

DIFERENTES TIPOS DE DIRETIVAS

Texto adaptado do livro
Windows Server 2003 – Curso Completo
Editora Axcel Books
2003



Segue abaixo uma breve explicação sobre os diferentes tipos de diretivas de segurança disponibilizadas na família de servidores 2003, da fabricante Microsoft.

Diretiva local: São aquelas diretivas ou regras que implementamos nas máquinas locais, por exemplo, ao inserir uma rotina para impedir o usuário de alterar o papel de parede, nós teremos que executar essas diretivas máquina por máquina.

Diretiva do controlador de domínio: São as diretivas aplicadas ao controlador do domínio da rede, ou seja, no servidor responsável pelo serviço de Active Directory.

Diretiva do domínio: Neste cenário, nosso controlador de domínio pode distribuir diretivas para as demais máquinas, sem precisar aplicar as diretivas localmente. Utilizando esse tipo de diretiva, as regras são aplicadas diretamente a todos os demais computadores pertencentes ao domínio.

POLÍTICAS DE SENHA PARA O DOMÍNIO

Ao criar um domínio, com a instalação do Active Directory (AD) no primeiro Controlador de Domínio (DC) do domínio, por padrão definidas algumas políticas de segurança relacionadas às senhas dos usuários. Por exemplo, por padrão é definido que a senha deve ter no mínimo sete caracteres e que deve ser trocada a cada 42 dias, dentre outras definições. O administrador do sistema pode alterar estas políticas de segurança, para adequá-los às necessidades da sua rede.

As políticas de segurança são definidas para o domínio como um todo, ou seja, uma vez definidas elas passam a valer em todo o domínio. Aliás, está é uma das características determinantes de um domínio, ou seja, o compartilhamento de um conjunto único de políticas de segurança.

As políticas relacionadas à senha do usuário estão divididas em três grupos, conforme descrito abaixo:

- **Políticas de Senha:** Estas políticas definem as características que as senhas devem ter. Por exemplo: qual o número mínimo de caracteres, devem ser trocadas de quantos em quantos dias, devem ou não atender a critérios de complexidade e assim por diante.

- **Políticas para Bloqueio de Senha:** Estas políticas definem quando uma conta será bloqueada, com base em um número de tentativas de logon sem sucesso. Por exemplo, o administrador pode definir que, se o usuário tentar fazer três logons sem sucesso (por exemplo, digitando uma senha incorreta para sua conta) dentro do período de uma hora, a conta será bloqueada. Estas políticas são utilizadas para evitar que um usuário mal-intencionado tente sucessivamente fazer o logon, usando diferentes senhas, em uma tentativa de “adivinhar” a senha do usuário.
- **Políticas de Kerberos:** O Kerberos é um protocolo padrão e muito utilizado de autenticação utilizado por muitos sistemas operacionais. Existem algumas políticas de segurança relacionadas ao protocolo Kerberos que podem ser definidas pelo administrador. Por exemplo, através destas regras de Kerberos, podemos definir como os tickets de sessão serão transmitidos, assim como, qual o tempo que esses tickets terão de duração, o qual é responsável pela concessão de permissão para utilização dos recursos da rede.

Recomendações sobre valores a serem definidos para as políticas de senha e políticas de bloqueio de senha, as quais foram descritas anteriormente:

- Defina uma política de segurança para a empresa como um todo, dentro da qual está a definição das políticas de senha. A política de segurança deve ser constantemente revisada e atualizada e, o mais importante, divulgada para todos na empresa.
- Habilite sempre as políticas para bloqueio de conta, de tal maneira que, após um número determinado de tentativas de logon sem sucesso, a conta do usuário seja bloqueada. Em ambientes em que a segurança é um fator crítico, defina também que somente o administrador pode desbloquear contas. Normalmente, utiliza-se o valor de três tentativas de logon sem sucesso em uma hora como limite para bloqueio de contas.
- Habilite a diretiva para tempo máximo e tempo mínimo de senha, conforme descrito anteriormente. Em conjunto com essas políticas, defina a política que define o histórico de senhas a ser armazenado no Active Directory. Valores normalmente utilizados para estas diretivas são um tempo máximo de 30 dias, um tempo mínimo de 10 dias e um histórico de cinco senhas. Com estas

diretivas, significa que o usuário deverá alterar sua senha a cada trinta dias, e uma vez alterada a senha ele poderá alterá-lo novamente somente daqui a 10 dias, e ao alterar a senha, o usuário não poderá utilizar uma senha que seja igual a uma das cinco últimas que ele utilizou.

- Defina um número mínimo de caracteres para a senha (*diretiva “comprimento mínimo da senha”*). Um valor normalmente utilizado é de 8 caracteres para ambientes empresariais e 10 caracteres para redes de segurança crítica. O máximo que você pode definir como tamanho mínimo é de 14 caracteres. A senha pode conter mais do que 14 caracteres; o que não é possível é definir que as senhas devem ter um mínimo superior a 14 caracteres.