Plataforma Novell NetWare

"A vida necessita de pausas"
Carlos Drummond de Andrade

Este capítulo não analisa o NetWare com tanta profundidade como no caso dos Unix e do Windows. A Novell tem uma política muito restritiva quanto à divulgação de aspectos internos de seus sistemas. Ao mesmo tempo, sistemas Novell são muito raros em soluções para a Web ou conectadas à Internet (uma exceção digna de nota é o site da CNN.com, que utiliza a tecnologia NDS para prover páginas dinâmicas personalizadas a cada um dos seus 6 milhões de assinantes, com acessos únicos superiores a 33 mil por dia).

Entretanto, redes corporativas baseadas em NetWare e NDS são extremamente populares em grandes e médias empresas, uma vez que o veterano sistema operacional de redes da Novell possui seus atributos de segurança, robustez e velocidade. Nada mais justo do que descrevê-lo, brevemente, em nossa obra.

Já com mais de 20 anos de estrada, o veterano NetWare nasceu de uma empresa de... hardware? Em 1979, a Novell Data Systems, Inc. iniciou suas atividades como fabricante de sistemas computacionais (hardware) e sistemas operacionais de disco. Em 1983, já com o nome definitivo de Novell, Inc., o foco da empresa foi deslocado para a fabricação de hardware e software para redes de computadores.

A empresa ajudou a criar os conceitos e tecnologias de redes corporativas já no início dos anos 80, uma época em que sistemas abertos de conectividade não eram sequer cogitados, e a tecnologia IP era considerada coisa acadêmica, amadorística e sem importância – realmente, IP não era uma opção naqueles dias. Mas quem começou a trabalhar com redes e conectividade nos anos 80 certamente passou por pelo menos uma experiência com redes NetWare. Ou melhor: eram raros os profissionais que tinham pouco contato com essa tecnologia. Na virada dos anos 80 para 90, a Novell detinha 70% do mercado de redes locais ou corporativas, só vindo a deixar essa posição com o advento do Windows NT e as peripécias midiáticas da turma de Redmond.

No início de tudo, uma rede local (hoje chamada de rede departamental) era simplesmente um cabo interligando computadores que compartilhavam arquivos e impressoras. O ano de 1983 foi decisivo para a empresa: além de trocar de nome e de presidente, a Novell introduziu o NetWare, o primeiro software de redes baseado na tecnologia de servidor de arquivos: uma máquina (o servidor) gerenciava o acesso à rede e aos periféricos (impressoras, principalmente), além de "guardar" os arquivos e dados das pessoas. Enquanto isso, o processamento era distribuído em estações de trabalho nas mesas dos usuários. Tal modelo representava uma mudança significativa na visão *network-centric* do mercado, massa cultural herdada da computação de grande porte.

Hoje, as tecnologias Novell migraram para esferas mais abrangentes. O foco agora é integrar várias tecnologias de vários fornecedores e fazê-las trabalhar em conjunto – sob a batuta do NDS, a tecnologia que torna essa mágica possível. Com isso, a Novell evoluiu de fornecedora de um sistema operacional de redes para uma fornecedora de soluções para grandes redes que permitem a grandes empresas obter uma verdadeira computação corporativa. Além do NDS, outra providência para integrar grandes redes foi a adoção do protocolo IP em detrimento do IPX, atendendo assim aos apelos do mercado e permitindo integração com serviços de Internet. Em 1999, a Novell lançou o eDirectory, um serviço de diretório baseado no NDS (catálogo, *sigh*[1]) que promete (e cumpre!) amarrar diversas plataformas em uma única rede.

Este capítulo não tem a pretensão de ser um guia definitivo para o NetWare. Nosso intuito é mostrar, em poucas páginas, um pouco da estrutura do sistema para que o leitor sinta-se familiarizado quando encontrar (ou invadir...) um sistema desses. Recomendamos, se possível, o acompanhamento desse texto em um sistema de testes. A própria Novell oferece gratuitamente para download uma versão do NetWare limitada a poucos usuários, destinada unicamente para pesquisa e estudo.

Desenrolando o novelo

Basicamente, o NetWare é um sistema operacional de redes (Network Operating System ou NOS) baseado no paradigma cliente/servidor. É baseado em programas clientes que rodam em MS-DOS, Windows 3.x, Windows 9x e Windows NT/2k/XP, além de Macintosh e OS/2 e em um ou mais servidores centrais dedicados, que autenticam os clientes e distribuem recursos a eles. Clientes Unix e mesmo recursos de servidores Unix são suportados, mas devem empregar ferramentas não nativas, desenvolvidas por terceiros. Mesmo o Linux possui um programinha cliente – o pacote NCPFS, também open source e recomendado oficialmente pela própria Novell, embora sem suporte técnico – para integrar-se a redes NetWare.

Os três grandes grupos de funções de um servidor NetWare são **autenticação**, **armazenamento de arquivos** e **distribuição de recursos** (impressão, single sign-on, drives remotos, periféricos centralizados...). Para cumprir essas três funções, o NetWare até a versão 3.12 usava um recurso chamado **bindery**. A partir da NetWare 4.11, foi introduzida a tecnologia **NDS** (NetWare Directory Service), que substituiu o bindery com vantagens e permitiu que o sistema gerenciasse redes mais abrangentes e, posteriormente, redes heterogêneas com soluções disparatadas de várias procedências.

Bindery

Os clientes precisam de autorização (ou *autenticação*) do servidor para utilizar os recursos da rede. Tal acesso, nas redes NetWare até a versão 4, era franqueado ao usuário se e somente se este estivesse autorizado no esquema de **bindery**.

O bindery era, grosso modo, uma entidade que permitia cadastrar usuários, outros servidores, workstations, diretórios e serviços de impressão e definir

*1. É muito importante não confundir o conceito de **diretório de arquivo** (como em C:\WINDOWS é um diretório do drive C:) com **diretório NDS**. Os nomes são parecidos, mas são idéias completamente diferentes. Por esse motivo, chamaremos sempre o sistema NDS de **diretório NDS**.*

relacionamentos entre eles. No bindery também eram definidos o que se chama hoje de **trustes**: relações de direito e permissões entre os usuários e objetos da rede. Como objetos, podemos citar os próprios usuários, arquivos, diretórios, discos, volumes e filas de impressão. Tais permissões eram definidas utilizando-se os direitos básicos da Novell: ler, escrever, ver ("dar dir", também conhecido como *File Scan*), criar, modificar, apagar, dar direitos e supervisão.

O bindery era um subsistema residente em dois arquivos, NET$PROP.SYS e NET$OBJ.SYS, e operava sob uma estrutura de banco de dados nativo. As informações relativas a usuários, diretórios e serviços de impressão eram cadastradas numa tabela simples que os "ligava" (daí o nome bindery – colagem) e, a partir daí, liberava ou bloqueava o acesso de cada usuário aos recursos da rede.

Existiam alguns utilitários básicos, que estavam disponíveis apenas para o administrador da rede e rodavam nas estações. O principal era o **syscon,** que permitia mexer no servidor e em suas propriedades. Havia ainda o printcon para gerenciar filas de impressão e o filer, uma espécie de gerenciador de arquivos. Todos eles muito eficientes e muito fáceis e intuitivos de operar. E todos em modo texto.

No console do servidor era possível rodar algumas ferramentas, como o pconsole para monitorar as filas de impressão, mas o recomendado era fazer tudo remotamente, pela conta do administrador, e deixar o servidor fisicamente trancafiado em algum armário – um sistema que roda completamente desatendido e, portanto, pode ter sua segurança física reforçada.

NDS

Ainda hoje o bindery seria uma solução viável para a maioria das redes de pequeno e médio porte. É imbatível nos quesitos segurança e filas de impressão, e possui um esquema de boot remoto supereficiente – muito útil na época dos XTs, quando discos rígidos eram muito caros e drives de disquete eram os principais pontos de contágio de vírus em uma rede. Era extremamente leve (rodava em máquinas 386 com 4 Mbytes de RAM) e possuía um kernel enxuto e muito rápido.

Mas a partir do NetWare 4.11, o antigo sistema de autenticação e controle do NetWare foi substituído pelo NDS. O veterano bindery era ineficiente para redes muito grandes, de 80 ou mais estações. Grandes redes muito segmentadas e comportando usuários e sistemas com necessidades diferentes não encontravam no bindery desempenho e flexibilidade de configuração. Além disso, um sistema baseado em texto num mundo dominado pelo Windows NT estava fadado a fracassar – era fora de moda...

O NDS é a fundação de todos os sistemas da Novell até hoje. É composto de três partes: o servidor de diretórios NDS, o software cliente (parecido com os clientes de bindery – para o usuário, é apenas a tela de login e de senha) e um software de administração, no qual o gerente da rede pode criar relações entre os objetos da rede de maneira visual, e pode definir regras para a criação de novos objetos. Por exemplo, quando um usuário é criado, deve pertencer a um grupo. Todos os usuários daquele grupo têm direito a acessar alguns objetos (alguns diretórios ou pastas nos drives de rede, a impressora do departamento a que pertence, o sistema de contabilidade, a Internet, acesso à tabela X do banco de dados, uma conta na máquina Linux do departamento de Engenharia...), portanto, a simples criação desse usuário nesse grupo automaticamente o ligará a todos os sistemas que o grupo pode acessar e barrará qualquer conexão a outros recursos.

Na parte de administração da rede, todos aqueles utilitários do bindery, mais os utilitários das máquinas Windows, Unix/Linux, Serviços Web, sistemas de grande porte e mainframes, etc, etc, etc, serão gerenciados pelo console do NDS – que é gráfico e se parece com o Windows Explorer. São enormes as possibilidades de gerenciamento de redes muito grandes, bastante heterogêneas e com idiossincrasias estranhas e complexas.

Os tipos de objetos principais no NDS são o **[root]** (assim mesmo, entre colchetes), **Contêineres** e Folhas ou **Leafs**. O objeto [root] é, na realidade, o topo da estrutura ou a raiz de uma árvore invertida (como o / nos sistemas Unix e o C:\ em um drive DOS ou Windows). Existe apenas para comportar todos os objetos que vêm abaixo dele.

Os **Contêineres** são objetos que, como o nome diz, podem conter outros. São, em nossa analogia da árvore invertida, os galhos mais grossos. O próprio [root] é um contêiner, mas só pode haver um [root] por diretório NDS, e ele não possui nenhuma propriedade para ser alterada ou herdada. Os objetos abaixo dele, entretanto, possuem já algumas propriedades e podem ser de três tipos:

- **Country** – organizam o diretório por códigos de país válidos (us = Estados Unidos, br = Brasil, de = Alemanha, fr = França...).
- **Organization –** representa a organização à qual pertence o diretório NDS, ou seja, o nome da empresa, ONG, igreja, associação, site, etc. que possui o sistema. Normalmente fica abaixo de um objeto do tipo Country.
- **Organizational Unit –** subdivisões da organização. Exemplos: filiais da empresa, escritórios da ONG, pontos de pregação da igreja, sedes da associação... Esse tipo de objeto pode ser colocado abaixo de um objeto Organization ou de outro Organizational Unit, e é opcional.
- **Leaf –** são os objetos realmente importantes na árvore do NDS. Enquanto os objetos acima são puramente organizacionais, servindo para classificar e configurar os diversos serviços e recursos da rede de uma forma lógica, os leafs ou folhas representam exatamente esses serviços e recursos. Há várias classes de leafs, representando os diferentes tipos de entidades que podem ser criados e manipulados na rede, como usuários, grupos, servidores, volumes, mapeamentos de drives e diretórios, programas, sistemas, gateways, rotas e redes, impressoras... Há 21 classes no total. Objetos do tipo Leaf não podem conter outros objetos, nem ser posicionados diretamente sob o objeto [root].

Qualquer objeto em uma árvore NDS é acessado por seu nome, num esquema parecido com o Domain Name Service (DNS – cuidado com as siglas similares!) dos domínios da Internet. Por exemplo, o usuário Ulbrich da filial Brasília da empresa Tatu Informática Ltda, seria referenciado, em um sistema NDS, pelo nome .**CN=Ulbrich.OU=BSA.O=TatuInformatica** – observe que há um ponto obrigatório antes de CN (Common Name – o nome objeto de mais baixo nível) e não pode haver ponto após o objeto de mais alto nível. Na verdade, os descritores de tipo não são obrigatórios (embora dêem clareza ao nome), portanto o nome acima poderia ser escrito como:

.Ulbrich.BSA.TatuInformática

O nome acima, com todos os identificadores até o [root], é chamado de **Fully Distinguished Name** ou FDN. Mas no NDS os usuários logam-se num **contexto**, que é basicamente um galho grosso em que estão pendurados os objetos a que o usuário tem direito ou que acessa com mais freqüência. Uma vez logado no contexto, sempre que o usuário referir-se a objetos dentro dele pode fazê-lo usando apenas o nome simples do objeto. No nosso exemplo, o usuário está logado no contexto **.BSA.TatuInformatica**; portanto, para acessar o objeto CN (no caso, as informações de login dele mesmo), basta chamar por **CN=Ulbrich**. Quando o usuário quiser acessar objetos presentes em outro contexto que não o seu de login (por exemplo, na filial de Curitiba), deverá usar o FDN dela – em nosso exemplo, **ERP.CWB.TatuInformatica**.

Dica: para navegar pelos contextos no prompt do DOS, use o comando CX, presente no SYS:PUBLIC.

Estrutura

Os discos rígidos em um sistema NetWare são divididos em **volumes**, que são unidades lógicas de armazenamento contendo o próprio NetWare e os softwares do usuário. Em sistemas NDS, os volumes são objetos Leaf na árvore.

Dividir o espaço de armazenamento em volumes pode significar mais organização e desempenho na rede – e também pode gerar uma grande confusão. Um volume pode ter mais de um disco, e um disco pode possuir mais de um volume. Atualmente, cada servidor NetWare suporta até 64 volumes, e cada volume pode estar contido em até 32 discos rígidos. Os volumes são formatados no sistema de arquivos padrão do NetWare, mas aparecerão para os usuários em suas estações de trabalho como drives MS-DOS comuns. São representados em notação **SERVIDOR\VOLUME:**, portanto o volume SYS: de um servidor chamado SERVDIGERATI seria representado como **SERVDIGERATI\SYS:**.

Os volumes têm nomes no formato **NOME:**, e o que vem depois dos dois-pontos são os diretórios principais daquele volume. Assim, em um volume hipotético chamado ADM, poderia haver uma árvore assim:

- ADM: – o diretório raiz (root) daquele volume;
- ADM:DADOS – diretório DADOS do volume ADM;
- ADM:CONFIG – diretório CONFIG do volume SYS;
- ADM:CONFIG\CONSOLE – arquivo ou diretório CONSOLE do diretório CONFIG do volume ADM.

Portanto, em nosso caso específico, o programa INSTALL.EXE dentro do subdiretório CONSOLE, no diretório CONFIG, no volume ADM do servidor SERVDIGERATI seria representado inteiramente como **SERVDIGERATI\ADM:CONFIG\CONSOLE\INSTALL.EXE**.

Há um volume especial, obrigatório em todos os NetWares, que contém os arquivos de sistema, módulos carregáveis e bibliotecas. Chamado de **SYS:**, possui a seguinte estrutura:

- **SYS:LOGIN** – tanto em sistemas bindery quanto NDS, é único diretório disponível para qualquer usuário **antes** que ele faça login. Contém os programas LOGIN.EXE, CX, NLIST e MAP.
- **SYS:SYSTEM** – diretório disponível apenas para os administradores, contendo diversas ferramentas administrativas e alguns utilitários.Também contém NLMs úteis para as tarefas de administração (veremos o que são NLMs mais à frente).
- **SYS:PUBLIC** – disponível para **todos** os usuários após o login. Contém comandos e utilitários para usuários comuns, como o NWADMIN, NETADMIN, NWUSER, NETUSER, MAP, NLIST, NDIR, NCOPY e PCONSOLE, entre outros.
- **SYS:MAIL** – em sistemas NetWare 3.x, era usado como mail spooler e podia conter o próprio subsistema de correio. Não é usado no 4.x e posteriores: o diretório é criado apenas por questões de compatibilidade.
- **SYS:NLS** – comporta o subsistema NLS (NetWare Language Support), cada diretório tem um subdiretório NLS. Ele identifica o idioma usado e apresenta suas messagens nesta língua.
- **SYS:ETC** – presente apenas no NetWare 4 e superiores, contém componentes estranhos aos padrões originais do sistema, como, por exemplo, os arquivos de configuração TCP/IP.
- **SYS:QUEUES** – também presente apenas nas distribuições baseadas em NDS. É usado pelo objeto Print Queue (gerenciador de filas de impressão) do NDS. Na verdade, não precisa ser necessariamente colocado no volume SYS, a localização depende do projeto da rede e pode estar em qualquer volume especificado no objeto Printer do NDS.
- **SYS:DELETED.SAV** – similar à lixeira do Windows, mas os utilitários Filer e NWAdmin são usados para recuperar os arquivos apagados. Também pode estar em qualquer volume.
- **SYS:DOC** – a documentação on-line do NetWare, em formato Dynatex.

Uma vez criados os volumes de acordo com as necessidades da rede e definidas as permissões de usuários e grupos para cada volume e cada diretório e arquivo do volume, podem-se fazer **mapeamentos de drives** (drive mappings), que são, simplesmente, a atribuição de letras de unidade a diretórios específicos. No nosso exemplo, ADM:CONFIG poderia ser o drive **K:**, ADM:DADOS o

drive **D:** e SYS:MAIL o drive **M:**. Usualmente, SYS:LOGIN é mapeado no drive **F:** e o diretório pessoal do usuário (que pode estar em qualquer volume à escolha do administrador) é mapeado em **U:**. Alguns mapeamentos são chamados de **search mappings** e servem como caminhos-padrão para o usuário – similar às variáveis **path** no Windows e nos Unix. O mapeamento pode ser feito pelo NDS ou com o auxílio do comando MAP – herdado de versões anteriores.

NLMs

O microkernel do NetWare pode ter funcionalidades adicionais com o carregamento de módulos chamados NLMs (NetWare Loadable Modules). Serviços como roteamento, alguns utilitários de rede e pilhas de rede TCP/IP, por exemplo, eram ativados por NLMs. Havia inclusive softwares de terceiros, como o ARCsolo (um utilitário de backup) que eram carregados também por NLMs. Todos os NLMs possuíam arquivos de configuracão em texto puro *a la* Unix.

Para rodar um NLM, basta usar, no console do servidor, o comando LOAD seguido do nome do NLM. Alguns NLMs fornecidos com o NetWare:

- INSTALL.NLM – módulo para instalar, gerenciar e manter o servidor. Contém diversas ferramentas e acesso a inúmeras configurações do kernel.
- MONITOR.NLM – módulo para gerenciar o funcionamento normal do servidor. Alguns administradores deixam o monitor carregado o tempo todo, para ter na tela do console e em tempo real um diagnóstico de utilização e falhas do servidor. Prática não recomendada, uma vez que hackers com conhecimento suficiente podem ter acesso físico ao console do servidor...
- SERVMAN.NLM – outro utilitário com informações em geral sobre o servidor.
- DSREPAIR.NLM – utilitário para reparar e configurar o banco de dados NDS.

Segurança do sistema

O NetWare até a versão 3 possuía um modelo de segurança baseado unicamente nas configurações de login, atributos de arquivo e posterior ***trustee assignment***. A partir da versão 4, a Novell implementou um modelo de segurança baseado em cinco camadas, o que quer dizer que hackers e usuários mal-intencionados têm dificuldades adicionais de contornar as regras de acesso e acessar recursos não autorizados. As camadas são, em ordem:

- **Autenticação (usuário/senha)** – SYS:LOGIN verifica na base de dados NDS se o usuário está autorizado a entrar no sistema. Senão, necas de pitibiriba.
- **Restrições pessoais do usuário –** restrições aplicadas a cada usuário. Pode ser, por exemplo, em quais estações o usuário pode se logar, quais os recursos de rede autorizados para ele, horas e dias da semana permitidos, entre outros.
- **Segurança do NDS –** uma vez logado, e aplicadas as restrições acima, o usuário pode usar os recursos da rede. Entretanto, o NDS aplica ACLs (listas de controle de acesso) a cada objeto, seja ele usuários, impressoras, pastas ou programas. Trocando em miúdos, o NDS diz quem pode acessar cada um dos objetos, e com que direitos.
- **Segurança do sistema de arquivos** – o NDS pode definir quem tem direito de acessar cada servidor, e cada recurso no servidor. Além dessas restrições, em cada servidor, localmente, podem-se definir, arquivo por arquivo, as restrições de acesso – o que quer dizer que uma pessoa que contorne todas as três camadas acima fatalmente terá de contornar esta também.
- **Atributos de arquivo** – como em qualquer Unix e nos Windows, os arquivos podem ser marcados como apenas de leitura, escondidos, de sistema, inibição de cópias, compressão, criptografia... É a camada de mais baixo nível, a mais perto do hardware, no esquema de segurança NetWare.

Num sistema NDS (como em qualquer outro) a segurança depende não somente das tecnologias envolvidas, mas das práticas e políticas de segurança da empresa ou organização e mesmo da cultura de segurança dos usuários. Portanto, apesar de soluções como LDAP, ADS e NDS serem o estado da arte em autenticação e gerenciamento corporativo, é necessário ter um bom plano de como as informações confidenciais devem ser preservadas, e o acesso ao sistema, deve ser controlado.

Mais recursos sobre NetWare e NDS

Infelizmente, a Novell trata o conhecimento como seu mais caro produto e cobra preços exorbitantes a quem deseja compartilhar dele. Se for de seu interesse, procure o centro de treinamento autorizado Novell mais próximo e matricule-se em um curso preparatório para CNE – Certified Novell Engineer. Vale a pena: profissionais com CNE são muito valorizados.

Entretanto, alguns sites trazem informações interessantes sobre o NetWare. O primeiro deles é o próprio site de documentação oficial da Novell (www.novell.com/documentation), confuso mas com toneladas de informações interessantes. Com um pouco de garimpagem e um sistema NetWare de testes para brincar, é possível aprender muito.

Outra dica, desta vez para iniciantes, são os tutoriais do site TechTutorials (http://www.techtutorials.com/Novell/).

E, obviamente, o Google é seu amigo. ;-)