**Políticas de Segurança no AD**

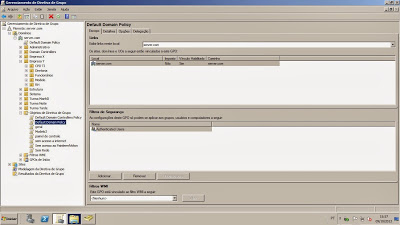
**As Políticas de Segurança são "scripts" que configuram e elevam o sistema de segurança de uma rede baseada em Domínio.**

* ESPECIFICAÇÕES:

- Diretivas de Segurança de Domínio  
- Diretivas de Segurança do Controlador de Domínio  
- Diretivas de Grupo associadas as UOs  
- Diretivas Locais  
- Delegação de Controle

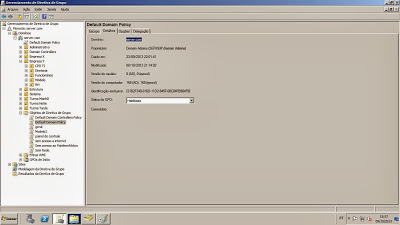
As GPOs configuram desde o tamanho da senha, até restrições avançadas que envolvem componentes de sistema, tais como bloqueios de dispositivos e execução de processos.  
  
Para a configuração, edição e aplicação das GPOs (Group Policy Objects), nos usaremos o Gerenciamento de Diretivas de Grupo.  
  
No site TechNet, a definição para o console de Gerenciamento de Diretivas de Grupo:  
  
"O Editor de Objectos de Política de Grupo consiste na ferramenta de gestão de configuração do utilizador e computador que é incluída com o Active Directory. As definições de Política de Grupo incluem definições de segurança no Editor de Objectos de Política de Grupo, embora as definições de segurança sejam apresentadas e processadas de forma diferente da maioria das definições de Política de Grupo. Por exemplo, as definições de segurança são persistentes no registo; enquanto que as definições de modelos administrativos de Política de Grupo são escritas novamente sempre que a política é actualizada.  
O Editor de Objectos de Política de Grupo é utilizado para editar todos os objectos de Política de Grupo, incluindo os que foram convertidos a partir do formato SCW. Por conseguinte, o SCW torna o Editor de Objectos de Política de Grupo mais útil, pois fornece GPOs personalizados para tipos de servidores."  
  
Primeiramente, iremos criar uma estrutura lógica no AD. Vamos acessar as Ferramentas Administrativas/Usuários e Computadores do AD. Criaremos uma estrutura lógica com UOs.

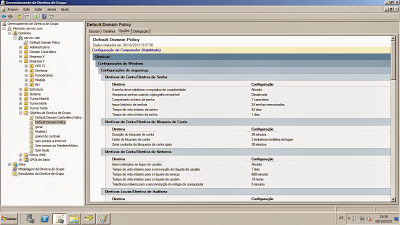
Iremos configurar as GPOs que serão válidas para o Domínio. Vamos acessar o Gerenciamento de Diretivas de Grupo.

[](http://4.bp.blogspot.com/--s7Bc0ve5h4/UlWoggjBdsI/AAAAAAAAB00/1wdlP7l4I58/s1600/1.jpg)

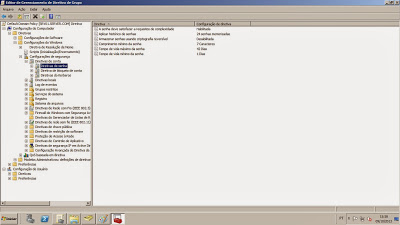
Na imagem acima, podemos visualizar o Escopo da configuração das GPOs, ou seja, para qual Domínio ela esta habilitada e qual o caminho de aplicação.

Nas imagens abaixo, já visualizamos em Detalhes, o Proprietário, a data da criação e modificação, bem como as versões do AD e Sysvol. Visualizamos também o relatório de GPOs associadas ao Domínio.

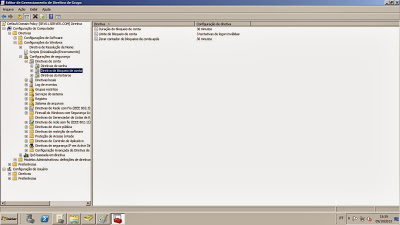
[](http://3.bp.blogspot.com/-s5q_rFvmSbw/UlWpRwkoW0I/AAAAAAAAB08/JJTgH722YS0/s1600/2.jpg)

[](http://4.bp.blogspot.com/-WlY8eBXq95M/UlWp51-e-dI/AAAAAAAAB1E/OjFi3XU0zXI/s1600/3.jpg)

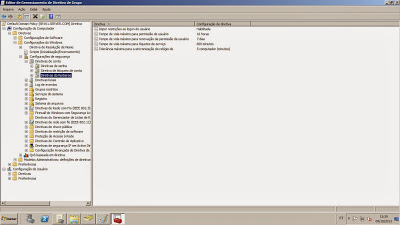
Na próxima imagem, veremos as configurações de Conta, no bloco de GPOs de Senha.

[](http://3.bp.blogspot.com/-4z5gcf_6vus/UlWqIOOEOHI/AAAAAAAAB1M/9ULxY7ktCKI/s1600/4.jpg)

OBS: todas as definições das GPOs de senha estão na apostila da disciplina.

[](http://4.bp.blogspot.com/-9K_ZcsKTXEs/UlWqi560PSI/AAAAAAAAB1U/XeasGsDDDGU/s1600/5.jpg)

Configurações de Bloqueio de Conta

[](http://2.bp.blogspot.com/-8YFQJppTDjs/UlWqwP3LHxI/AAAAAAAAB1c/l9vlhv-I1eE/s1600/6.jpg)

Configurações de Kerberos.

**Kerberos:** De acordo com a Wikipedia, Kerberos é um protocolo de autenticação do Projeto Athena. Tem esse nome em alusão ao Cão guarda de três cabeças (Cérbero) do deus Hades da Mitologia grega. Diversas versões do protocolo já existiram, as versões 1 até a 3 foram utilizadas somente dentro da MIT. Steve Miller e Clifford Neuman, foram os principais projetistas da versão 4 do Kerberos, publicada nos anos 80, ainda com foco no Projeto Athena.

A versão 5 foi projetada por John Kohl e Clifford Neuman e publicada em 1993 no RFC 1510 (Ficou obsoleto ao RFC 4120 de 2005), e teve como intenção melhorar a segurança e as limitações relativas a versão 4.

A MIT disponibilizou uma implementação livre sob licença BSD.

Autoridades Norte-americanas/Estadundenses proibiram o uso do Kerberos, pois esse utiliza um algoritmo de criptografia com uma chave de 56-bit, chamado DES. Eles consideraram que o protocolo prejudica a segurança nacional, porque impede que mensagens interceptadas sejam entendidas (Assim como qualquer aplicativo que utilize criptografia com chave maior que 40-bit). Uma implementação não americana do Kerberos, KTH-KRB foi desenvolvida pela Royal Institute of Technology na Suécia, tornando assim o sistema disponível fora dos EUA, até a mudança da regulamentação de exportação de criptografias. A implementação Sueca é baseada em uma versão chamada eBones. eBones é baseado em um release da versão eBones da MIT (Retirado a criptografia e as chamadas a mesma) que por sua vez foi baseado na versão 4 do Kerberos atualização 9. Esse Kerberos limitado é chamado hoje como eBones. Uma implementação chamada Heimdal, foi feita basicamente, pelo mesmo grupo de pessoas e é baseada na versão 5 do Kerberos.

De acordo com o site TechNet (abaixo):

## Autenticação Kerberos V5

O Kerberos V5 é o principal protocolo de segurança para autenticação em um domínio. O protocolo Kerberos V5 verifica a identidade do usuário que solicita a autenticação assim como o servidor que fornece a autenticação solicitada. Essa verificação bidirecional é conhecida também como autenticação mútua.

#### Visão geral sobre como o Kerberos V5 trabalha

O mecanismo de autenticação Kerberos V5 emite tíquetes para permitir o acesso aos serviços de rede. Esses tíquetes contêm dados criptografados, incluindo senha criptografada, que confirma a identidade do usuário para o serviço solicitado. Exceto pela inserção de uma senha e das credenciais do cartão inteligente, todo o processo de autenticação é invisível para o usuário.

Um serviço importante no Kerberos V5 é o Centro de Distribuição de Chaves (KDC). O KDC é executado em cada controlador de domínio como parte do serviço de diretório do Active Directory, que armazena todas as senhas de cliente e outras informações sobre contas.

O processo de autenticação Kerberos V5 funciona da seguinte maneira:

1. O usuário em um sistema cliente, com uma senha ou um cartão inteligente, fornece autenticação ao KDC.
2. O KDC emite um tíquete de concessão de tíquete (TGT) especial para o cliente. O sistema cliente usa esse TGT para acessar o serviço de concessão de tíquete (TGS), que faz parte do mecanismo de autenticação Kerberos V5 no controlador de domínio.
3. Em seguida, o TGS emite um tíquete de serviço para o cliente.
4. O cliente apresentará esse tíquete de serviço ao serviço de rede que foi solicitado. O tíquete de serviço comprova a identidade do usuário para o serviço e a identidade do serviço para o usuário.

Os serviços do Kerberos V5 serão instalados em cada controlador de domínio e um cliente Kerberos será instalado em cada estação de trabalho e servidor.

Todo controlador de domínio atua como um KDC. Um cliente usa uma pesquisa de sistema de nomes de domínios (DNS) para localizar o controlador de domínio disponível mais próximo. O controlador de domínio funcionará como o KDC preferencial para esse usuário durante a sessão de logon do usuário. Se o KDC preferencial ficar indisponível, o sistema localizará um KDC alternativo para fornecer autenticação.

Para obter mais informações sobre como o Kerberos V5 fornece autenticações, consulte [Kerberos Authentication Technical Reference](http://technet.microsoft.com/pt-br/library/cc739058(v=ws.10).aspx) na Referência Técnica sobre o Windows Server 2003.

Para obter mais informações sobre o Kerberos, consulte a seção sobre logon e autenticação no [Microsoft Windows Resource Kits](http://go.microsoft.com/fwlink/?LinkId=4546).  
  
Continuando ....

**Kerberos - LDAP e GC (Catálogo Global)**

**- Protocolo Kerberos:** o Kerberos foi desenvolvido para fornecer poderosa autenticação em aplicações usuário/servidor, onde ele funciona como a terceira parte neste processo, oferendo autenticação ao usuário, ou seja, "dizendo" para o sistema servidor/cliente quem realmente é o usuário. Na verdade, este mecanismo identifica o usuário trazendo consigo as sincronizações referentes aos processos da rede agregadas as políticas de segurança aplicadas a este objeto (user).

No caso do Windows Server, o Kerberos entra em cena com o seu**KDC (Centro de Distribuição de Chaves para autenticação)**. De acordo com o site Technet, o Kerberos é integrado com outros serviços de segurança do Windows Server que são executados no controlador de domínio. O KDC utiliza o banco de dados do serviço de diretório do Active Directory como seu banco de dados de conta de segurança. O Active Directory é necessário para implementações padrão do Kerberos dentro do domínio ou floresta. No Windows Server 2012 e anteriores, a autenticação Kerberos pode ser aproveitada para resolver problemas de falta de conectividade com o controlador de domínio da conectividade remota ao colocar em proxy a autenticação Kerberos e as mensagens de alteração de senha para usuários do DirectAccess ou da Área de Trabalho Remota que estão solicitando o acesso ao domínio.

|  |
| --- |
|  |
| Imagem, site TechNet |

**Aplicações práticas (fonte, site TechNet)**

O protocolo Kerberos V5 é mais seguro, mais flexível e mais eficiente que o NTLM. Os benefícios obtidos com o uso da autenticação Kerberos são:

**Autenticação delegada.**

Os serviços Windows representam um cliente quando acessa os recursos em nome do cliente. Em muitos casos, um serviço pode concluir seu trabalho para o cliente ao acessar recursos no computador local. O NTLM e o protocolo Kerberos V5 fornecem as informações de que o serviço precisa para representar seu cliente localmente. No entanto, alguns aplicativos distribuídos são projetados de forma que um serviço front-end deva representar clientes ao se conectar a serviços back-end em outros computadores. O protocolo Kerberos V5 inclui um mecanismo de proxy que permite que um serviço represente seu cliente ao se conectar com outros serviços. Não há nada equivalente disponível no NTLM.

**Interoperabilidade.**

A implementação da Microsoft do protocolo Kerberos V5 é baseada em especificações de acompanhamento de padrões que são recomendadas para IETF (Internet Engineering Task Force). Como resultado, a implementação do Windows do protocolo Kerberos V5 coloca uma base para a interoperabilidade com outras redes em que o protocolo Kerberos V5 é usado para autenticação.

**Autenticação mais eficiente para servidores.**

Com a autenticação NTLM, um servidor de aplicativo deve se conectar a um controlador de domínio para autenticar cada cliente. Por outro lado, com o protocolo de autenticação Kerberos V5, o servidor não precisa ir até um controlador de domínio. Em vez disso, o servidor pode autenticar o cliente examinando as credenciais apresentadas pelo cliente. Os clientes podem obter as credenciais para um determinado servidor um vez e depois reutilizá-las por toda a sessões de logon na rede. Os tíquetes de sessão renováveis substituem a autenticação de passagem.

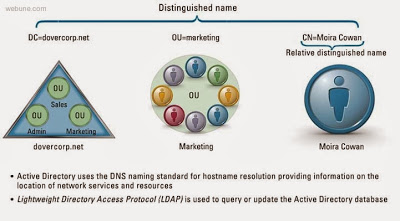
**Autenticação mútua.**

Ao utilizar o protocolo Kerberos, uma parte na extremidade de uma conexão de rede pode verificar se a parte no outra extremidade é a entidade que ela diz ser. Embora o NTLM permita que os servidores verifiquem as identidades de seus clientes, ele não permite que os clientes verifiquem a identidade de um servidor, nem que um servidor verifique a identidade de outro servidor. A autenticação NTLM foi projetada para um ambiente de rede em que supõe-se que os servidores sejam genuínos. O protocolo Kerberos V5 não faz nenhuma suposição.

<http://technet.microsoft.com/pt-br/library/hh831553.aspx>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**- LDAP: Lightweight Directory Access Protocol**, ou LDAP, é um protocolo para atualizar e pesquisar diretórios rodando sobre TCP/IP. Um diretório LDAP geralmente segue o modelo X.500, que é uma árvore de nós, cada um consistindo de um conjunto de atributos com seus respectivos valores. O LDAP foi criado como uma alternativa ao muito mais incômodo Directory Access Protocol (DAP). Ele trabalha de forma hierárquica e define vários limites geográficos e políticos da rede. O LDAP se utiliza das referências nominais do DNS. A atualização dos diretórios de informação dos objetos de rede se baseia na estruturação dos níveis mais básicos desta hierarquia. Mais profundamente, podem aparecer usuários, unidades organizacionais, impressoras, documentos, grupos de usuários ou qualquer outra coisa que represente um objeto da rede.  
De acordo com a Wikipedia, o LDAP oferece uma grande escalabilidade. É possível replicar servidores (para backup ou balanceamento de carga) e incluir novos servidores de uma forma hierárquica, interligando departamentos e filiais de uma grande multinacional por exemplo.**A organização dos servidores neste caso é similar ao DNS: é especificado um servidor raiz e a partir daí é possível ter vários níveis de sub-servidores, além de mirrors do servidor principal.**

[](http://1.bp.blogspot.com/-a891KXtO15c/UnJPueSEvYI/AAAAAAAAB2c/KlKyXaI70mc/s1600/17--ldap.jpg)

**GC - Catálogo Global:** O catálogo global é o conjunto de todos os objetos de uma floresta dos Serviços de Domínio Active Directory (AD DS - Domain Services). O servidor do catálogo global é um **controlador de domínio que armazena uma cópia completa de todos os objetos no diretório para seu domínio host e uma cópia parcial somente leitura de todos os objetos para todos os outros domínios na floresta.** Os servidores do catálogo global respondem as consultas relacionadas com o catálogo global.

Quando o AD é instalado, o catálogo global da nova floresta é criado automaticamente no primeiro controlador de domínio da floresta. É possível adicionar a funcionalidade do catálogo global a outros controladores de domínio. Também é possível remover o catálogo global de um controlador de domínio.

**Funções do CG: (fonte TechNet)**

**Localiza objetos.**

O catálogo global ativa as pesquisas de informações de diretório do usuário em todos os domínios de uma floresta, independentemente do local onde os dados estão armazenados. As pesquisas na floresta são executadas com máxima velocidade e tráfego de rede mínimo.

Quando um usuário pesquisa pessoas ou impressoras no menu Iniciar ou seleciona a opção Pasta Inteira em uma consulta, ele está utilizando o catálogo global. Depois que o usuário insere uma solicitação de pesquisa, esta será encaminhada à porta 3268 do catálogo global e enviada a um servidor de catálogo global para resolução.

**Fornece a autenticação do nome principal do usuário.**

Um servidor de catálogo global resolve o nome principal do usuário (UPN) quando o controlador de domínio da autenticação desconhece a conta de usuário. Por exemplo, se uma conta de usuário for localizada em sales1.cohovineyard.com e o usuário efetuar logon com o UPN luis@sales1.cohovineyard.com de um computador localizado em sales2.cohovineyard.com, o controlador de domínio em sales2.cohovineyard.com não encontrará a conta de usuário e deverá contatar um servidor do catálogo global para concluir o processo de logon.

**Valida as referências de objeto em uma floresta.**

Os controladores de domínio usam o catálogo global para validar as referências a objetos de outros domínios na floresta. Quando um controlador de domínio dispõe de um objeto de diretório com um atributo contendo uma referência a um objeto de outro domínio, ele valida essa referência, contatando um servidor do catálogo global.

Fornece informações sobre a associação ao grupo universal em um ambiente de vários domínios.

O controlador de domínio também pode descobrir associações de um usuário ao grupo local do domínio e ao grupo global e a associação a esses grupos não será replicada no catálogo global. Em uma floresta com um único domínio, o controlador também pode descobrir associações ao grupo universal. Todavia, os grupos universais podem ter membros de domínios diferentes. Por esse motivo, o atributo membro dos grupos universais, que contém a lista de membros no grupo, é replicado no catálogo global. Quando um usuário de uma floresta de vários domínios efetua logon em um domínio onde os grupos universais são permitidos, o controlador de domínio deve contatar um servidor de catálogo global para recuperar as associações desse usuário ao grupo universal em outros domínios.

|  |
| --- |
|  |
| Imagem, site TechNet |

Se um servidor de catálogo global não estiver disponível quando um usuário efetuar logon em um domínio em que os grupos universais estão disponíveis, o computador cliente do usuário poderá usar as credenciais armazenadas em cache para fazer logon, se o usuário tiver se conectado no domínio anteriormente. Se, por outro lado, o usuário não tiver se conectado no domínio anteriormente, ele poderá fazer logon no computador local apenas.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_