Exemplo de configuração do Syslog ASA

Índice

Introdução

Este documento fornece uma configuração de exemplo que demonstra como configurar opções de registro diferentes em uma ferramenta de segurança adaptável (ASA) essa versão de código 8.4 das corridas ou mais atrasado.

A versão ASA 8.4 introduziu técnicas de filtração muito granuladas a fim permitir que somente determinados mensagens do syslog especificados sejam apresentados. A seção básica do Syslog deste documento demonstra uma configuração tradicional do Syslog. A seção avançada do Syslog deste documento mostra as características novas do Syslog na versão 8.4. Refira mensagens de Log de sistema guia do dispositivo do Cisco Security, versão 8.x e 9.x para o guia completo dos mensagens de Log de sistema.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 5515 com versão de software 8.4 ASA
- Versão 7.1.6 do Cisco Adaptive Security Device Manager (ASDM)

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

> Nota: Refira ASA 8.2: Configurar o Syslog usando o ASDM para mais informação para detalhes de configuração similares com versão 7.1 e mais recente ASDM.

Syslog básico

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Incorpore estes comandos a fim permitir o registro, os logs da vista, e os ajustes de configuração da vista.

- **registrar permite** - Permite a transmissão dos mensagens do syslog a todos os lugar da saída.
- **nenhum registro permite -** Inutilizações que registram a todos os lugar da saída.
- **registro da mostra -** Alista os índices do buffer do Syslog assim como informação e estatísticas que se referem a configuração atual.

O ASA pode enviar mensagens do syslog aos vários destinos. Incorpore os comandos a estas seções a fim especificar os lugar que você como a informação de syslog seria enviado:

Envie a informação de registro ao buffer interno

```
logging buffered severity_level
```

O software externo ou o hardware não são exigidos quando você armazena os mensagens do syslog no buffer interno ASA. Inscreva o **comando show logging** a fim ver os mensagens do syslog armazenados. O buffer interno tem um tamanho máximo do 1 MB (configurável com o comando de **registro do tamanho de buffer**). Em consequência, pôde envolver muito rapidamente. Mantenha isto na mente quando você escolhe um nível de registro para o buffer interno como uns níveis mais verbosos do registro puderam rapidamente se encher, e o envoltório, o buffer interno.

Envie a informação de registro a um servidor de SYSLOG

```
logging host interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]
logging trap severity_level
logging facility number
```

Um server que execute um aplicativo do Syslog é exigido a fim enviar mensagens do syslog a um host externo. O ASA envia o Syslog na porta 514 UDP à revelia, mas o protocolo e a porta podem ser escolhidos. Se o TCP é escolhido como o protocolo de registro, este faz com que o ASA envie Syslog através de uma conexão de TCP ao servidor de SYSLOG. Se o server é inacessível, ou a conexão de TCP ao server não pode ser estabelecida, o ASA, à revelia, obstruirá TODAS AS novas conexões. Este comportamento pode ser desabilitado se você permite a **licença-hostdown de registro**. Veja o manual de configuração para obter mais informações sobre do comando de **registro da licença-hostdown**.

Envie a informação de registro como email

```
logging mail severity_level
logging recipient-address email_address
logging from-address email_address
smtp-server ip_address
```

Um servidor SMTP é exigido quando você envia os mensagens do syslog nos email. A configuração correta no servidor SMTP é necessária a fim assegurar-se de que você possa com sucesso retransmitir email do ASA ao cliente de email especificado. Se este nível de registro é ajustado a um nível muito verboso, como *debugar* ou *informativo,* você pôde gerar um número significativo de Syslog desde que cada email enviado por esta configuração de registro causa para cima uns logs de quatro ou mais adicionais a ser gerados.

Envie a informação de registro ao console serial

```
logging console severity_level
```

O logging de console permite mensagens do syslog de indicar no console ASA (tty) como ocorrem. Se o logging de console é configurado, todos registram a geração no ASA ratelimited a 9800 bps, a velocidade do console serial ASA. Isto pôde fazer com que os Syslog sejam deixados cair a todos os destinos, que incluem o buffer interno. Não use o logging de console para Syslog verbosos por este motivo.

Envie a informação de registro a uma sessão do telnet/SSH

```
logging monitor severity_level
terminal monitor
```

O monitor de registro permite mensagens do syslog de indicar enquanto ocorrem quando você alcança o console ASA com telnet ou o SSH e o comando terminal monitor estão executados dessa sessão. A fim parar a impressão dos logs a sua sessão, não inscreva **nenhum comando terminal monitor**.

Indique mensagens de registro no ASDM

```
logging asdm severity_level
```

O ASDM igualmente tem um buffer que possa ser usado para armazenar mensagens do syslog. Inscreva o **comando show logging asdm** a fim indicar o índice do buffer do Syslog ASDM.

Envie logs a uma estação do gerenciamento de SNMP

```
logging history severity_level
snmp-server host [if_name] ip_addr
snmp-server location text
snmp-server contact text
snmp-server community key
snmp-server enable traps
```

Os usuários precisam um ambiente funcional existente do Simple Network Management Protocol (SNMP) a fim enviar mensagens do syslog com SNMP. Veja comandos ajustando-se e controlando destinos de emissor para uma referência completa nos comandos que você pode se usar para ajustar e controlar destinos de emissor. Veja as mensagens alistadas pelo nível de seriedade para as mensagens alistadas pelo nível de seriedade.

Adicionar Timestamps aos Syslog

A fim ajudar a alinhar e os eventos da ordem, timestamps podem ser adicionados aos Syslog. Isto é recomendado a fim ajudar a seguir as edições baseadas no tempo. A fim permitir timestamps, inscreva o **comando logging timestamp**. Estão aqui dois exemplos do Syslog, um sem o timestamp e um com:

```
%ASA-6-302016: Teardown UDP connection 806353 for outside:172.18.123.243/24057 to
identity:172.18.124.136/161 duration 0:02:01 bytes 313

Jul 03 2014 14:33:09: %ASA-6-302014: Teardown TCP connection 806405 for
inside:10.0.0.100/50554 to identity:172.18.124.136/51358 duration 0:00:00 bytes
442 TCP Reset-I
```

Exemplo 1

Esta saída mostra uma configuração de exemplo para registrar no **buffer** com o nível de seriedade da **eliminação de erros**.

```
logging enable
logging buffered debugging
```

Esse é o exemplo de saída.

```
%ASA-6-308001: console enable password incorrect for number tries (from 10.1.1.15)
```

Configurar o Syslog básico com ASDM

Este procedimento demonstra a configuração ASDM para todos os destinos disponíveis do Syslog.

1. A fim permitir a abertura do ASA, configurar primeiramente os parâmetros de registro básicos. Escolha a **configuração > as características > as propriedades > instalação de registro > de registro**. Verifique a caixa de verificação de **registro Enable** a fim permitir Syslog.
2. A fim configurar um servidor interno como o destino para Syslog, para escolher **servidores de SYSLOG no** registro e no clique **adicionar** a fim adicionar um servidor de SYSLOG. Incorpore os detalhes do servidor de SYSLOG à caixa do servidor de SYSLOG adicionar e escolha-os **ESTÁ BEM** quando você é feito.
3. Escolha a **instalação do email na** ordem de abertura enviar mensagens do syslog como email aos receptores específicos. Especifique o endereço email da fonte na caixa do endereço email da fonte e escolha-o **adicionam** a fim configurar o endereço email do destino dos receptores do email e do nível de severidade da mensagem. Clique a **APROVAÇÃO** quando você é feito.
4. Escolha a **administração do dispositivo**, **registrando,** escolha o **S TP**, e incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor primário a fim especificar o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor SMTP.
5. Se você quer enviar Syslog como o SNMP traps, você deve primeiramente definir um servidor SNMP. Escolha o **SNMP** dentro no menu do **acesso de gerenciamento** a fim especificar o endereço das estações do gerenciamento de SNMP e de suas propriedades específicas.
6. Escolha **adicionam** a fim adicionar uma estação do gerenciamento de SNMP. Incorpore os detalhes do host SNMP e clique a **APROVAÇÃO**.
7. A fim permitir logs de ser enviado a alguns dos destinos mencionados prévios, escolha **filtros de registro na** seção de registro. Isto apresenta-o com cada destino de registro possível e o nível atual dos logs que são enviados 2 aqueles destinos. Escolha o destino de registro desejado e o clique **edita**. Neste exemplo, o destino dos “servidores de SYSLOG é alterado.
8. Escolha uma severidade apropriada, neste caso **informativa, do filtro na** lista de drop-down da **severidade**. Clique a **APROVAÇÃO** quando você é feito.
9. O clique **aplica-se** depois que você retorna ao indicador de registro dos filtros.

Envie mensagens do syslog sobre um VPN a um servidor de SYSLOG

No projeto simples do VPN de Site-para-Site ou no projeto de hub-and-spoke mais complicado, o administrador pôde querer monitorar todos os Firewall remotos ASA com o servidor SNMP e o servidor de SYSLOG situados em uma instalação central.

A fim configurar a configuração de VPN do IPSec local a local, refira PIX/ASA 7.x e acima: Exemplo da configuração de túnel PIX-à-PIX VPN. Independentemente da configuração de VPN, você tem que configurar o SNMP e o tráfego interessante para o servidor de SYSLOG na central e na site local.

Configuração central ASA

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the ASA 5515.

access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote ASA.

access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514


logging enable
logging trap debugging

!--- Define logging host information.
logging facility 16
logging host inside 172.22.1.5

!--- Define the SNMP configuration.
snmp-server host inside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

Configuração remota ASA

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind ASA 5515.
access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS (TCP/UDP port - 162) and
!--- syslog traffic (UDP port - 514) sent from this ASA outside
!--- interface to the SYSLOG server.
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 514

!--- Define syslog server.
logging facility 23
logging host outside 172.22.1.5

!--- Define SNMP server.
snmp-server host outside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

Refira a monitoração do Firewall seguro de Cisco ASA usando o SNMP e syslog por meio de túnel VPN para obter mais informações sobre de como configurar a versão ASA 8.4

Syslog avançado

A versão ASA 8.4 fornece diversos mecanismos que o permitem de configurar e controlar mensagens do syslog nos grupos. Estes mecanismos incluem o nível de severidade da mensagem, a classe de mensagem, o ID de mensagem, ou uma lista do mensagem personalizada que você cria. Com o uso destes mecanismos, você pode inscrever um comando único que se aplique aos grupos pequenos ou grandes de mensagens. Quando você estabelece Syslog esta maneira, você pode capturar mensagens do grupo especificado da mensagem e já não todas as mensagens da mesma severidade.

Use a lista da mensagem

Use a lista da mensagem a fim incluir somente os mensagens do syslog interessados pelo nível de seriedade e o ID em um grupo, a seguir associe esta lista da mensagem com o destino desejado.

Termine estas etapas a fim configurar uma lista da mensagem:

1. Entre no ***message_list da*** **lista de registro /** comando ***nivelado do [class message_class] do severity_level*** a fim criar uma lista da mensagem que inclua mensagens com uma lista especificada do nível de seriedade ou da mensagem.
2. Inscreva o **comando logging list message_list message syslog_id-syslog_id2** a fim adicionar mensagens adicionais à lista da mensagem apenas criada.
3. Inscreva o **comando logging destination message_list** a fim especificar o destino da lista da mensagem criada.

Exemplo 2

Incorpore estes comandos a fim criar uma lista da mensagem, que inclua toda a severidade 2 mensagens (críticas) com a adição da mensagem 611101 611323, e igualmente tenha-os enviados ao console:

```
logging list my_critical_messages level 2
logging list my_critical_messages message 611101-611323
logging console my_critical_messages
```

Configuração ASDM

Este procedimento mostra uma configuração ASDM por exemplo 2 com o uso da lista da mensagem.

1. Escolha **lista do evento** sob o registro e o clique **adiciona** a fim criar uma lista da mensagem.
2. Dê entrada com o nome da lista da mensagem na caixa de nome. **Os my_critical_messages** são usados neste caso. O clique **adiciona** sob filtros da classe de evento/severidade.
3. Escolha **tudo da** lista de drop-down da classe de evento. Escolha **crítico da** lista de drop-down da severidade. Clique a **APROVAÇÃO** quando você é feito.
4. O clique **adiciona** sob os filtros do ID de mensagem se as mensagens adicionais são exigidas. Neste caso, você precisa de pôr nas mensagens com ID 611101-611323.
5. Põe na escala ID na caixa dos ID de mensagem e clique a **APROVAÇÃO**.

6. Vá para trás ao menu de **registro dos filtros** e escolha o **console** como o destino.
7. Escolha **my_critical_messages da** lista de drop-down da **lista do evento do uso**. Clique a **APROVAÇÃO** quando você é feito.
8. O clique **aplica-se** depois que você retorna ao indicador de registro dos filtros.

Isto termina as configurações ASDM com o uso de uma lista da mensagem segundo as indicações do exemplo 2.

Use a classe de mensagem

Use a classe de mensagem a fim enviar todas as mensagens associadas com uma classe ao lugar especificado da saída. Quando você especifica um ponto inicial do nível de seriedade, você pode limitar o número de mensagens enviadas ao lugar da saída.

```
logging class message_class destination | severity_level
```

Exemplo 3

Incorpore este comando a fim enviar todas as mensagens da classe Ca com um nível de seriedade das emergências ou mais alto ao console.

```
logging class ca console emergencies
```

Configuração ASDM

Este procedimento mostra as configurações ASDM por exemplo 3 com o uso da lista da mensagem.

1. Escolha o menu de **registro dos filtros** e escolha o **console** como o destino.
2. Clique o **desabilitação que registra de todas as classes de evento**.
3. Sob os Syslog das classes de evento específicas, escolha a classe de evento e a severidade que você quer adicionar.Este procedimento usa o **Ca** e as **emergências** respectivamente.
4. O clique **adiciona** a fim adicionar isto na classe de mensagem e clicar a **APROVAÇÃO**.
5. O clique **aplica-se** depois que você retorna ao indicador de registro dos filtros. O console recolhe agora a mensagem da classe Ca com emergências do nível de seriedade como mostrado no indicador de registro dos filtros.

Isto termina a configuração ASDM por exemplo 3. Refira as mensagens alistadas pelo nível de seriedade para uma lista dos níveis de seriedade do mensagem de registro.

Envie debugam mensagens de registro a um servidor de SYSLOG

Para o Troubleshooting avançado, o específico da característica/protocolo debuga logs é exigido. À revelia, estes mensagens de registro são indicados no terminal (SSH/Telnet). O dependente no tipo de debuga, e a taxa de debuga as mensagens geradas, uso do CLI pôde provar que difícil se debuga estão permitidos. Opcionalmente, debugar mensagens pode ser reorientado ao processo de SYSLOG e ser gerado como Syslog. Estes Syslog podem ser enviados a todo o destino do Syslog como qualquer outro Syslog. A fim desviar debuga aos Syslog, incorporam o comando de **registro do debugar-traço**. Esta configuração envia o resultado do debug, como Syslog, a um

servidor de SYSLOG.

```
logging trap debugging
logging debug-trace
logging host inside 172.22.1.5
```

Uso da lista e das classes de mensagem de registro junto

Inscreva o **comando list de registro** a fim capturar o Syslog para o LAN para LAN e as mensagens do IPSec VPN do Acesso remoto apenas. Este exemplo captura todos os mensagens de Log de sistema da classe VPN (IKE e IPsec) com nível de debug ou mais altamente.

Exemplo

```
hostname(config)#logging enable
hostname(config)#logging timestamp
hostname(config)#logging list my-list level debugging class vpn
hostname(config)#logging trap my-list
hostname(config)#logging host inside 192.168.1.1
```

Batidas do log ACL

Adicionar o *log a* cada elemento da lista de acessos (ACE) que você deseja a fim registrar quando uma lista de acessos é batida. Use esta sintaxe:

```
access-list id {deny | permit protocol} {source_addr source_mask}
{destination_addr destination_mask} {operator port} {log}
```

Exemplo

```
ASAfirewall(config)#access-list 101 line 1 extended permit icmp any any log
```

Os ACL, à revelia, registram cada pacote negado. Não há nenhuma necessidade de adicionar a opção do log **para negar** ACL para gerar Syslog para pacotes negados. Quando a opção do *log* é especificada, gerencie o mensagem do syslog `106100` para o ACE a que é aplicado. O mensagem do syslog `106100` é gerado para cada fluxo de harmonização do permit or deny ACE que passa com o Firewall ASA. O fluxo do primeiro-fósforo é posto em esconderijo. Os fósforos subsequentes incrementam a contagem da batida indicada no **comando show access-list**. O comportamento de registro da lista de acessos do padrão, que é a palavra-chave do *log* não especificada, é que se um pacote é negado, a seguir a mensagem `106023` é gerado, e se um pacote é permitido, a seguir nenhum mensagem do syslog é gerado.

Um nível opcional do Syslog (0 - 7) pode ser especificado para os mensagens do syslog gerados (`106100`). Se nenhum nível é especificado, o nível padrão é 6 (informativo) para um ACE novo. Se o ACE já existe, a seguir seu nível atual do log permanece inalterado. Se a opção do *desabilitação do log* é especificada, o registro da lista de acessos está desabilitado completamente. Nenhum mensagem do syslog, incluindo a mensagem `106023`, é gerado. A opção padrão do *log* restaura o comportamento de registro da lista de acessos do padrão.

Termine estas etapas a fim permitir o mensagem do syslog `106100` de ver nas saídas do console:

1. Inscreva o **comando logging enable** a fim permitir a transmissão dos mensagens de Log de sistema a todos os lugar da saída. Você deve ajustar um lugar das saídas de registro a fim ver todos os logs.
2. Incorpore o comando do *<severity_level> do* **nível do** *<message_number> do* **mensagem de**

registro a fim ajustar o nível de seriedade de um mensagem de Log de sistema específico.Neste caso, incorpore o comando do **mensagem de registro 106100** a fim permitir a mensagem `106100`.

3. Entre no **message_list do console de registro |** comando do **severity_level** a fim permitir mensagens de Log de sistema de indicar no console da ferramenta de segurança (tty) como ocorrem. Ajuste o `severity_level de` 1 a 7 ou use o nome nivelado. Você pode igualmente especificar que mensagens são enviadas com a variável do `message_list`.
4. Incorpore o comando do **mensagem de registro da mostra** a fim indicar uma lista de mensagens do mensagem de Log de sistema que foram alteradas da configuração padrão, que são as mensagens que foram atribuídas um nível de seriedade diferente e as mensagens que fossem desabilitados.Este é exemplo de saída do comando do **mensagem de registro da mostra**:
```
ASAfirewall#show logging message 106100
syslog 106100: default-level informational (enabled)
ASAfirewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106
100
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Se você quer suprimir um mensagem do syslog específico a ser enviado ao servidor de SYSLOG, a seguir você deve incorporar o comando como mostrado.

```
hostname(config)#no logging message <syslog_id>
```
Refira o comando do mensagem de registro para mais informação.

%ASA-3-201008: Recusando novas conexões

`O %ASA-3-201008: Recusando novas conexões.` o Mensagem de Erro está considerado quando um ASA é incapaz de contactar o servidor de SYSLOG e nenhuma nova conexão está permitida.

Solução

Esta mensagem aparece quando você permitiu a Mensagem do log de sistema TCP e o servidor de SYSLOG não pode ser alcançado, ou quando você usa o servidor de SYSLOG de Cisco ASA (PFSS) e o disco no sistema do Windows NT está completo. Termine estas etapas a fim resolver este Mensagem de Erro:

- Desabilite a Mensagem do log de sistema TCP se é permitida.
- Se você usa o PFSS, livre acima o espaço no sistema do Windows NT onde o PFSS reside.
- Assegure-se de que o servidor de SYSLOG esteja ascendente e você pode sibilar o host do console de Cisco ASA.
- Reinicie a ordem de abertura da mensagem de sistema TCP para permitir o tráfego.

Se o servidor de SYSLOG vai para baixo e o registro TCP está configurado, use o comando de

registro da licença-hostdown ou comute-o ao registro UDP.

Informações Relacionadas

- Software de firewall de Cisco ASA
- Referências do comando Cisco Secure PIX Firewall
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems