

Conceitos básicos

Última revisão feita em 30 de Junho de 2007.

Para entender melhor a ferramenta Network Monitor separei seis itens básicos conceituando suas características. Acompanhe:

As duas versões do Network Monitor

A versão fornecida junto com o Windows 2003 (também com o NT e 2000) é uma versão básica, também conhecida com Lite, se comparada com a versão completa, conhecida como Full, que acompanha o Microsoft Systems Management Server (SMS).

Filtro de Captura (Capture Filter)

Com esta função você filtra em tempo real os frames que serão capturados durante o monitoramento do tráfego de rede. Uma vez configurada você poderá definir os protocolos a serem filtrados (SAP/ETYPE), o par de endereços para o monitoramento (Address Pairs) ou ainda por algum padrão encontrado nos frames (Pattern Matches).

Filtro de Exibição (Display Filter)

Este filtro é aplicado aos frames já capturados pelo Netmon, ou seja, servem para organizar os dados exibidos pela ferramenta. Você poderá filtrar os dados apresentados com base nos protocolos utilizados, uma propriedade específica de algum protocolo ou ainda por endereço IP de algum computador.

Trigger de Captura (Capture Trigger)

Uma função que servirá para que uma captura inicie ou termine a partir de um critério como quando o buffer chegar a um limite pré-definido, ou algum frame apresentar uma seqüência ASCII ou hexadecimal específica, ou ainda combinando estes dois critérios. Obedecendo ao critério definido por você o Trigger irá executar uma ação que pode ser a execução de algum programa ou linha de comando.

Buffer de Captura (Capture Buffer)

O Buffer armazena temporariamente os frames coletados durante um processo de captura. Por padrão o tamanho deste arquivo de buffer é de 1mb, porem pode ser aumentado. Este armazenamento funciona de uma forma circular, baseado no método FIFO (first in, first out).

Modo de Captura Dedicada (Dedicated Capture Mode)

Este é um modo de captura diferenciado para ser utilizado em casos específicos, como quando o computador com o Netmon instalado está com falta de recursos ou ainda quando a captura está gerando muitos frames. As estatísticas não são apresentadas em tempo real durante o processo para liberar mais recursos para a captura.

Bibliografia

Referências utilizadas na elaboração deste artigo:

1. Microsoft Brasil. www.microsoft.com.br
2. TechNet Brasil. www.technetbrasil.com.br

Escreveu,

Cleber Marques

contato@clebermarques.com

Sábado, 30 de Junho de 2007.