

# ASA 8.2: Configurar o Syslog usando o ASDM

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configuração básica do Syslog usando o ASDM](#)

[Permita o registro](#)

[Desabilite o registro](#)

[Registro a um email](#)

[Registro a um servidor de SYSLOG](#)

[Configuração avançada do Syslog usando o ASDM](#)

[Trabalho com lista do evento](#)

[Trabalho com filtros de registro](#)

[Limite de taxa](#)

[Registrando as batidas de uma regra do acesso](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Problema: Conexão perdida -- Conexão do Syslog terminada --](#)

[Solução](#)

[Não pode ver o tempo real entra Cisco ASDM](#)

[Solução](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento fornece a informação em como configurar o Syslog na ferramenta de segurança adaptável de Cisco (ASA) 8.x usando o Security Device Manager adaptável (ASDM) GUI. Os mensagens de Log de sistema são as mensagens geradas por Cisco ASA para notificar o administrador em toda a mudança na configuração, em mudanças na instalação de rede, ou em mudanças no desempenho do dispositivo. Analisando os mensagens de Log de sistema, um administrador pode facilmente pesquisar defeitos o erro executando uma análise da causa raiz.

Os mensagens do syslog são diferenciados principalmente baseados em seu nível de seriedade.

1. Severidade 0 - Mensagens de emergência - O recurso é inusável
2. Severidade 1 - Mensagens de alerta - A ação imediata é precisada
3. Severidade 2 - Mensagens crítica - Condições crítica

4. Severidade 3 - Mensagens de Erro - Condições de erro
  5. Severidade 4 - Mensagens de advertência - Condições de advertência
  6. Severidade 5 - Mensagens de notificação - Normal mas condições significativas
  7. Severidade 6 - Mensagens informativa - Mensagens informativa somente
  8. Severidade 7 - Mensagens de debugging - Mensagens de debugging somente
- Nota:** O nível de seriedade o mais alto é uma emergência e o mais baixo nível de seriedade está debugando.

Os mensagens do syslog da amostra gerados por Cisco ASA são mostrados aqui:

- %ASA-6-106012: Negue o IP de IP\_address a IP\_address, opções IP encantam.
- %ASA-3-211001: Erro de alocação de memória
- %ASA-5-335003: ACL padrão NAC aplicado, ACL: ACL-nome - host address

O valor numérico X especificado em "%ASA-X-YYYYYY: ", denota a severidade da mensagem. Por exemplo, "%ASA-6-106012" é um mensagem informativa e "%ASA-5-335003" é um Mensagem de Erro.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

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

- Versão ASA 8.2 de Cisco
- Versão ASDM Cisco 6.2

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.

### Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## Configuração básica do Syslog usando o ASDM

### Permita o registro

Conclua estes passos:

1. Escolha a *configuração > o Gerenciamento de dispositivos > instalação* e marca de verificação de *registro > de registro a opção de registro da possibilidade*.
2. Você pode registrar os mensagens do syslog a um buffer interno especificando o tamanho

de buffer. Você pode igualmente escolher salvar os índices do buffer à memória Flash clicando *configura o uso instantâneo* e a definição dos ajustes instantâneos.

3. Os mensagens de Buffered Log podem ser enviados a um servidor FTP antes que estado overwritten. Clique *configuram ajustes FTP* e especificam os detalhes do servidor FTP como mostrado aqui:

## Desabilite o registro

Você pode desabilitar o Syslog específico ID baseado em sua exigência.

**Nota:** Selecionando a marca de verificação para o *timestamp incluir na opção dos Syslog*, você pode adicionar a data e hora que estiveram gerados como um campo aos Syslog.

1. Selecione os Syslog para desabilitar e o clique *edita*.
2. Da janela de configuração do Syslog ID da edição, da marca de verificação a opção das mensagens do desabilitação e da APROVAÇÃO do clique.
3. Os Syslog deficientes podem ser vistos em uma aba separada selecionando o Syslog desabilitado ID do menu suspenso da instalação do Syslog ID.

## Registro a um email

Termine estas etapas usando o ASDM a fim enviar os Syslog a um email:

1. Escolha a *configuração > o Gerenciamento de dispositivos > registrando > instalação do email*. O campo do *endereço email da fonte* é útil em atribuir um email ID como a fonte para os Syslog. Especifique o endereço email da fonte. Agora, o clique *adiciona* para adicionar os receptores do email.
2. Especifique o *endereço email do destino* e escolha o *nível de seriedade*. Baseado nos níveis de seriedade, você pode definir receptores diferentes do email. Clique a APROVAÇÃO para retornar de volta à placa da *instalação do email*. Isto conduz a esta configuração:
3. Escolha a *configuração > a instalação de dispositivo > registrando > SMTP* e especifique o servidor SMTP.

## Registro a um servidor de SYSLOG

Você pode enviar todos os mensagens do syslog a um servidor de SYSLOG dedicado. Execute estas etapas usando o ASDM:

1. Escolha a *configuração > o Gerenciamento de dispositivos > registrando > servidores de SYSLOG* e o clique *adiciona* para adicionar um servidor de SYSLOG. O indicador do *servidor de SYSLOG adicionar* aparece.
2. Especifique a relação que o server está associado com junto com o endereço IP de Um ou Mais Servidores Cisco ICM NT. Especifique o *protocolo* e os *detalhes de porta* segundo sua instalação de rede. Então, APROVAÇÃO do clique. **Nota:** Certifique-se de que você tem a alcançabilidade ao servidor de SYSLOG de Cisco ASA.
3. O servidor de SYSLOG configurado é visto como mostrado aqui. As alterações podem ser feitas quando você seleciona este server, a seguir clicam *editam*. **Nota:** Marca de verificação o *tráfego de usuário reservar a passar quando o servidor de SYSLOG TCP for abaixo da*

opção. Se não, as sessões de novo usuário são negadas com o ASA. Isto é aplicável somente quando o protocolo de transporte entre o ASA e o servidor de SYSLOG é TCP. À revelia, as sessões novas do acesso de rede estão negadas por Cisco ASA quando um servidor de SYSLOG está para baixo por qualquer razão. A fim de definir o tipo de mensagens do syslog que devem ser enviadas ao servidor de SYSLOG, veja a seção de [registro do filtro](#).

## Configuração avançada do Syslog usando o ASDM

### Trabalho com lista do evento

As listas do evento permitem-nos de criar as listas personalizadas que contêm o grupo de mensagens do syslog que devem ser enviadas a um destino. As listas do evento podem ser criadas em três maneiras diferentes:

- ID de mensagem ou escala dos ID de mensagem
- Gravidade da mensagem
- Classe de mensagem

#### **ID de mensagem ou escala dos ID de mensagem**

Execute estas etapas:

1. Escolha a *configuração > o Gerenciamento de dispositivos > registrando > lista do evento* e clique *adiciona* para criar uma lista nova do evento.
2. Especifique um nome no *campo de nome*. O clique *adiciona na placa dos filtros do ID de mensagem* para criar uma lista nova do evento.
3. Especifique a escala do mensagem do syslog ID. Aqui os mensagens do syslog TCP tomaram por exemplo. **APROVAÇÃO** do clique a terminar.
4. **A APROVAÇÃO** do clique outra vez a fim reverter de volta ao *evento alista* o indicador.

#### **Gravidade da mensagem**

1. As listas do evento podem igualmente ser definidas com base na gravidade da mensagem. O clique *adiciona* para criar uma lista separada do evento.
2. Especifique o nome e o clique *adiciona*.
3. Selecione o nível de seriedade como *erros*.
4. Clique em OK.

#### **Classe de mensagem**

As listas do evento são configuradas igualmente com base na classe de mensagem. Uma classe de mensagem é um grupo de mensagens do syslog relativos a uma característica da ferramenta de segurança que o permita de especificar uma classe inteira de mensagens em vez de especificar uma classe para cada mensagem individualmente. Por exemplo, use a classe do AUTH para selecionar todos os mensagens do syslog que são relacionados à autenticação de usuário. Algumas classes de mensagens disponíveis são mostradas aqui:

- Tudo — Todas as classes de evento
- AUTH — Autenticação de usuário
- ponte — Firewall transparente
- Ca — Autoridade de certificação PKI

- relação do comando config
- ha — Failover
- IP — Serviço de proteção contra intrusão
- IP — Pilha de IP
- NP — Processador de rede
- OSPF — Roteamento OSPF
- rasgo — Roteamento do RASGO
- sessão — Sessão do usuário

Execute estas etapas para criar uma classe de evento baseada na classe de mensagem dos `vpnclient-erros`. A classe de mensagem, `vpnc`, está disponível para categorizar todos os mensagens do syslog relativos ao `vpnclient`. O nível de seriedade para esta classe de mensagem é escolhido como “erros”.

1. O clique adiciona para criar uma lista nova do evento.
2. Especifique o nome para ser relevante à classe de mensagem que você cria e o clique *adiciona*.
3. Selecione o `vpnc` da lista de drop-down.
4. Selecione o nível de seriedade como `erros`. Este nível de seriedade é aplicável para aquelas mensagens que são registradas para esta classe de mensagem somente. Clique a **APROVAÇÃO** para reverter de volta ao indicador da lista do evento adicionar.
5. A classe de evento/severidade é mostrada aqui. Clique a **APROVAÇÃO** para terminar configurar a lista do evento dos “`vpnclient-erros`”. Igualmente mostra-se no tiro de tela seguinte que uma lista nova do evento, o “`USER-AUTH-Syslog`”, é criado com uma classe de mensagem como o “`AUTH`” e no nível de seriedade para os Syslog desta classe de mensagem específica como “`avisos`”. Configurando isto, a lista do evento especifica todos os mensagens do syslog que são relacionados à classe de mensagem do “`AUTH`”, com níveis de seriedade **até** o nível dos “`avisos`”. **Nota:** Aqui, o termo “até” é do significado. Ao denotar o nível de seriedade, mantenha na mente que todos os mensagens do syslog estarão registrados até que esse nível. **Nota:** Uma lista do evento pode conter classes de evento múltiplo. A lista do evento dos “`vpnclient-erros`” é alterada clicando **edita** e definindo uma classe de evento nova “`SSL/erro`”.

## Trabalho com filtros de registro

Os filtros de registro são usados para enviar os mensagens do syslog a um destino especificado. Estes mensagens do syslog podem ser baseados na “`severidade`” ou “`alista mesmo`”.

Estes são os tipos de destinos a que estes filtros são aplicáveis:

- Buffer interno
- Armadilha de SNMP
- E-mail
- Console
- Sessões de Telnet
- ASDM
- Servidores de SYSLOG

Execute estas etapas:

1. Escolha a **configuração > o Gerenciamento de dispositivos > filtros de registro > de registro** e selecione o destino de registro. Então, o clique **edita** para alterar os ajustes.
2. Você pode enviar os mensagens do syslog baseados na severidade. Aqui, as **emergências** foram selecionadas para mostrar como um exemplo.
3. Uma lista do evento pode igualmente ser selecionada especificar que tipo de mensagem deve ser enviada a um destino particular. Clique em **OK**.
4. Verifique a alteração.

Estas são as etapas em como enviar um grupo de mensagens (baseadas em seu nível de seriedade) ao server do email.

1. Selecione o **email** no campo de destino de registro. Então, o clique **edita**.
2. Escolha o **filtro na** opção da **severidade** e selecione o nível de seriedade exigido. Aqui, os **alertas** foram selecionados como o nível de seriedade. Você pode ver que todos os mensagens do syslog alertas devem ser enviada ao email configurado.

## Limite de taxa

Isto especifica o número de mensagens do syslog que Cisco ASA envia a um destino em um período especificado. É definido geralmente para o nível de seriedade.

1. Escolha a **configuração > o Gerenciamento de dispositivos > registrando > limite de taxa** e selecione o nível de seriedade exigido. Então, o clique **edita**.
2. Especifique o número de mensagens a ser enviadas junto com o intervalo de tempo. Clique em **OK**. **Nota:** Estes números são dados como um exemplo. Estes diferem segundo o ambiente do tipo de rede. Os valores alterados são considerados aqui:

## Registrando as batidas de uma regra do acesso

Você pode registrar as batidas da regra do acesso usando o ASDM. O comportamento de registro do padrão é enviar um mensagem do syslog para todos os pacotes negados. Não haverá nenhum mensagem do syslog para os pacotes permitidos e estes não serão registrados. Contudo, você pode definir um nível de seriedade de registro feito sob encomenda à regra do acesso para seguir a contagem dos pacotes que bate esta regra do acesso.

Execute estas etapas:

1. Selecione a regra exigida do acesso e o clique *edita*. A *edição* o indicador da *regra do acesso* aparece. **Nota:** Nesta imagem, a *opção padrão* no campo do *nível de registro* indica o comportamento de registro do padrão de Cisco ASA. Para obter mais informações sobre disto, refira a seção de [registro da atividade da lista de acessos](#).
2. A marca de verificação a *opção de registro da possibilidade* e especifica o nível de seriedade exigido. Então, **APROVAÇÃO** do clique. **Nota:** Clicando *mais* aba da gota-para baixo das *opções*, você pode ver a opção de *registro do intervalo*. Esta opção é destacada somente quando o acima *permitem a opção de registro* são tiquetaqueados. O valor padrão deste temporizador é 300 segundos. Este ajuste é útil em especificar o valor de intervalo para que as fluxo-estatísticas sejam suprimidas quando não há nenhum fósforo para essa regra do acesso. Se há alguma batida, a seguir o ASA espera até o tempo de intervalo de registro e envia aquele ao Syslog.
3. As alterações são mostradas aqui. Alternativamente, você pode fazer duplo clique o campo

de *registro da* regra específica do acesso e ajustar o nível de seriedade lá. **Nota:** Este método alternativo de especificar o *nível de registro na* mesma placa das *regras do acesso* fazendo duplo clique trabalha para somente entradas manualmente criadas da regra do acesso, mas não às regras implícitas.

## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Use a [Command Lookup Tool \(somente clientes registrados\)](#) para obter mais informações sobre os comandos usados nesta seção.

## Configurações

Este documento utiliza as seguintes configurações:

```
CiscoASA
: Saved
:
ASA Version 8.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.0
!
interface Ethernet0/2
 nameif inside
 security-level 100
 ip address 10.78.177.11 255.255.255.192
!
!!--- Output Suppressed ! access-list inside_access_in
extended permit ip host 10.10.10.10 host 20.20.20.200
log errors access-list inside_access_in extended permit
ip host 10.10.10.20 any access-list inside_access_in
extended deny ip 10.20.10.0 255.255.255.0 host
20.20.20.200 access-list inside_access_in extended
permit ip 10.78.177.0 255.255.255.192 any log
emergencies pager lines 24 logging enable logging list
user-auth-syslog level warnings class auth logging list
TCP-conn-syslog message 302013-302018 logging list
syslog-sev-error level errors logging list vpnclient-
errors level errors class vpnc logging list vpnclient-
errors level errors class ssl logging buffered user-
auth-syslog logging mail alerts logging from-address
```

```
test123@example.com logging recipient-address
monitorsyslog@example.com level errors logging queue
1024 logging host inside 172.16.11.100 logging ftp-
bufferwrap logging ftp-server 172.16.18.10 syslog
testuser **** logging permit-hostdown no logging message
302015 no logging message 302016 logging rate-limit 600
86400 level 7 mtu outside 1500 mtu inside 1500 icmp
unreachable rate-limit 1 burst-size 1 asdm image
disk0:/asdm-623.bin asdm history enable arp timeout
14400 ! !--- Output Suppressed ! timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout sip-provisional-media 0:02:00
uauth 0:05:00 absolute timeout TCP-proxy-reassembly
0:01:00 dynamic-access-policy-record DfltAccessPolicy !
!--- Output Suppressed ! telnet timeout 5 ssh timeout
5 console timeout 0 threat-detection basic-threat
threat-detection statistics access-list no threat-
detection statistics TCP-intercept ! !--- Output
Suppressed ! username test password /FzQ9W6s1KjC0YQ7
encrypted privilege 15 ! ! class-map inspection_default
match default-inspection-traffic ! ! policy-map type
inspect dns preset_dns_map parameters message-length
maximum 512 policy-map global_policy class
inspection_default inspect dns preset_dns_map inspect
ftp inspect h323 h225 inspect h323 ras inspect netbios
inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip
inspect xdmcp ! service-policy global_policy global
smtp-server 172.18.10.20 prompt hostname context
Cryptochecksum:ad941fe5a2bbea3d477c03521e931cf4 : end
```

## [Verificar](#)

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- Você pode ver os Syslog do ASDM. Escolha a **monitoração > registrando > Log Viewer do tempo real**. Uma saída de exemplo é mostrada aqui:

## [Troubleshooting](#)

### [Problema: Conexão perdida -- Conexão do Syslog terminada --](#)

Este erro é recebido ao tentar permitir o ASDM que registra no painel do dispositivo para alguns dos contextos.

"Conexão perdida -- Conexão do Syslog terminada --"

Quando o ASDM estiver usado para conectar diretamente ao contexto admin e registro ASDM estiver desabilitado lá, a seguir interruptor a um subcontext e para permitir o registro ASDM. Os erros são recebidos, mas os mensagens do syslog estão alcançando muito bem ao servidor de



SYSLOG.

## Solução

Este é um comportamento conhecido com Cisco ASDM e documentou na identificação de bug Cisco [CSCsd10699](#) ([clientes registrados somente](#)). Como uma ação alternativa, permita o asdm que registra quando registrado no contexto admin.

## Não pode ver o tempo real entra Cisco ASDM

Uma edição é que os logs do tempo real não podem ser vistos no ASDM. Como isto é configurado?

## Solução

Configurar o seguinte em Cisco ASA:

```
ciscoasa(config)#logging monitor 6 ciscoasa(config)#terminal monitor ciscoasa(config)#logging on  
ciscoasa(config)#logging trap 6
```

## Informações Relacionadas

- [Apoio do Dispositivos de segurança adaptáveis Cisco ASA série 5500](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)