FNDE

Necessidade para auditar dados não estruturados e reforçar auditoria em serviços de rede como Active Directory e Exchange

FNDE
Fundo Nacional de Desenvolvimento da Educação

Introdução

- O FNDE é uma autarquia vinculada ao Ministério da Educação;
- Possui atualmente cerca de 2 mil funcionários internos usando estações Windows com Office e Servidor de Contas em plataforma MS Active Directory;
- Recebe acessos via internet de inúmeros clientes externos para os diversos Sistemas Corporativos;
- A TI do FNDE possui uma infraestrutura composta de 270 servidores Linux e Windows;
- Possui cerca de 170 departamentos internos, cada um usando uma pasta compartilhada em servidor de arquivos central totalizando cerca de 3TB de dados.
- O serviço de correio eletrônico atende a 3 mil caixas pessoais e corporativas.

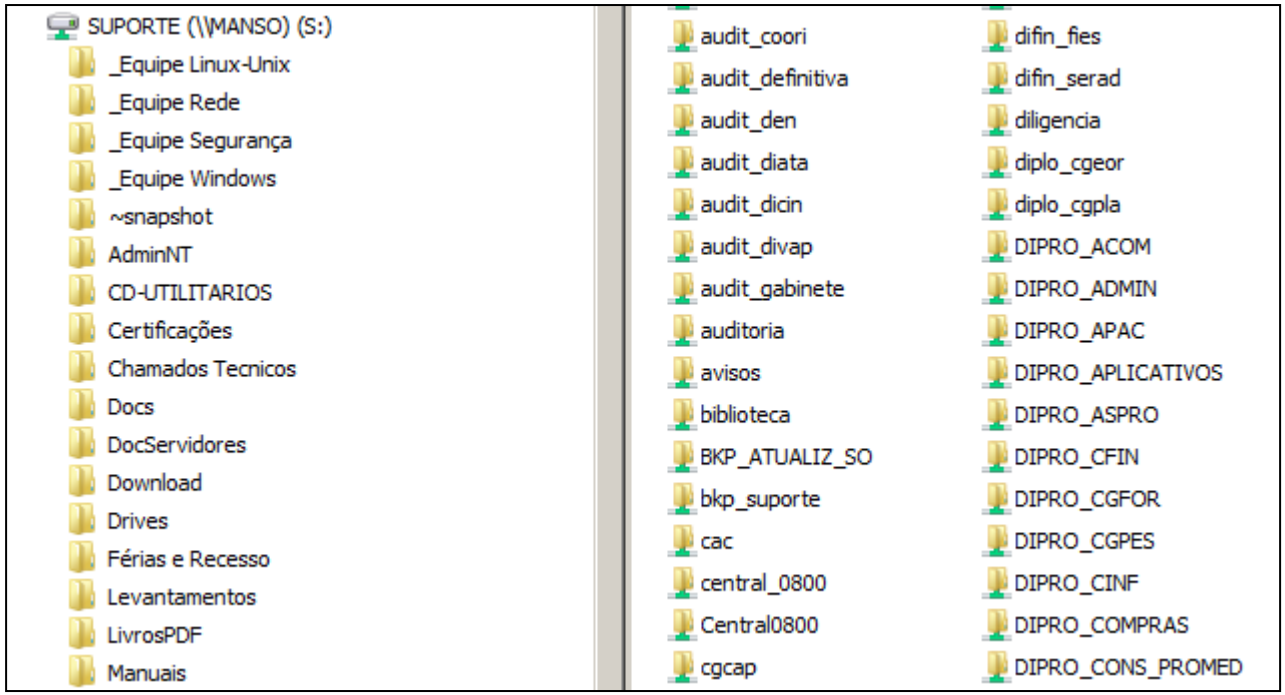
Introdução

O FNDE possui dados que estão espalhados em diversos pontos que são difíceis de monitorar e auditar, como:

I. Servidor de Arquivos;
II. Correio eletrônico;
III. Servidor LDAP (MS-Active Directory)

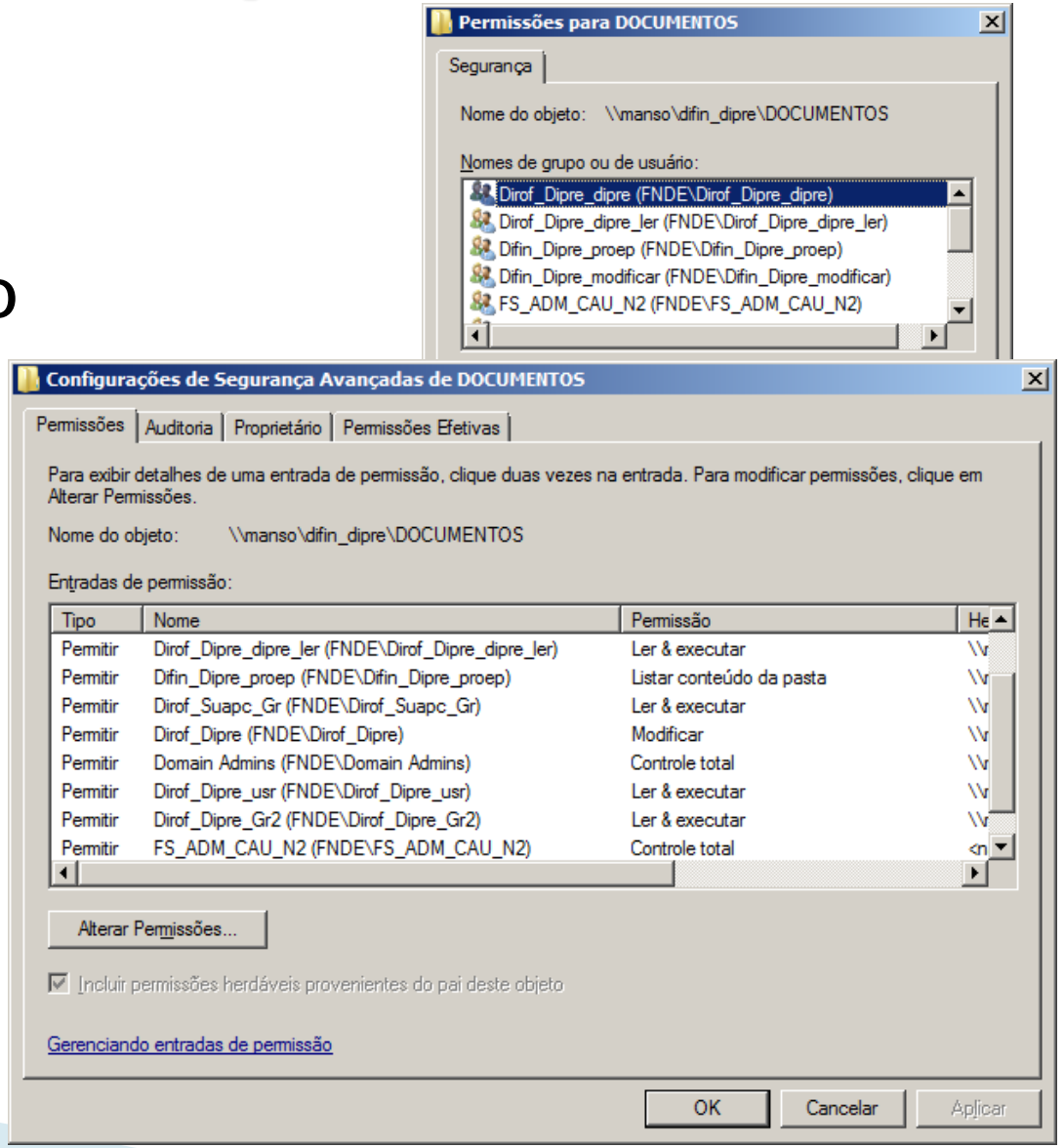
I – Servidor de Arquivos

- Cada departamento do FNDE possui inúmeras pastas compartilhadas no servidor de arquivos corporativo:



I – Servidor de arquivos

Cada pasta possui inúmeras formas de permissão de acesso com granularidades que dificultam o mapeamento da segurança e a operacionalização dos atendimentos.



FNDE
Fundo Nacional de Desenvolvimento da Educação

I – Necessidades para o Servidor de Arquivos

- Identificar excessos de permissões ou permissões desnecessárias;
- Identificar quem acessou (leu, excluiu, modificou) qualquer dado em pastas compartilhadas;
- Identificar quem alterou as permissões (ACL) nos objetos, pois existem muitos administradores de rede;
- Obter detalhamento da auditoria como: data, hora, estação de origem, usuário que acessou, objeto modificado, tipo de modificação;
- Armazenar auditoria por tempo determinado em servidor de banco de dados separado;
- Não usar auditoria interna do Windows;
- Facilitar aplicação de permissões com previsão de impacto.

II – Correio Eletrônico

- Serviço de rede crítico onde se trafega informações delicadas;
- Muitos negócios são fechados por meio do Correio Eletrônico;
- As mensagens eletrônicas possuem valor probatório e jurídico;
- Auditoria padrão do MS-Exchange é limitado (*tracking de mensagens*)

II – Necessidades para o Correio Eletrônico

- Identificar quem possui acesso às caixas de correio pessoais e corporativas;
- Auditar quem acessou determinada caixa: (enviou, apagou, encaminhou, usou 'em nome de')
- Auditar **de quem e para quem** a mensagem foi trafegada;
- Armazenar logs de auditoria em banco de dados separado;
- Armazenar auditoria por tempo determinado

III- Serviço de Active Directory (LDAP)

- Contas de usuários do FNDE de todos os níveis da hierarquia estão armazenados no AD;
- A administração dos diversos serviços de rede são integrados ao AD, como Servidor de Arquivos, Proxy, Correio Eletrônico, Estações de trabalho;
- Muitos administradores de rede possuem acesso ao AD com privilégios avançados.

III – Necessidades para o Active Directory

- Identificar as permissões nos objetos do AD de forma mais fácil e abrangente;
- Auditar quem modificou objetos, como: GPO, grupos e contas;
- Identificar acessos por data, hora, tipo de objetos;
- Armazenar os logs em local separado e de fácil manipulação (BD);
- Não utilizar logs padrão do Windows.

IV- Necessidades gerais

- Emitir relatórios em vários formatos amigáveis, como PDF, HTML, CSV;
- Possuir ferramenta de fácil manipulação e interatividade;
- Utilizar padrão Windows GUI;
- Possuir opção de Backup e Restore da ferramenta;
- Ter opção de alta disponibilidade do serviço de auditoria;
- Possuir suporte técnico em Brasília com atendimento remoto ou *on-site*.