum para ambos os tipos de política. A configuração global atribui apenas os objetos e configurações globais definidos aos dominios.
- Clique em Publish & Assign
- Repita o procedimento para cada domínio
- Quando terminar, suas atribuições globais deverão ter a seguinte aparência:

Reassign

Quando você faz alterações nos itens de configuração global, o status de “**assign”** muda para "**Not Up to Date**".

Para reatribuir as configurações globais:

- Conecte-se ao MDS com o SmartConsole
- Vá para: Multi-Domain > Global Assignments
- Clique com o botão direito do mouse em um ou mais domínios e clique em "Reassign" (Reatribuir)

Criação de objetos SmartEvent no domínio Global

- Conecte-se ao MDS com o SmartConsole
- Abra o domínio Global
- Dentro do dominio Global adicione um novo objeto "Check Point Host".
- Configure o IP
- Estabeleça o SIC
- Configure as blades:
- SmartEvent Server:
- SmartEvent Server
- SmartEvent Correlation Unit
- Logging & Status
- SmartEvent Correlation Unit:
- SmartEvent Correlation Unit
- Logging & Status

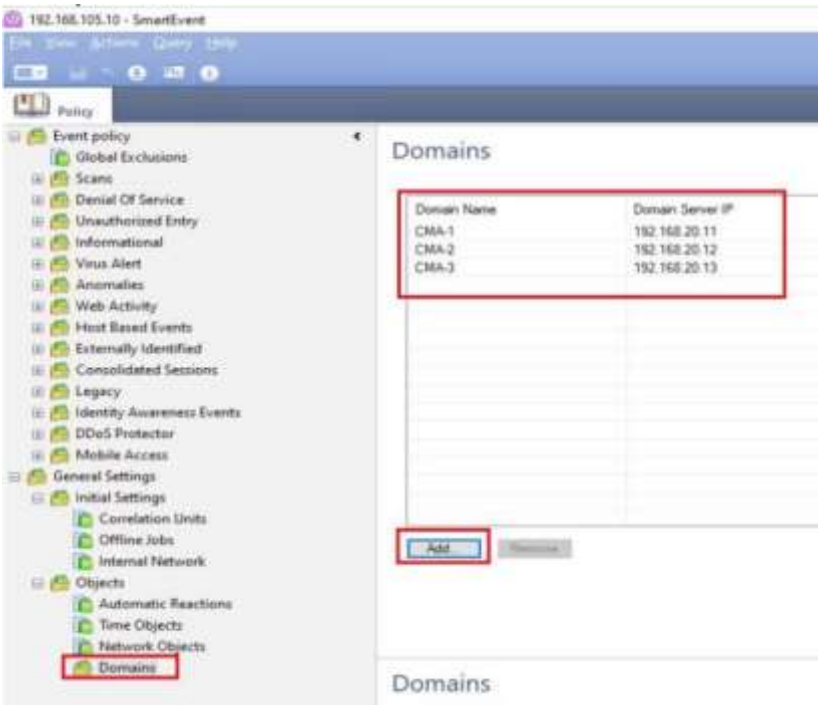
Geral

Após as etapas anteriores:

- Conclua a reatribuição da política global
- Instale o banco de dados (Install Database) em cada domínio para todos os objetos disponíveis

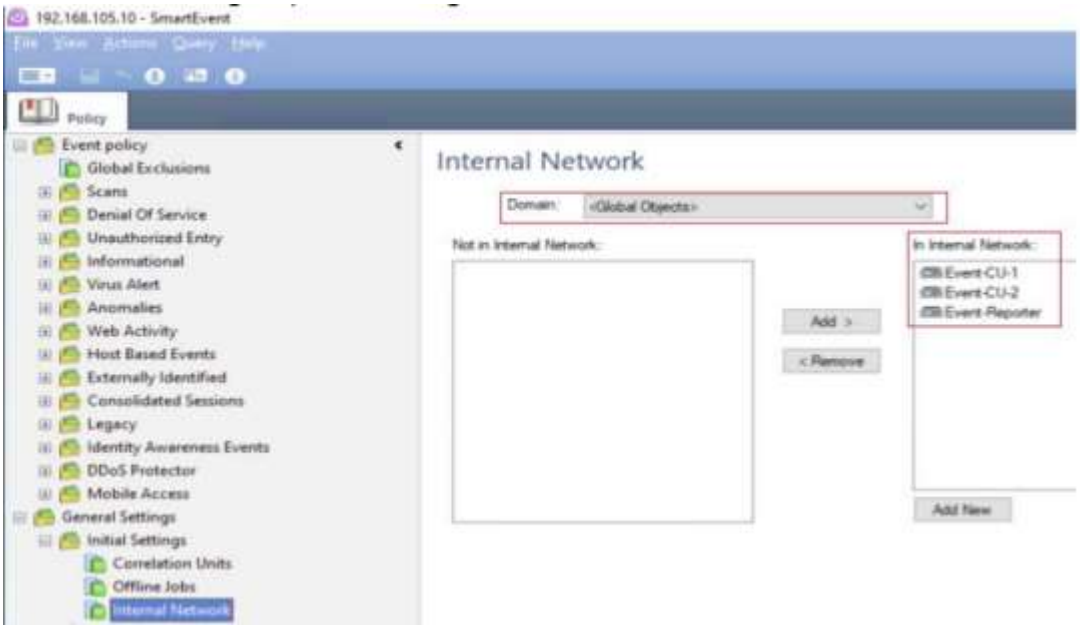
Configuração do cliente legado SmartEvent:

Abra o cliente legado do SmartEvent: 'AnalyzerClient.exe', digite o IP do servidor SmartEvent dedicado e após o login, conclua a ativação do domínio:



Defina rede interna

- Acesse: General Settings > Initial Settings > Internal Network
- Para cada domínio (global e não global), adicione-o à rede interna:
- Objetos do servidor SmartEvent
- Grupo de rede que contém todas as redes internas



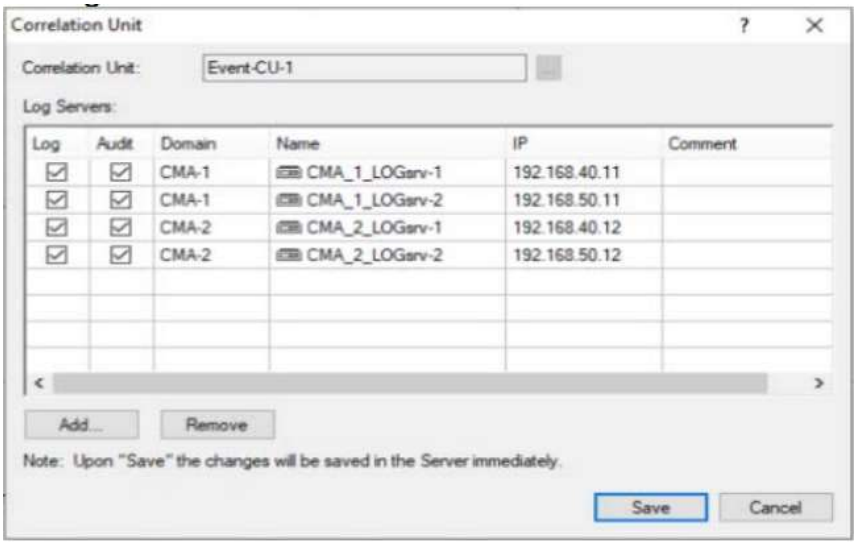
Correlation Units

A Event Policy será instalada nas correlation units adicionadas nesta seção. Consulte o plano de mapeamento da unidade de correlação - servidor de log criado durante a fase de planejamento

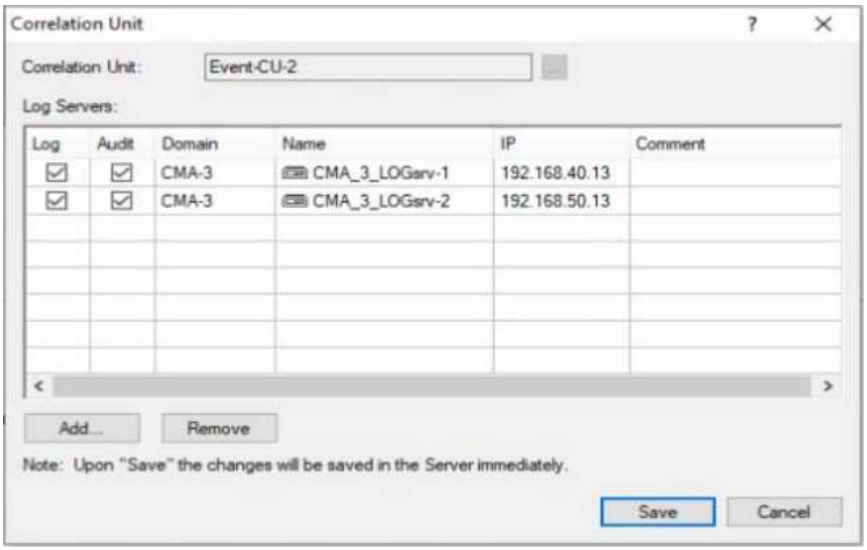
- Vá para: General Settings (Configurações gerais) > Initial Settings (Configurações iniciais) > Correlation Units (Unidades de correlação)
- Configure de acordo com o plano de mapeamento

Neste laboratório:

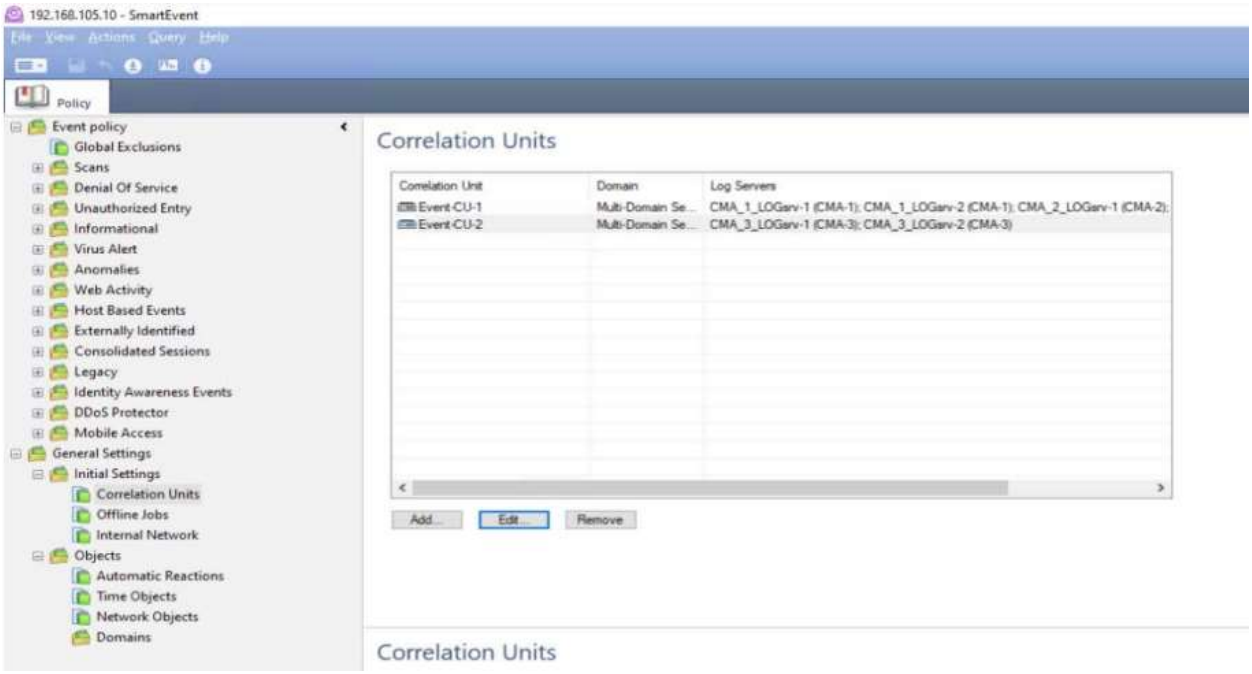
Configuração da Correlation Unit - Event-CU-1:



Configuração da Correlation Unit - Event-CU-2:



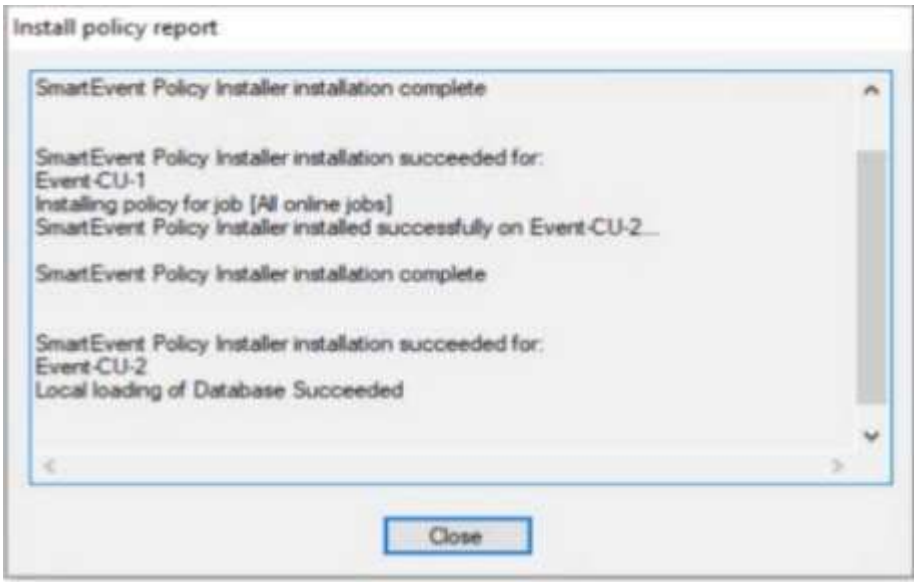
Comple a configuração para ambos Correlation Units



Instale a política de eventos

- Actions > Install Event Policy

Verifique se a instalação da política foi bem-sucedida em todas as unidades de correlação:



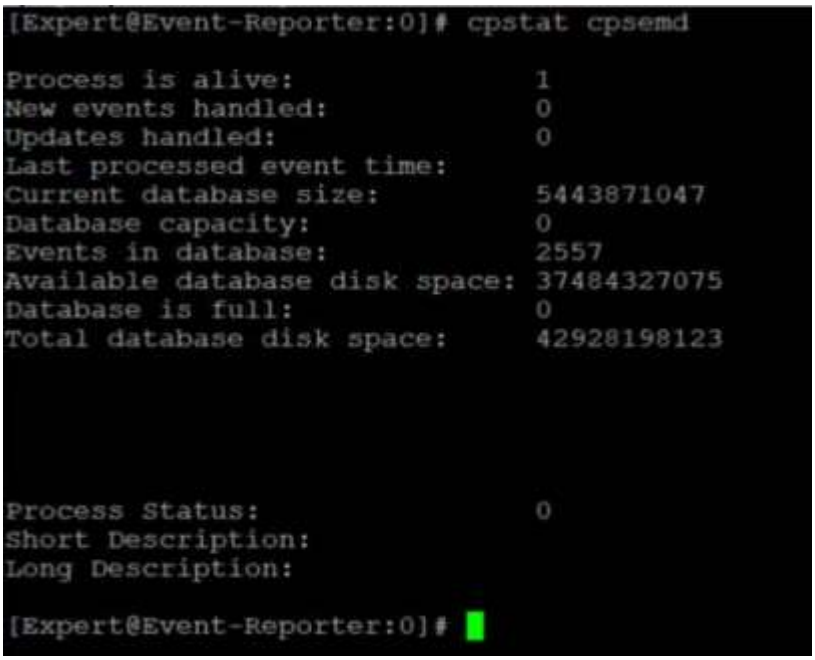
Ativação do SmartEvent por CMA

Para cada CMA adicional que precisa ser integrado ao SmartEvent, siga todas as etapas documentadas na seção anterior na ordem mostrada. Execute todas as etapas aplicáveis.

Verificação

Verificação do sistema SmartEvent:

- Servidor do SmartEvent Reporter:
- cpstat cpsemd



- Servidor do SmartEvent Correlation Unit
- cpstat cpsead

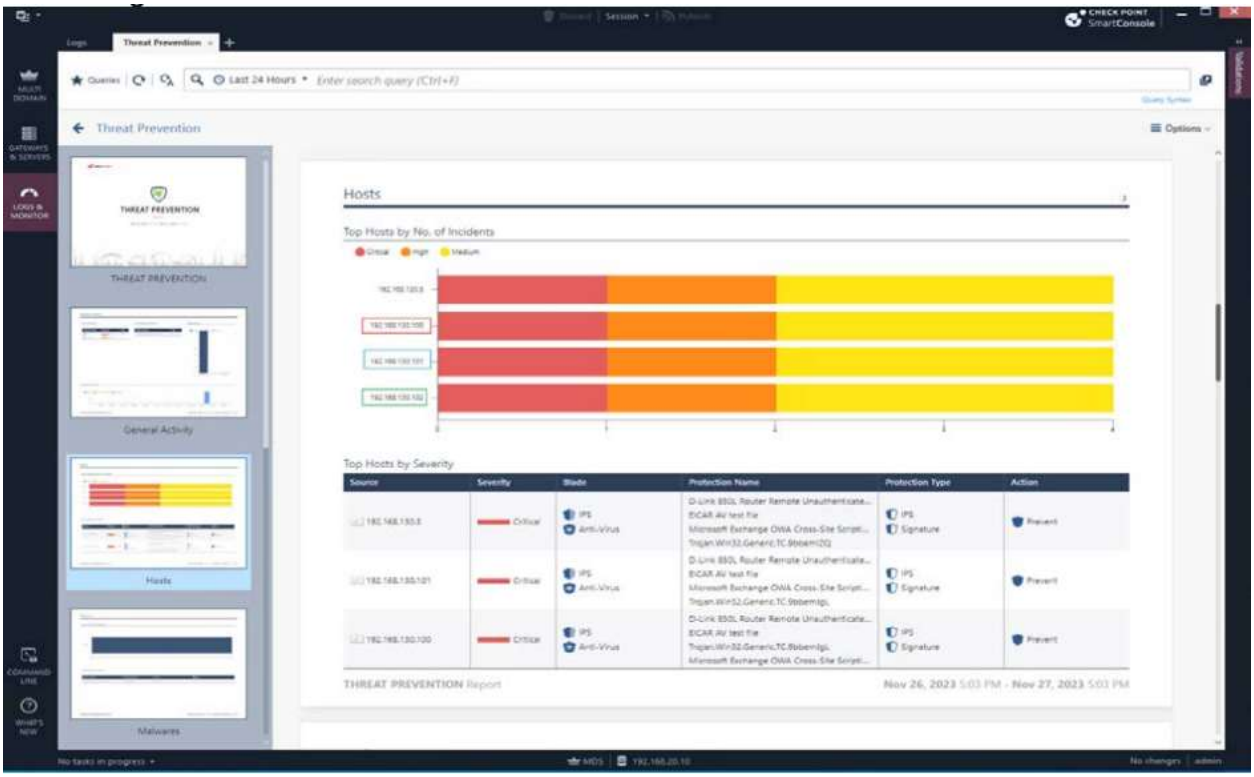
Como esperado, o servidor Event-CU-2 está coletando ativamente os registros de ambos os servidores de registro do Domain

Realize um teste manual para garantir que o SmartEvent esteja funcionando corretamente:

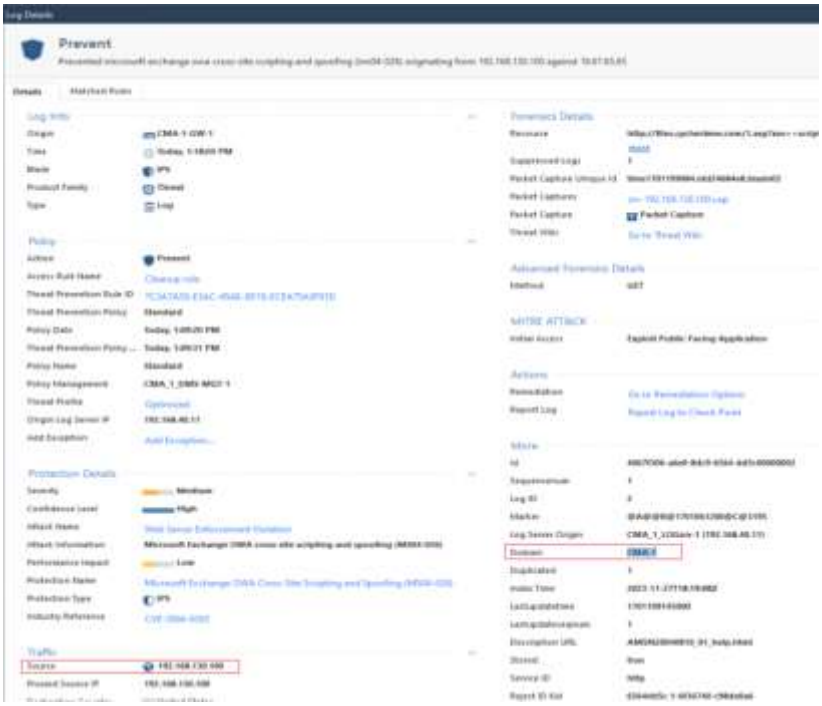
- Obter acesso a um host que esteja na rede protegida da CMA em questão
- Identificar o IP do usuário e o horário do teste
- Faça com que esse usuário acesse: https://cpcheckme.com
- Concluir os testes de segurança de rede
- Verifique os registros na SmartConsole para verificar se os logs de várias layers de ameaças foram acionados
- Execute os relatórios do SmartEvent para verificar se você pode identificar os eventos aplicáveis
- Os relatórios do SmartEvent podem ser executados no nível do MDS ou no nível de domínio
- Os relatórios/visualizações em nível de MDS conterão os registros de todas as CMAs
- Os relatórios/visualizações no nível da CMA conterão os registros apenas desta CMA

Resultados do laboratório:

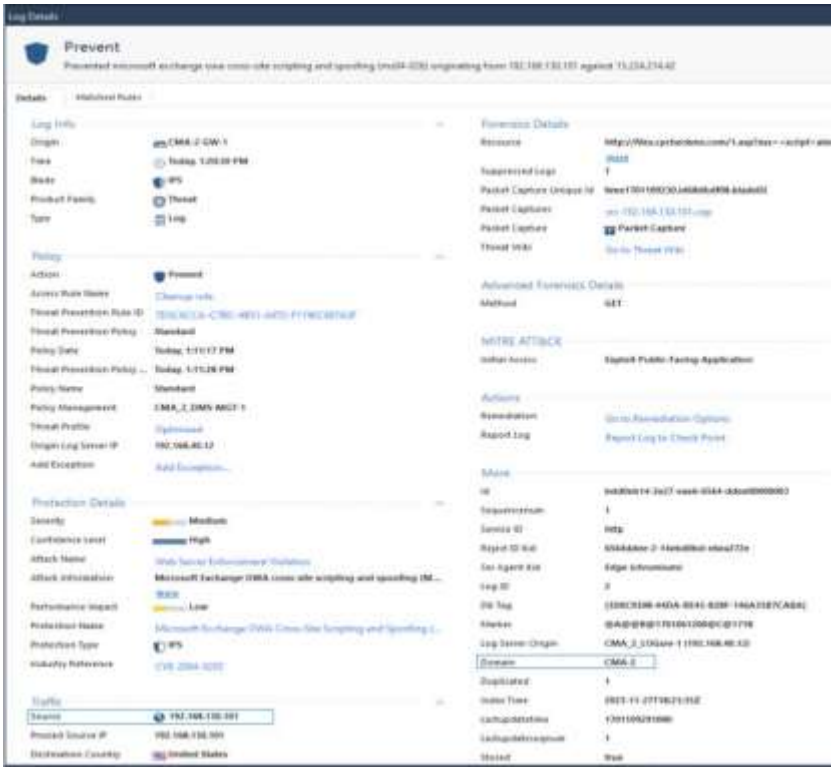
- De acordo com o diagrama de laboratório abaixo:
  - A estação de trabalho "User-CMA-1" (192.168.130.100) aponta para a CMA-1-GW-1 como seu GW padrão.
  - A estação de trabalho "User-CMA-2" (192.168.130.101) aponta para a CMA-2-GW-1 como seu GW padrão.
  - A estação de trabalho 'User-CMA-3' (192.168.130.102) aponta para o CMA-3-GW-1 como seu GW padrão.
- O teste documentado acima foi executado em cada uma das três estações de trabalho de teste de laboratório
- Relatório em nível global:
  - Conforme mostrado abaixo, o relatório pronto para uso "Threat Prevention" captura registros/eventos de ameaças de cada uma das estações de teste do laboratório. Captura os registros/eventos de ameaças de cada uma das 3 estações de trabalho de teste de cada uma das 3 CMAs.



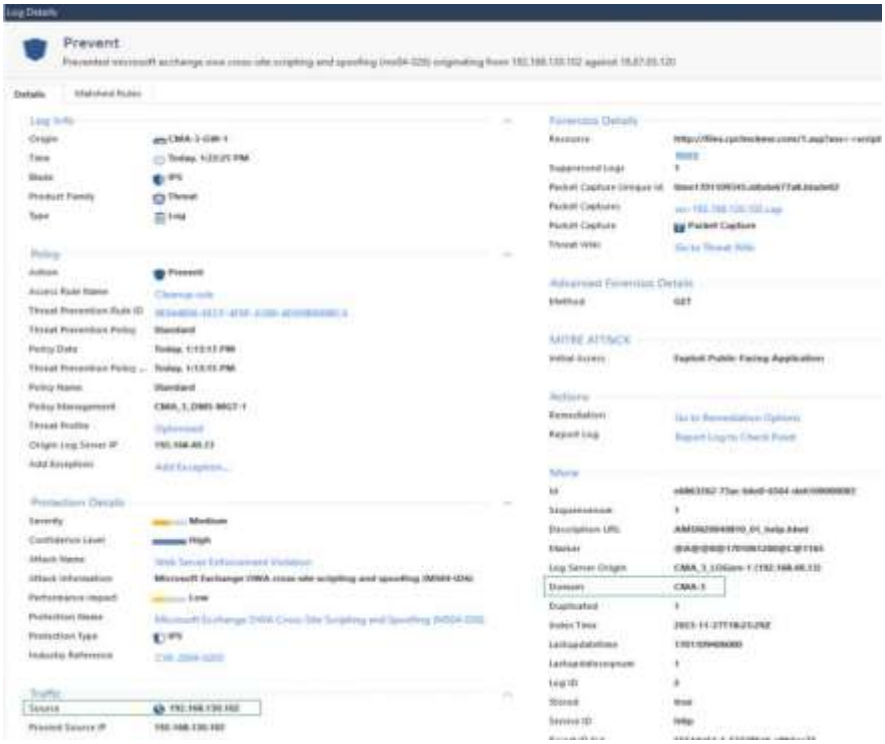
Log CMA-1:



Log CMA-2:



Log CMA-3:



- Relatório no nível do CMA:
- Conforme mostrado abaixo, o mesmo relatório foi executado no nível do CMA apenas com os logs/eventos desse CMA (somente os eventos de 192.168.130.100 são mostrados)