**GPOs de Domínio - Auditorias**

**Servidores**

[**Políticas de Segurança no AD - Parte II**](http://sistemaoperacionalserver.blogspot.com/2015/12/aula-xi-politicas-de-seguranca-no-ad_10.html)

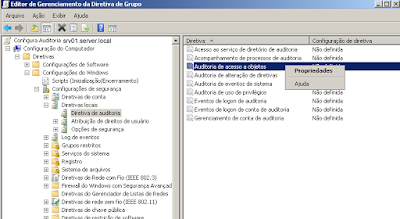
**Auditorias e Logs - Windows Server**

As auditorias são recursos de segurança responsáveis por monitorar toda e qualquer operação do usuário e do sistema. É a melhor maneira de controlar o que está acontecendo nos sistemas de rede servidor/cliente. As auditorias podem ser utilizadas para reunir informações relacionadas à utilização de recursos como acessos de arquivos, pastas ou mesmos recursos mais avançados do sistema.

Sempre que ocorre uma ação cuja a auditoria foi configurada, ela é gravada em um log específico, normalmente um de segurança. Para visualizar e gerenciar os logs de Eventos, usamos sempre o Visualizador de Eventos do server.

**Configuração das Diretivas de Auditoria**

Componente da rede servidor/cliente do Windows server, as auditorias são essenciais para garantir e elevar a segurança de uma rede baseada em domínio. Além de forçar a integridade do sistema (rede), será permitido aos administradores do domínio o controle efetivo das operações do usuário e do próprio sistema.



**Quais são as auditorias?**

**- Auditoria de eventos de logon de conta:** Controla eventos relacionados ao logon/logoff do usuário.

**- Auditoria de gerenciamento de contas:** Controla o gerenciamento de contas por intermédio do console Usuários e Computadores do AD. Eventos são gerados sempre que as contas do usuário, computador ou um grupo são criados, modificados ou excluídos. Tipo de auditoria que controla o próprio administrador de domínio, bem como power users.

**- Auditoria de acesso ao serviço de diretório:** Controla o acesso ao AD. Logs de eventos são gerados quando usuários e computadores acessam o AD.

**- Auditoria de eventos de logon:** Controla eventos relacionados ao logon/logoff e às conexões remotas do usuário em todo o sistema da rede baseada em Windows Server e AD.

**- Auditoria de acesso a objetos:** Controla a utilização de recursos da rede baseada em domínio e que sejam associadas aos arquivos, diretórios, compartilhamentos, impressoras e demais objetos do AD.

**- Auditoria de alteração de diretivas:** Controla toda e qualquer operação que os usuários administradores e power users na alteração de GPOs, permissões e restrições dos demais usuários da rede.

**- Auditoria de uso de privilégios:** Controla o uso de direitos e privilégios do usuário, como direito de fazer backup de arquivos e diretórios.

- Auditoria de controle de processos: Controla processos de sistema e todos os recursos por ele utilizados.

**- Auditoria de eventos de sistema:** Controla a inicialização, o desligamento e o reboot do sistema. Controla também toda e qualquer ação que envolva a segurança da rede baseada em AD.

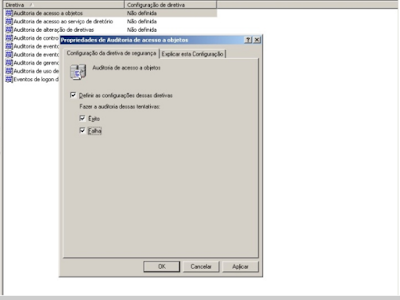
**Como as auditorias são configuradas?**

Toda a auditoria deve passar por um processo de planejamento para poder ser aplicada ao domínio, isso porque, suas configurações, de forma incorreta para determinadas situações podem prejudicar a performance da rede baseada em domínio.

As configurações são feitas de duas formas:

**- Êxito (sucesso):** registra os eventos que tiveram êxito, eventos que possuem permissão de execução, como por exemplo as tentativas de logon bem sucedidas.

**- Falha (erro):** registra os eventos que não tiveram êxito, como tentativas de acesso a uma unidade de compartilhamento na qual o usuário não possui permissão.



**Visualizando e gerenciando os Logs de eventos:**

Um Log é uma mensagem, um relatório de todas as operações de uma rede servidor/cliente baseada em um Domínio. Uma mensagem no log do sistema, possui informações tais como o usuário que executou a ação, a ação executada e se esta foi executada com sucesso ou não. O log de eventos do Windows Server 2012 pode ser configurado, de tal maneira que o Administrador escolha quais eventos devem ser gravados no log, como por exemplo:

- tentativas de logon com sucesso, tentativas de logon sem sucesso ou

ambas . Além disso, podemos definir se devem ser monitorados somente acessos bem sucedidos ou acessos negados  (sem  sucesso),  tais  como  um usuário  com  permissão  somente  de  leitura  que  tenta  alterar um determinado arquivo, em uma pasta compartilhada.

Os logs do sistema são acessados utilizando a opção:

**Visualizar Eventos em Ferramentas Administrativas ou Gerenciamento do Computador.**

Quando ocorrer algum evento relacionado com a auditoria habilitada, o Windows 2012 grava esse evento no log de segurança. Para visualizarmos esses eventos utilizamos o Visualizador de Eventos. As informações gravadas no log de segurança são as seguintes:

**- Ação executada.**

**- Usuário que executou a ação.**

**- Êxito ou falha na ação, e quando ocorreu a ação.**

**- Computador no qual a ação foi executada.**

**Existem três categorias de Logs:**

**- Log de Aplicativo:** contém erros, avisos e mensagens informativas de diversos programas que rodam no Windows Server 2012. Por exemplo, softwares desenvolvedores de Banco de Dados, gravam uma série de eventos no log Aplicativo. O log do aplicativo contém eventos registrados por aplicativos ou programas. Os desenvolvedores  de  software  decidem  quais  eventos monitorar,  isto  é,  ao  desenvolver  um  programa,  é possível definir quais eventos o programa irá gravar no log de eventos do Windows Server 2012.

**-Log de Segurança:** contém informações sobre o sucesso ou não de eventos de auditoria, de acordo com definições da política de auditoria. De acordo com o que foi configurado nas Diretivas de Auditorias, o Administrador define quais os eventos de segurança que serão monitorados. **Portanto, uma Diretiva depende da outra para que seu Domínio fique bem protegido.** O log de segurança registra eventos como tentativas de logon válidas e inválidas, assim como eventos relacionados ao uso de recursos, como criar, abrir ou excluir arquivos ou outros objetos. Um exemplo, se você ativou a auditoria de logon, as tentativas de logon no sistema serão registradas no log de segurança. Por padrão somente usuários com permissão de administrador podem acessar o log de segurança.

**-Log de Sistema:** contém erros, avisos e informações geradas pelo próprio Windows Server 2012. O Windows Server 2012 define quais os eventos serão gerados. O log do sistema contém eventos registrados pelos componentes de sistema do Windows Server 2012. Por exemplo, a falha de um driver ou de outro componente do sistema ao ser carregado durante a inicialização é registrada no log do sistema. Os tipos de evento registrados no log pelos componentes do sistema são determinados previamente pelo Windows Server

2012.

**Em Logs de Eventos, existem cinco tipos de relatórios exibidos no utilitário Visualizar Eventos:**

**- Erro:** representado por um círculo vermelho com um x branco. Indica um problema sério tal como perda de dados ou de alguma funcionalidade de um serviço ou dispositivo que não está operando corretamente. Por exemplo, se um serviço falhar (DHCP, por exemplo),  durante a inicialização, um evento de erro será logado.

**- Aviso:** representado por um triângulo amarelo com um ponto de exclamação. Um evento que não é necessariamente um erro, mas pode representar um problema futuro. Por exemplo, quando o espaço em disco está ficando pequeno, um  aviso  será gravado.

**- Informações:** representado por um balão branco, com um ponto de exclamação azul. dentro. Descreve uma operação de sucesso de uma aplicação, execução de usuário, driver ou serviço. Por exemplo, quando um driver de rede é carregado com sucesso, um evento de informação é gerado.

**- Auditoria com Êxito:** representado por uma chave amarela. Evento gravado no log Segurança. Indica o evento de um acesso com sucesso. Por exemplo, se for habilitada a auditoria de tentativas de logon com sucesso, esse evento pode indicar um usuário que fez o logon com sucesso.