Rastreador de Pacotes - Registro de Várias Origens

# Objetivos

**Parte 1: Usar syslog para capturar arquivos de log de vários dispositivos de rede**

**Parte 2: Observe o registro de acesso do usuário AAA**

**Parte 3: Observar as informações do NetFlow**

# Histórico/Cenário

Nesta atividade, você usará o Rastreador de Pacotes para exibir dados de rede gerados pelo syslog, AAA e NetFlow.

# Instruções

## Exibir Entradas de Log com Syslog

### O servidor syslog

O Syslog é um sistema de mensagens projetado para suportar o registro remoto. Os clientes Syslog enviam entradas de log para um servidor syslog. O servidor syslog concentra e armazena entradas de log. O Packet Tracer suporta operações básicas de syslog e pode ser usado para demonstração. A rede inclui um servidor syslog e clientes syslog. R1, R2, Core Switch e o Firewall são clientes syslog. Esses dispositivos são configurados para enviar suas entradas de log para o servidor syslog. O servidor syslog coleta as entradas de log e permite que elas sejam lidas.

As entradas de log são categorizadas por sete níveis de gravidade. Níveis mais baixos representam eventos mais graves. Os níveis são: emergências (0), alertas (1), críticos (2), erros (3), avisos (4), notificações (5), informativos (6) e depuração (7). Os clientes Syslog podem ser configurados para enviar entradas de log para servidores syslog com base no nível de gravidade.

* + - 1. Clique no **servidor Syslog** para abrir sua janela.
      2. Selecione a guia **Serviços** e selecione **SYSLOG** na lista de serviços mostrada à esquerda.
      3. Clique em **On** para ativar o serviço Syslog.
      4. Entradas de syslog provenientes de clientes syslog serão mostradas na janela à direita. Atualmente, não há entradas.
      5. Mantenha esta janela aberta e visível e passe para a **Etapa 2**.

### Ativar o Syslog.

Os dispositivos já estão configurados para enviar mensagens de log para o servidor syslog, mas o Rastreador de Pacotes suporta somente o log para o nível de gravidade de depuração com syslog. Devido a isso, devemos gerar mensagens de nível de depuração (nível 7) para que possam ser enviadas para o servidor syslog.

* + - 1. Clique em **R1> guia CLI.**
      2. Pressione Enter para obter um prompt de comando e digite o comando **enable**.
      3. Insira o comando **debug eigrp packets** para habilitar a depuração do EIGRP. O console de linha de comando irá preencher imediatamente com mensagens de depuração.
      4. Retorne à janela **Servidor Syslog**. Verifique se as entradas de log aparecem no servidor syslog.
      5. Depois que algumas mensagens forem registradas, clique no botão de opção para **desligar** o serviço syslog.

#### Pergunta:

Quais são algumas das informações incluídas nas mensagens do syslog que estão sendo exibidas pelo Servidor Syslog?

Digite suas respostas aqui.

* + - 1. Feche a janela do dispositivo R1.

## Log de Acesso de Usuário

Outro tipo importante de log está relacionado ao acesso do usuário. Ter registros de logins de usuários é crucial para solução de problemas e análise de tráfego. O Cisco IOS suporta autenticação, autorização e contabilidade (AAA). Com o AAA, é possível não apenas delegar a tarefa de validação do usuário a um servidor externo, mas também registrar atividades.

TACACS+ é um protocolo projetado para permitir autenticação remota através de um servidor centralizado.

O Packet Tracer oferece suporte básico AAA e TACACS+. R2 também é configurado como um servidor TACACS+. R2 perguntará ao servidor se esse usuário é válido verificando nome de usuário e senha, e concederá ou negará acesso com base na resposta. O servidor armazena as credenciais do usuário e também é capaz de registrar transações de login do usuário. Siga as etapas abaixo para fazer login no R2 e exibir as entradas de log relacionadas a esse login:

* + - 1. Clique no **servidor Syslog** para abrir sua janela.
      2. Selecione a guia **Área de trabalho** e selecione **Contabilidade AAA**. Deixe essa janela aberta.
      3. Clique em **R2 > CLI**.
      4. Pressione Enter para obter um prompt de comando. **R2** pedirá nome de usuário e senha antes de conceder acesso à CLI. Insira as seguintes credenciais de usuário: **analista** e **cyberops** como nome de usuário e senha, respectivamente.
      5. Retorne à janela Registros de Contabilidade AAA do Servidor Syslog.

#### Pergunta:

Quais informações estão na entrada de log?

Digite suas respostas aqui.

* + - 1. Em R2, digite o comando **logout**.

#### Pergunta:

O que aconteceu na janela de contabilidade da AAA?

Digite suas respostas aqui.

## NetFlow e Visualização

Na topologia, o servidor Syslog também é um coletor NetFlow. O firewall é configurado como um exportador NetFlow.

* + - 1. Clique no **Servidor Syslog** para abrir sua janela. Feche a janela Registros Contábeis AAA.
      2. Na guia **Área de Trabalho** , selecione **Coletor de Fluxo de Rede**. Os serviços de coletor NetFlow devem ser ativados.
      3. De qualquer PC, execute ping no Corp Web Server em 209.165.200.194. Após um breve atraso, o gráfico de pizza será atualizado para mostrar o novo fluxo de tráfego.

**Observação**: os gráficos de pizza exibidos variam de acordo com o tráfego na rede. Outros fluxos de pacotes, como tráfego relacionado ao EIGRP, estão sendo enviados entre dispositivos. O NetFlow está capturando esses pacotes e exportando estatísticas para o NetFlow Collector. Quanto mais tempo o NetFlow tiver permissão para ser executado em uma rede, mais estatísticas de tráfego serão capturadas.

# Reflexão

Embora as ferramentas apresentadas nesta atividade sejam úteis, cada uma tem seu próprio serviço e pode precisar rodar em dispositivos totalmente diferentes. Uma maneira melhor, explorada mais tarde no curso, é que todas as informações de registro sejam concentradas em uma única ferramenta, permitindo fácil referência cruzada e recursos poderosos de pesquisa. As plataformas SIEM (Security Information and Event Management, gerenciamento de eventos e informações de segurança) podem coletar arquivos de log e outras informações de diversas fontes e integrar as informações para acesso por uma única ferramenta.

Fim do documento