Dispositivo Cisco NAC (Clean Access) 4.x: Configurar os ajustes do Syslog para o registro dos eventos

Índice

Introdução

Este documento descreve como configurar os ajustes do Syslog a fim registrar os eventos a um servidor interno no dispositivo do Cisco Network Admission Control (NAC), conhecido anteriormente como o acesso limpo de Cisco (CA).

Pré-requisitos

Requisitos

Este documento supõe que o Access Manager limpo de Cisco (CAM) e os servidores de acesso limpos de Cisco (CAS) estão instalados e trabalham corretamente.

Componentes Utilizados

A informação neste documento é baseada na ferramenta NAC de Cisco que executa a versão de software 4.0 e mais atrasado.

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.

Interpretando log de eventos

Clique os **log de eventos** ligam no módulo da **monitoração** a fim ver o evento Syslog-baseado entra o console admin. Há três abas dos log de eventos:

- **Logs da vista**
- **Ajustes dos logs**
- **Ajustes do Syslog**

Logs da vista

Figura 1
A aba dos logs da vista inclui esta informação:

- Estatística de sistema para os servidores de acesso limpos, que são gerados cada hora à revelia.
- Atividade do usuário, com tempos do fazer logon do usuário, tempos do fazer logoff, tentativas falhadas do fazer logon, e mais.
- Eventos da configuração de rede, que incluem mudanças as lista ao Media Access Control (MAC) ou da transmissão IP, e adição ou remoção de servidores de acesso limpos.
- Eventos do gerenciamento de switch para fora da banda (OOB), que incluem quando as armadilhas de linkdown estiverem recebidas, e quando uma porta mudar ao AUTH ou ao LAN virtual (VLAN) do acesso.
- Mudanças ou atualizações às verificações de acesso limpas, às regras, e ao AntiVirus/à lista apoiados produto de AntiSpyware.
- Mudanças à configuração limpa do protocolo de configuração dinâmica host (DHCP) do servidor de acesso.

A estatística de sistema é gerada para cada CAS controlado pelo Access Manager limpo cada hora à revelia. Veja configurar a ordem de abertura do Syslog para mudar como frequentemente as verificações de sistema ocorrem.

Note: A maioria de acontecimentos recentes aparecem primeiramente na coluna dos eventos.

A tabela 1 descreve a navegação, as capacidades da busca, e o Syslog real indicado em logs da vista.

Tabela 1

	Coluna	Descrição
Navegação	**Primeiramente/ precedente/em seguida/último**	Página destes links da navegação através do log de eventos. A maioria de acontecimentos recentes aparecem primeiramente na

		coluna dos eventos. **O último** link mostra-lhe os eventos os mais velhos no log. Um máximo de 25 entradas é indicado em uma página.
	Coluna	Clique uma coluna acima, tal como o tipo ou a categoria, a fim classificar o log de eventos por essa coluna.
Critérios de pesquisa	Tipo	Procure por estes o tipo critérios da coluna, e clique então a **vista**: • Algum tipo • Falha • Informações • Sucesso
	Categoria	A busca por estes critérios da coluna da categoria, e clica então a **vista**: • Autenticação [1] • Administração • Cliente • Clean Access Server • Limpe o acesso • SW_Management, se OOB é permitido • Diversos • DHCP
	Tempo	Procure por estes critérios do tempo, e clique então a **vista**: • Dentro de uma hora • Dentro de um dia • No prazo de dois dias • Dentro de uma semana • Quando • Uma hora há • Um dia há • Dois dias há • Uma semana há
	Busca no texto do log	Datilografe o texto desejado da busca e clique a **vista**.
Controles	**Vista**	Depois que os critérios de pesquisa desejados são escolhidos, clique a **vista** a fim indicar os resultados.
	Restaure a vista	Se você clica a **opinião da restauração**, restaura o visualização padrão, em que os logs dentro de um dia são indicados.

	Supressão	Se você clica a **supressão**, remove os eventos filtrados com os critérios de pesquisa através do número de páginas aplicáveis. A supressão remove os eventos filtrados do armazenamento limpo do Access Manager. Se não, o log de eventos persiste com o fechamento do sistema. Use o indicador do evento do filtro mostrado em figura 1 a fim ver o número total de eventos filtrados que são sujeitos ao supressão.
Exibição de status	Tipo	• Flag vermelho () = falha — indica um erro ou um evento de outra maneira inesperado • Bandeira verde () = sucesso — indica um evento bem sucedido ou do uso normal, tal como o login bem-sucedido e a atividade da configuração • Bandeira amarela () = informação — indica a informação do desempenho de sistema, tal como a informação de carga e a utilização de memória
	Categoria	Indica o módulo ou o componente de sistema que iniciaram o evento do log. Para uma lista, refira a **categoria** sob os critérios de pesquisa da seção. Note que, à revelia, a estatística de sistema está gerada cada hora para cada servidor de acesso limpo que é controlado pelo Access Manager limpo.
	Tempo	Indica a data e hora (HH: milímetro: ss) do evento, com a maioria de acontecimentos recentes primeiramente na lista.
	Evento	Indica o evento para o módulo, com a maioria de acontecimentos recentes alistados primeiramente. Veja a tabela 2 - A coluna do evento

		coloca para um exemplo de um evento limpo do servidor de acesso.

Notas de rodapé - Tabela 1

1 As entradas do tipo do autenticação podem incluir fornecedor do artigo ": type> do <provider, Access point: N/A, rede: N/A." a fim continuar a fornecer o apoio para o cliente Wireless do legado do fim da vida útil (EOL), se atual e PRE-configurado no gerente, "o Access point: N/A, rede: Campos N/Aos" fornecem o Access Point (AP) MAC e a informação do Service Set Identifier (SSID) respectivamente para o cliente do legado.

Exemplo do log de eventos

A tabela 2 explica o exemplo limpo típico do evento da saúde do servidor de acesso:

```
CleanAccessServer 2006-04-03 15:07:53 192.168.151.55 System Stats:
 Load factor 0 (max since reboot: 9) Mem Total: 261095424 bytes Used: 246120448
 bytes Free: 14974976 bytes Shared: 212992 bytes Buffers: 53051392 bytes Cached:
 106442752 bytes CPU User: 0% Nice: 0% System: 97% Idle: 1%
```

Tabela 2 - Campos da coluna do evento

Valor	Descrição
`CleanAccessServer`	Um servidor de acesso limpo relata o evento
`2006-04-03 15:07:53`	Data e hora do evento
`192.168.151.55`	Endereço IP de Um ou Mais Servidores Cisco ICM NT de relatar o servidor de acesso limpo
`Fator de carga 0`	O fator de carga indica o número de pacotes que esperam para ser processados pelo servidor de acesso limpo, isto é, a carga atual que é segurada por CAS. Quando o fator de carga cresce, é uma indicação que os pacotes esperem na fila a ser processada. Se o fator de carga excede 500 para qualquer período de tempo consistente, tal como cinco minutos, este indica que o servidor de acesso limpo tem uma carga elevada constante do tráfego de entrada/pacotes. Seja referido se este número aumenta a 500 ou mais alto.
`(máximo desde a repartição: <n>)`	O número máximo de pacotes na fila a qualquer altura. Ou seja a carga máxima segurada pelo servidor de acesso limpo.
`Total de Mem: 261095424 bytes`	Estas são as estatísticas da utilização de memória. Há seis números mostrados aqui: • memória total • memória usada • memória livre • memória compartilhada • memória do buffer
`Usado: 246120448 bytes`	
`Livre:`	

14974976 bytes Comparti lhado: 212992 bytes Bufferes : 53051392 bytes Posto em esconder ijo: 10644275 2 bytes	• memória posta em esconderijo
Usuário CPU: 0% Agradáve l: 0% Sistema: 97% Quietude : 1%	Estes números indicam a carga do processador de CPU no hardware, nas porcentagens. Estes quatro números indicam o tempo passado pelo sistema no usuário, agradável, no sistema, e em processos inativos. **Note**: O tempo passado pelo CPU no processo do sistema é tipicamente maior de 90 por cento em um servidor de acesso limpo. Isto indica um sistema saudável.

Limite o número de eventos registrados

O ponto inicial do log de eventos é o número de eventos a ser armazenados no base de dados limpo do Access Manager. O número máximo de eventos do log mantidos no CAM, à revelia, é 100,000. Você pode especificar um ponto inicial do log de eventos de até 200,000 entradas a ser armazenadas no base de dados CAM em um momento. O log de eventos é um log circular. As entradas as mais velhas overwritten quando o log passa o ponto inicial do log de eventos.

A fim mudar o número máximo de eventos:

1. Clique os **logs que ajustam a** aba nas páginas da **monitoração > dos log de eventos**.
2. Incorpore o número novo aos campos **máximos dos log de eventos**.
3. Clique em **Update**.

Configurar o registro do Syslog

A estatística de sistema é gerada cada hora, à revelia, para cada servidor de acesso limpo que é controlado pelo Access Manager limpo. À revelia, os log de eventos são escritos ao CAM. Você pode reorientar log de eventos CAM a um outro server, tal como seu próprio servidor de SYSLOG.

Adicionalmente, você pode configurar como frequentemente você quer o CAM registrar a informação de status de sistema. A fim fazer isto, ajuste o valor no campo do **intervalo do log da saúde do Syslog**. O padrão é **60** minutos.

A fim configurar o registro do Syslog:

1. Escolha a **monitoração > os log de eventos > os ajustes do Syslog**.
2. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de SYSLOG ao campo de **endereço de servidor de SYSLOG**. O padrão é **127.0.0.1**.
3. Inscreva a porta para o servidor de SYSLOG no campo de **porta do servidor de SYSLOG**. O padrão é **514**.
4. Entre em como frequentemente você quer o CAM registrar a informação de status de sistema, nos minutos, no campo do **intervalo do log das saúdes de sistema**. O padrão é **60** minutos. Este ajuste determina como as estatísticas de CAS são entradas frequentemente o log de eventos.
5. **Atualização do** clique a fim salvar suas mudanças.**Note**: Depois que você estabelece seu servidor de SYSLOG no CAM, você pode testar sua configuração. A fim fazer isto, termine e registre de novo no console CAM admin. Isto gerencie um evento de syslog. Se o evento CAM não é considerado em seu servidor de SYSLOG, certifique-se de que o servidor de SYSLOG recebe o User Datagram Protocol (UDP) 514 pacotes e de que não estão obstruídos em outra parte em sua rede.**Note**: Configurar servidores syslog múltiplos não é possível porque não é apoiado. Você pode somente enviar a um servidor de SYSLOG.

Arquivos de registro

O log de eventos é ficado situado na tabela de base de dados limpa do Access Manager e nomeado tabela do log_info. alista outro entra o Access Manager limpo.

Tabela 3

Arquivo	Descrição
`/var/log/messages`	Partida
`/var/log/dhcplog`	Transmissão de DHCP, logs DHCP
`/tmp/perfigo-log0.log.*`	Log de serviço do perfigo para 3.5(4) e mais cedo [1]
`/perfigo/logs/perfigo-log0.log.*`	Log de serviço do perfigo para 3.5(5) e mais tarde [1,2]
`/perfigo/logs/perfigo-redirect-log0.log.0`	erros de conexão Certificado-relacionados CAM/CAS
`/var/nessus/logs/nessusd.messages`	Logs do teste do plugin Nessus
`/perfigo/control/apache/logs/ *`	Certificados do secure sockets layer (SSL), log de erros de Apache
`/perfigo/control/tomcat/logs/localhost *.`	Tomcat, reorienta, JavaServer pagina os logs (JSP)
`/var/log/ha-log`	Alta disponibilidade dos logs para o

	CAM e o CAS

Notas de rodapé - Tabela 3

1. 0 em vez de * mostra o log o mais recente.

2. O gerenciamento de switch que os eventos para as notificações recebidas pelo CAM do Switches são escritos somente ao entra o sistema de arquivos (/perfigo/logs/perfigo-log0.log.0). Além disso, estes eventos estão escritos ao disco somente quando o nível do log é ajustado à INFORMAÇÃO ou mais fino.

Informações Relacionadas

- Página de suporte da ferramenta NAC de Cisco
- Suporte Técnico e Documentação - Cisco Systems