Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Automatizando Serviços de Arquivos

(File Services)

Elaborador:	Gustavo Tinelli Martins
Orientador:	Maria Cristina Aranda

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

M343a MARTINS, Gustavo Tinelli

Automatizando serviços de arquivos (file services). / Gustavo Tinelli Martins. – Americana, 2019.

27f.

Relatório técnico (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Dra. Maria Cristina Aranda

1. Sistemas de informação 2. Segurança em sistemas de informação I. ARANDA, Maria Cristina II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: *681.518*

681.518.5

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

GUSTAVO TINELLI MARTINS

Automatizando Serviços de Arquivos (File Services)

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia - FATEC/ Americana.

Área de concentração: Segurança da Informação

Americana, 10 de junho de 2019.

Banca Examinadora:

Maria Cristina Aranda

Doutora

Fatec Americana

Marcus Vinícius Lahr Giraldi

Especialista

Fatec Americana

Benedito Aparecido Cruz

Mestre

Fatec Americana

SUMÁRIO

Lista de Figuras

1 Objetivo deste documento

O conceito de *file service* está diretamente ligado à sua nomenclatura, ou seja, serviço de arquivos. O tipo de rede responsável por disponibilizar esta função de *storage* é NAS (*Network Attached Storage*). Através de protocolos de comunicação como *Common Internet File System* (CIFS) e *Network File System* (NFS), o *hardware* é capaz de disponibilizar caminhos virtuais em redes públicas ou privadas que podem ser utilizados para armazenar qualquer tipo de arquivo. É comum que esta solução seja implementada nas empresas com o intuito de prover um ambiente de rede compartilhado, no qual os funcionários possam compartilhar e armazenar arquivos departamentais diversos.

Toda empresa, independentemente de sua proporção, necessita de um local para armazenar suas informações, sejam elas pessoais, profissionais, confidenciais, etc. A computação em nuvem é uma alternativa muito utilizada nas organizações atuais, com soluções *on demand* como *OneDrive*, *DropBox*, *Google Drive*, *iCloud*, *Amazon S3* entre outros. Porém muitas dessas soluções limitam-se ao puro armazenamento do dado, não proporcionando a possibilidade de estruturação de um ambiente arquitetado apropriadamente para o negócio em questão.

Baseando-se na afirmação acima, o intuito deste documento é explorar uma arquitetura desenvolvida para o armazenamento e a gestão dos dados empresariais, provendo opções de serviços para os usuários finais através de automações desenvolvidas em ferramentas como *PowerShell*, *Structured Query Language* (SQL), *Automation Bus*, entre outras. Essas automações, baseiam-se no processamento automático de solicitações de recursos de arquivamento feitas por usuários comuns, como pastas compartilhadas, gerenciamento de permissões e restauração de dados. A solução automática a ser analisada deve percorrer sequencialmente as seguintes etapas:

- Requisição de serviço de arquivo através de uma plataforma online
- Integração da plataforma com um banco de dados SQL
- Integração com a ferramenta de gestão de scripts em PowerShell
- Entrega do serviço solicitado ao usuário final

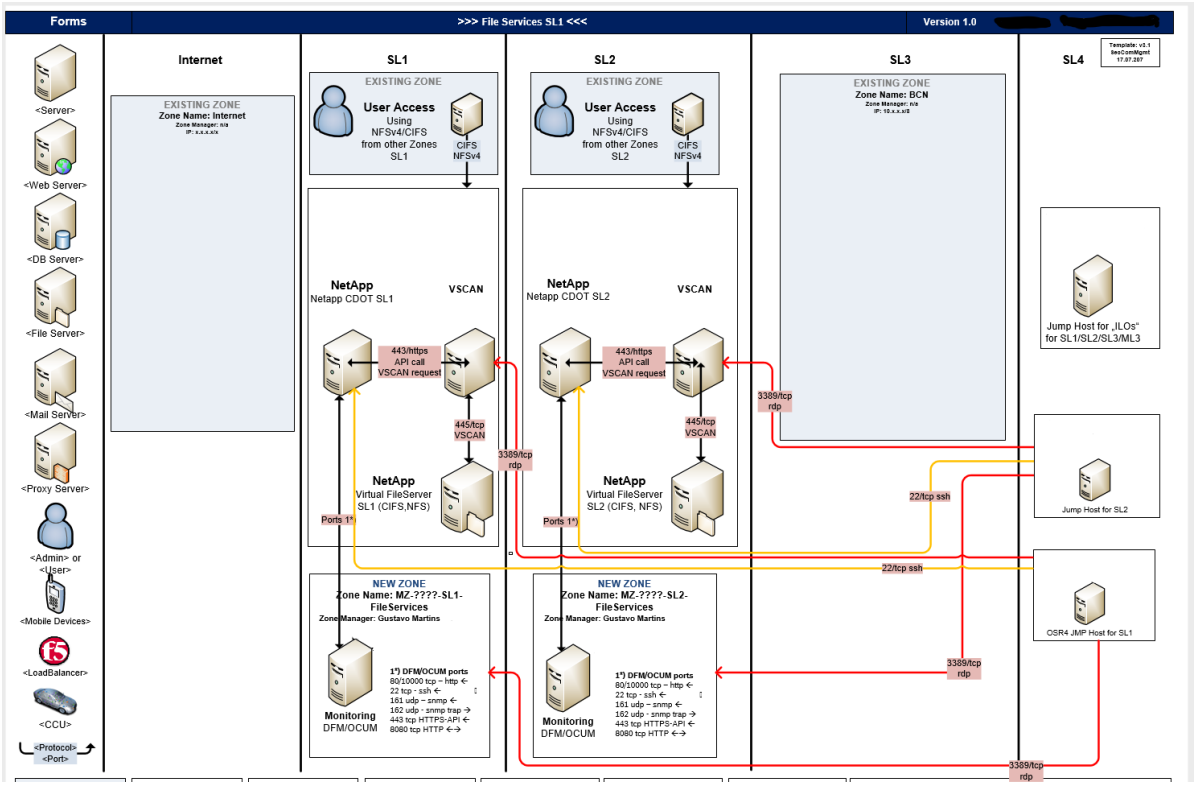
2 Desenvolvimento

Cada vez mais as organizações estão gerando uma enorme quantidade de dados que são recebidos a partir de várias fontes e armazenados de diferentes maneiras, o que demanda um processo de gestão específico para garantir a sua qualidade (VIANNA; DUTRA; FRAZZON, 2016).

Para o desenvolvimento deste projeto foi necessária a definição de uma arquitetura com equipamentos específicos, devido à complexidade de testes em diferentes ambientes e a dificuldade para obter todos os recursos que podem integrar uma solução desta magnitude.

A Figura 1 apresenta os dispositivos que integram a solução proposta neste documento. As subdivisões nomeadas como SL1, SL2, SL3, SL4 e Internet são segregações de rede com delimitações baseadas em regras de *firewall*. Os equipamentos em SL4 são *jump hosts* que possuem acesso as zonas SL1 e SL2, caracterizando uma possível arquitetura de *demilitarized* zone (DMZ). Dentro das zonas SL1 e SL2 estão todos os outros componentes, *storage Netapp*, servidor de antivírus, ferramenta de monitoração e interfaces de usuários, que serão descritos com maior clareza em itens subsequentes.

Figura 1 – Arquitetura do Ambiente



Fonte: Próprio autor

Em linhas gerais, o equipamento de armazenamento escolhido para o âmbito deste estudo foi o *Netapp Fabric Attached Storage* (FAS). A Netapp é líder de mercado no segmento de NAS há mais de 10 anos e possui reconhecimento como a tecnologia mais robusta para prover sistemas de arquivamento multiprotocolo.

Adjacentes ao equipamento físico, outros dispositivos foram integrados a solução, para monitoração ativa do ambiente e comunicação das automações com bancos de dados necessários.

2.1 Netapp – Família FAS

De acordo com a fabricante de mídias de armazenamento físico Seagate (2019), um sistema NAS é um dispositivo de armazenamento conectado a uma rede que possibilita o armazenamento e a recuperação de dados de um local centralizado para usuários autorizados da rede e clientes heterogêneos.

Conforme a retórica anterior, a Netapp lidera o mercado de NAS há muito tempo e por esse motivo foi escolhida para o estudo de caso, que visa não

só exemplificar o recurso de armazenamento como prover evidências da facilidade de implementação da solução.

Muitos modelos de *hardware* podem ser utilizados para prover um serviço de arquivamento eficiente e seguro, variando em aspectos lógicos relacionados à capacidade de espaço, de processamento e de escalabilidade.

Devido a quantidade exponencial de variações de modelos e aplicações para os mesmos, a família de equipamentos denominada *Fabric Attached Storage* (FAS) será alvo deste estudo. Os modelos da mesma estão apresentados na Figura 2.

Figura 2 – Modelos Netapp FAS

	Model	FAS9000	FAS8200	FAS2650	FAS2620
	Front View				
	Max Capacity Decimal | Binary	14.4PB | 12.8PiB	7.3PB | 6.5PiB	2.2PB | 1.95PiB	2.1PB | 1.9PiB
	Max System Cache Flash Pool + Flash Cache	144TiB	72TiB	24TiB	24TiB
	Max Aggregate Size	400TiB	400TiB	400TiB	400TiB
	Max FlexVol Size	100TiB	100TiB	100TiB	100TiB
	Max Cluster Nodes NAS | SAN	24 | 12	24 | 12	8 | 8	8 | 8
	Max Drive Quantity HDD | SSD	1440 | 480	480 | 480	144 | 144 24 int + 124 ext	144 | 144 12 int + 124 ext
Environmental All values based on HA configurations	Rack Units	8U	3U	2U	2U
	Weight English | Metric	214.5lb | 97.3kg	76.0lb | 34.5kg	58.64lb | 26.6kg	61.95lb | 28.1kg
	Amps[3] Typical | Worst-case	17.50 | 18.36 @100V 8.58 | 9.0 @200V	5.65 | 6.49 @100V 2.77 | 3.19 @200V	4.94 | 6.38 @100V 2.43 | 3.13 @200V	4.15 | 5.58 @100V 2.04 | 2.74 @200V
	BTU/hr[3] Typical | Worst-case	5854 | 6140 @100V 5738 | 6021 @200V	1888 | 2171 @100V 1850 | 2130 @200V	1652 | 2134 @100V 1622 | 2093 @200V	1386 | 1864 @100V 1359 | 1830 @200V
Specifications HA configurations	Processor	4x 64-bit 72 total cores	2x 64-bit 32 total cores	2x 64-bit 12 total cores	2x 64-bit 12 total cores
	Memory	1024GB	256GB	64GB	64GB
	NVRAM	64GB	16GB	8GB	8GB
	Expansion Slots	20x IO Modules	4x PCIe	-	-

Fonte: Netapp Hardware Universe, 2018

Todos os modelos desta família de equipamentos possuem um alto grau de escalabilidade, ou seja, possuem a capacidade de crescimento não disruptivo. Através da adição de gavetas de discos *Serial Advanced Technology Attachment* (SATA), *Serial Attached SCSI* (SAS) ou *Solid State Drive* (SSD) é possível expandir a capacidade de armazenamento e processamento dos dispositivos, permitindo variações que se adequem a diversos cenários de configuração.

O sistema operacional da Netapp é proprietário, conhecido como *Data Ontap*. É um sistema baseado em Unix que integra funções de armazenagem relacionadas a *Storage Area Network* (SAN) e NAS.

O mercado ainda disponibiliza suporte à versão legada desse sistema operacional conhecida como *7-mode*, que pode ser atualizada até a versão 8.2.X. A versão atual do SO é conhecida como *Clustered Data Ontap* (CDOT) e foi

disponibilizada para equipamentos seletos na versão 8.1. Atualmente todos os equipamentos são produzidos na nova versão e operam com as funcionalidades de alta-disponibilidade atribuídas a ela.

O *background* do desenvolvimento cronológico do sistema operacional faz-se pertinente para a compreensão de uma característica especifica do CDOT. Os servidores virtuais ou *Virtual File Servers* (vServers) funcionam como máquinas virtuais independentes e são responsáveis pela segregação lógica do Netapp, permitindo a coexistência de ambientes que disponibilizam diferentes serviços e utilizam diferentes recursos físicos, aumentando as opções de uso da solução.

Uma vez que o ambiente é particionado e os recursos são atribuídos, as configurações de *File Services* podem ser iniciadas através de dois protocolos, o *Common Internet File System* (CIFS) e o *Network File System* (NFS).

Apesar do mérito de analise deste documento estar relacionado à automação do processo de *File Services,* sem um processo automatizado a gerência das funcionalidades de arquivamento continua bastante simples. As unidades lógicas de armazenamento disponibilizadas através de pontos de montagem com os protocolos mencionados anteriormente são basicamente os recursos necessários para que o serviço esteja operante.

2.2 vSCAN – Servidor de Antivírus

Considerando o conceito básico da Symantec (2019) Antivírus é um *software* ou tecnologia usado para detectar aplicativos de computador mal-intencionados, impedir que eles infectem um sistema e limpar arquivos ou aplicativos que estejam infectados por vírus de computador.

Como parte do processo de automação é imprescindível a existência de um servidor de aplicação, no qual os serviços possam ser acionados e acionem os gatilhos necessários. O sistema operacional utilizado para o servidor neste caso de estudo é o *Microsoft Windows Server 2012 Standard*.

Uma das maiores preocupações de um ambiente de arquivos é a possibilidade de infecção do mesmo. Devido ao frequente manuseio dos dados por parte de usuários ou aplicações e as diferentes *interfaces* com dados de redes internas e externas, o ambiente de arquivos é uma das estruturas mais suscetíveis a contaminação por *softwares* maliciosos (*malware*).

Ciente da necessidade de um servidor de aplicação e de um *software* de antivírus robusto é pertinente que ambos operem em um mesmo dispositivo com capacidade de processamento compatível. Com isso, além de centralizar a operacionalização de agentes externos que possuem comunicação com o Storage, gera-se também uma economia na utilização de recursos, sejam eles lógicos, físicos, operacionais ou financeiros.

Para o estudo de caso, o *software* utilizado para o escaneamento dos dados armazenados no Netapp foi o Symantec. Além da interoperabilidade

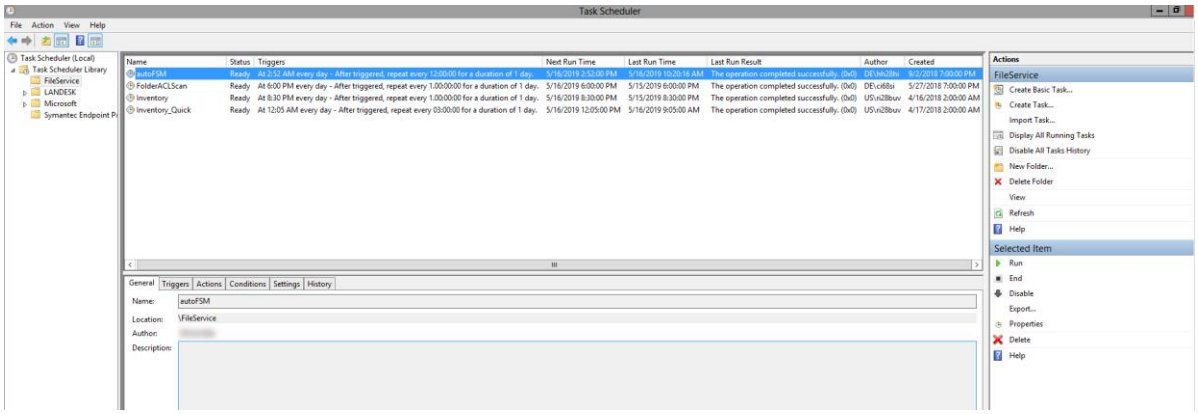
comprovada, o Netapp opera como um cliente do Symantec, ou seja, um mesmo servidor pode responsabilizar-se por mais de um Storage, dependendo da demanda computacional e da quantidade de dados a serem analisados. A Figura 3 apresenta a tela inicial do *Symantec Endpoint Protection*, o cliente da aplicação instalada no servidor.

Figura 3 – Symantec Endpoint Protection

Fonte: Próprio autor

Para o processo automático apresentado, existe a necessidade de criação de um inventário confiável, com dados relacionais de cada um dos equipamentos de *Storage* envolvidos, portanto os *scripts* de coleta destes dados, também rodam através do servidor de antivírus em tarefas agendadas. A Figura 4 mostra algumas tarefas de coleta agendadas no servidor.

Figura 4 – Tarefas agendadas dos scripts de coleta



Fonte: Próprio autor

2.3 OCUM – *OnCommand Unified Manager*

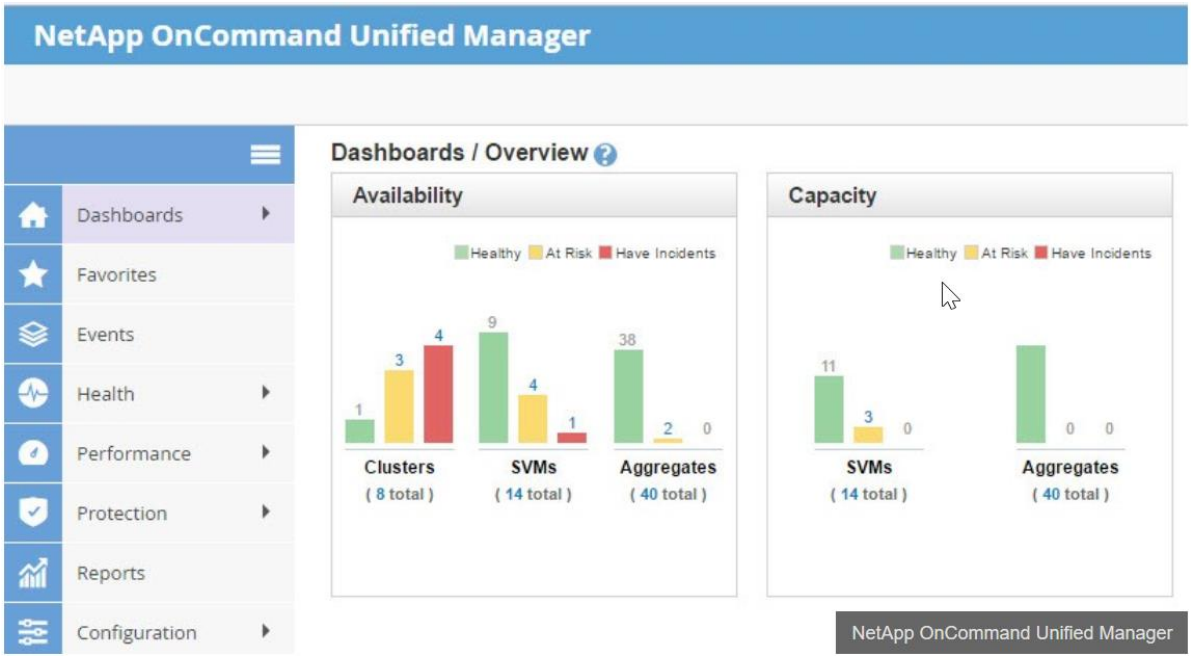
Ferramentas de monitoração são imprescindíveis para a gestão e segurança da informação. Monitorar eventos e logs faz-se necessário conforme recomendação do CertBR (2003), logs possibilitam o acompanhamento do que acontece com a rede e com os seus sistemas. Para tanto, é importante que eles sejam monitorados com frequência para permitir que eventuais problemas sejam rapidamente identificados.

Desde as primeiras versões do sistema operacional (SO) *Data Ontap* a Netapp disponibiliza uma interface gráfica de gerência e monitoração de seus equipamentos. Nas versões legadas, essa interface era integrada ao código e operava através de portas especificas como HTTPS (443).

Para o CDOT não há mais solução integrada. A Netapp deixou de ser apenas uma fornecedora de *hardware* e passou a prover serviços diversos, o que fez com que a mesma identificasse oportunidades de *cross-selling* com seu próprio portfólio de produtos. Apesar de muitos serviços internos dos equipamentos estarem associados a licenças integradas ao SO, *softwares* de monitoração, análise e gerenciamento são vendidos separadamente do *hardware*.

Um dos *softwares* mais conhecidos e utilizados da Netapp é o *OnCommand Unified Manager* (OCUM). Através de uma *interface* gráfica amigável é possível ter uma visão macro do ambiente em *dashboards* customizáveis e gerenciar a maioria dos objetos lógicos do sistema, com exceção de algumas ações destrutivas ou que demandem permissões avançadas ao ambiente. Alguns dos gráficos apresentados nos *dashboards* da aplicação estão expostos na Figura 5.

Figura 5 – *Oncommand Unified Manager Dashboard*



Fonte: Netapp Blog, 2017

2.4 *Jump Hosts*

Segurança da informação é um dos pilares da tecnologia, sendo responsável pela definição de múltiplos fatores decisivos durante o planejamento de uma infraestrutura. Assim como o plano de continuidade de negócios, plano de recuperação de desastres e a análise de risco em geral, as precauções com os métodos de acesso ao dado também devem ser consideradas.

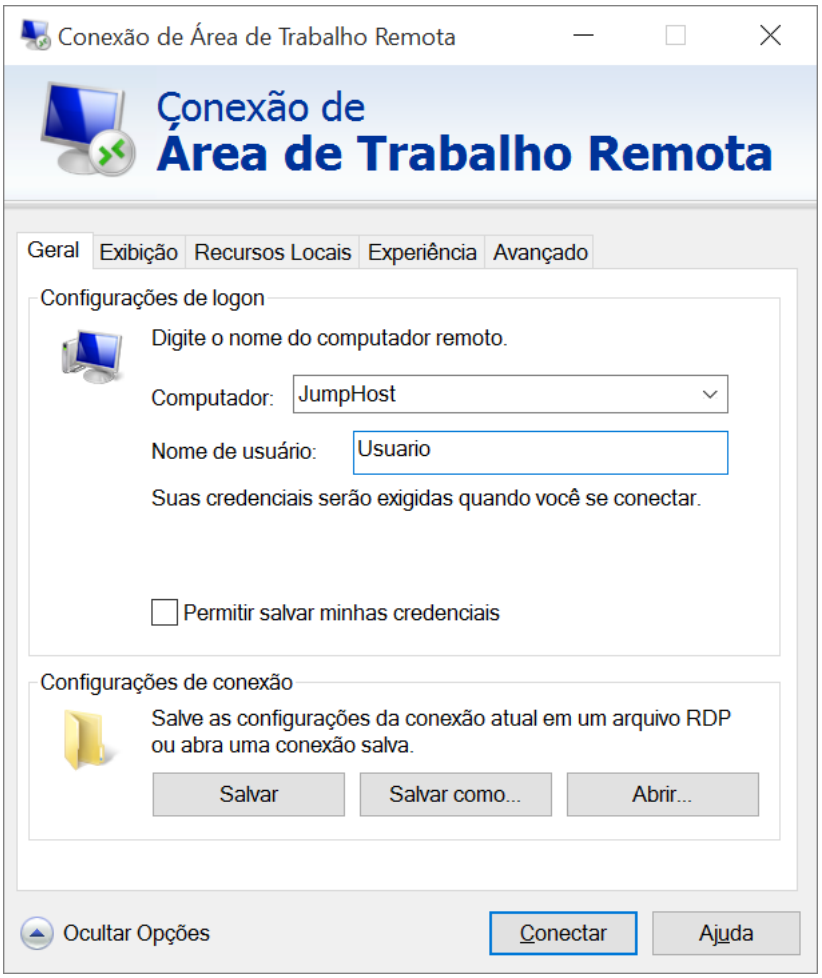
Em uma estrutura de rede que disponha de poucos recursos, é comum que a segregação do ambiente de infraestrutura e de acesso do cliente seja feita através de máscaras de rede ou distribuições de IPs em redes virtuais (VLANs), porém em soluções mais robustas, é comum que os dispositivos com acesso a rede dos equipamentos produtivos também sejam limitados.

De acordo com a Microsoft (2016), com a Conexão de Área de Trabalho Remota, é possível conectar-se a um computador com o Windows a partir de outro computador com o Windows que esteja conectado à mesma rede ou à Internet.

Os *Jump Hosts*, são servidores que podem acessar a rede na qual os equipamentos produtivos foram incluídos. Essa liberação de acesso para servidores específicos é feita através de regras de acesso em *firewalls* implementados entre ambas as redes. Os acessos aos servidores de conexão remota também são limitados, sendo gerenciados por times de segurança que determinam a real necessidade de acesso de um usuário àquele ambiente. Os *jump hosts* são comumente usados em soluções de DMZ, uma área de rede que

permanece entre a rede interna de uma organização e uma rede externa. Na Figura 1 os *jump hosts* estão na zona SL4. A Figura 6 apresenta a tela de conexão da Área de Trabalho Remota.

Figura 6 – Tela da Área de Trabalho Remota



Fonte: Próprio autor

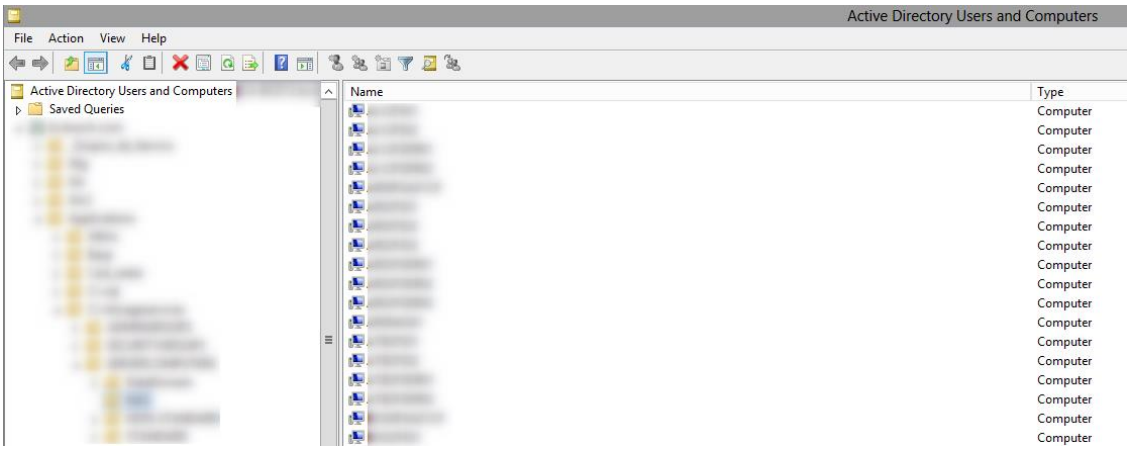
2.5 *Microsoft Active Directory*

A Microsoft (2017) define o *Active Directory* (AD) como uma estrutura hierárquica que armazena informações sobre objetos na rede. Um serviço de diretório fornece métodos para armazenar dados de diretório e disponibilizá-los para os administradores e usuários da rede.

O AD é uma ferramenta fundamental no processo de automação do sistema de arquivo. Sua primeira função é estabelecer uma comunicação entre o Netapp e a rede de arquivos através da criação de um objeto para cada máquina virtual e do uso deste objeto em uma configuração CIFS do lado do *Storage*.

Além de estabelecer a configuração necessária para que as unidades lógicas de arquivamento possam ser disponibilizadas, o AD também se responsabiliza pela armazenagem de grupos de acesso, determinando quais dispositivos ou usuários podem ter acesso em determinados caminhos na rede. A Figura 7 traz uma exemplificação de objetos de computadores no AD.

Figura 7 – Estrutura de objetos no *Active Directory*



Fonte: Próprio autor

2.6 *Microsoft SQL Server*

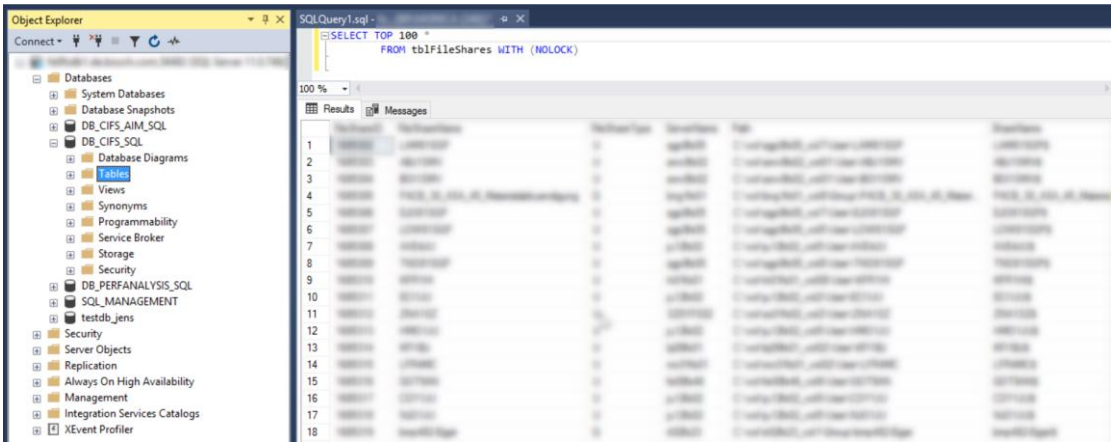
O *Microsoft SQL Server* é um sistema gerenciador de banco de dados relacional desenvolvido pela Microsoft.

Um banco de dados relacional formata os dados em tabelas, ou seja, é um ótimo recurso para organização de inventário e para consultas de automações que busquem informações especificas em campos singulares ou não.

O SQL Server nesta solução desempenha o papel de armazenamento dos registros que são gerados com a automação e também opera como base de dados para futuras consultas que populam as lacunas dos scripts desenvolvidos em *PowerShell*.

Através dos dados existentes nas tabelas do banco de dados, é possível fazer consultas complexas para identificar a data de criação da informação, a quem ela está atribuída, se houve alteração desde sua criação, etc. A Figura 8 traz exemplos de registros em uma tabela do banco de dados SQL.

Figura 8 – Tela do banco SQL no *Microsoft SQL Server Management Studio*



Fonte: Próprio autor

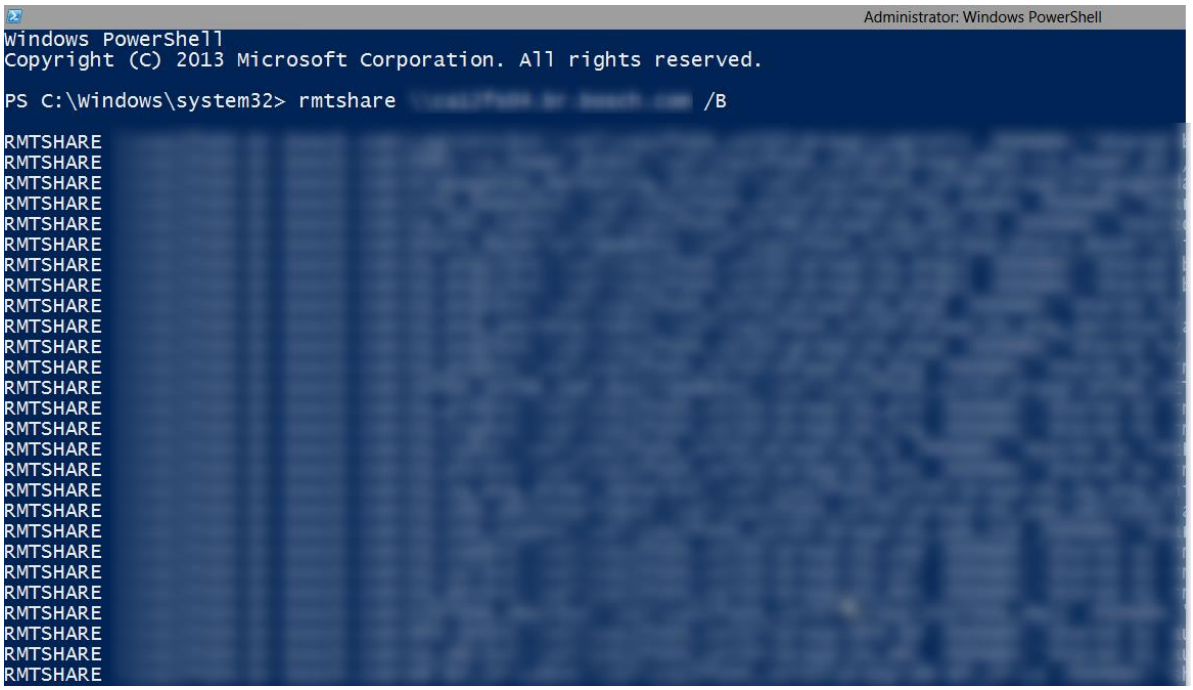
2.7 *Windows PowerShell*

De acordo com a Microsoft (2017) o *PowerShell* é uma *interface* de linha de comando do Windows desenvolvido especialmente para administradores do sistema. O *Windows PowerShell* inclui um *prompt* interativo e um ambiente de *script* que pode ser usado independentemente ou em conjunto.

O *PowerShell* apresenta o conceito de um cmdlet, uma ferramenta de linha de comando de função única simples integrada ao *shell*. Cada cmdlet pode ser utilizado separadamente, mas seu potencial é atingido quando essas ferramentas simples são utilizadas em conjunto para realizar tarefas complexas. A ferramenta inclui mais de uma centena de cmdlets principais e permite que cmdlets proprietários sejam criados e compartilhados com outros usuários.

A Netapp possui seu próprio conjunto de cdmlets, ou seja, através da *interface* de linha de comando do *PowerShell* é possível rodar comandos que interagem diretamente com comandos nativos do Netapp. Devido a essa compatibilidade, a ferramenta da Microsoft é considerada por muitos o recurso mais prático para o desenvolvimento de automações relacionadas a serviços de arquivamento. A Figura 9 traz a interface do Windows *PowerShell* sendo utilizada para visualizar a estrutura de permissão de *File Shares*, através de um recurso do Windows não desenvolvido especificamente para instruções no Netapp.

Figura 9 – Windows *PowerShell*



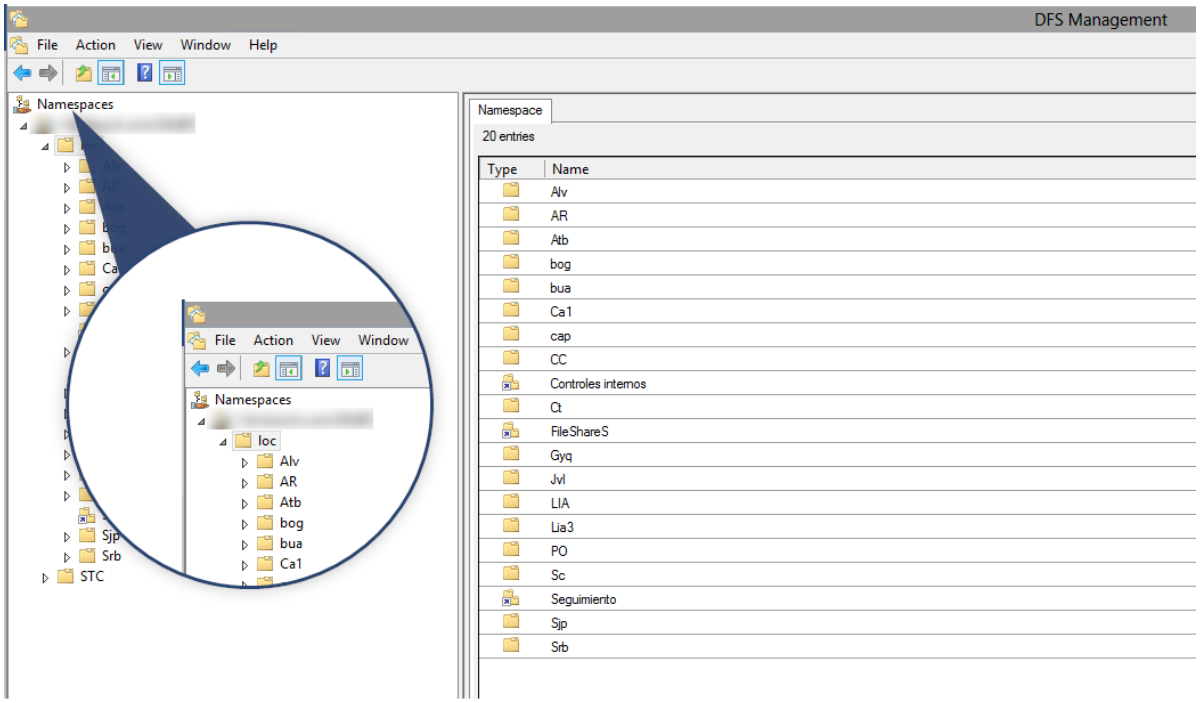
Fonte: Próprio autor

2.8 *Distributed File System* (DFS)

As funções do *Distributed File System* (DFS) fornecem a capacidade de agrupar logicamente os *shares* (pastas compartilhadas) em vários servidores e vincular de forma transparente os compartilhamentos em uma única estrutura hierárquica de nomes. O DFS organiza recursos compartilhados em uma rede com uma estrutura semelhante a uma árvore.

A automação via *PowerShell* também possui cmdlets que gerenciam a aplicação de DFS, porém a função do DFS é criar uma camada virtual sobre as estruturas de diretório, que permitam alterações no *background* de maneira não disruptiva para o usuário. Na Figura 10 é exposta a estrutura de *Namespace*, ou seja, do ambiente virtual proporcionado via DFS. Na Figura 10 são apresentados os *links* de DFS de um determinado *Namespace*.

Figura 10 – Estrutura Virtual do DFS



Fonte: Próprio autor

Um DFS *Link* é um apontamento virtual para um caminho na rede, disponibilizado através de um servidor de arquivos, seja ele local ou externo através de um equipamento de *Storage*.

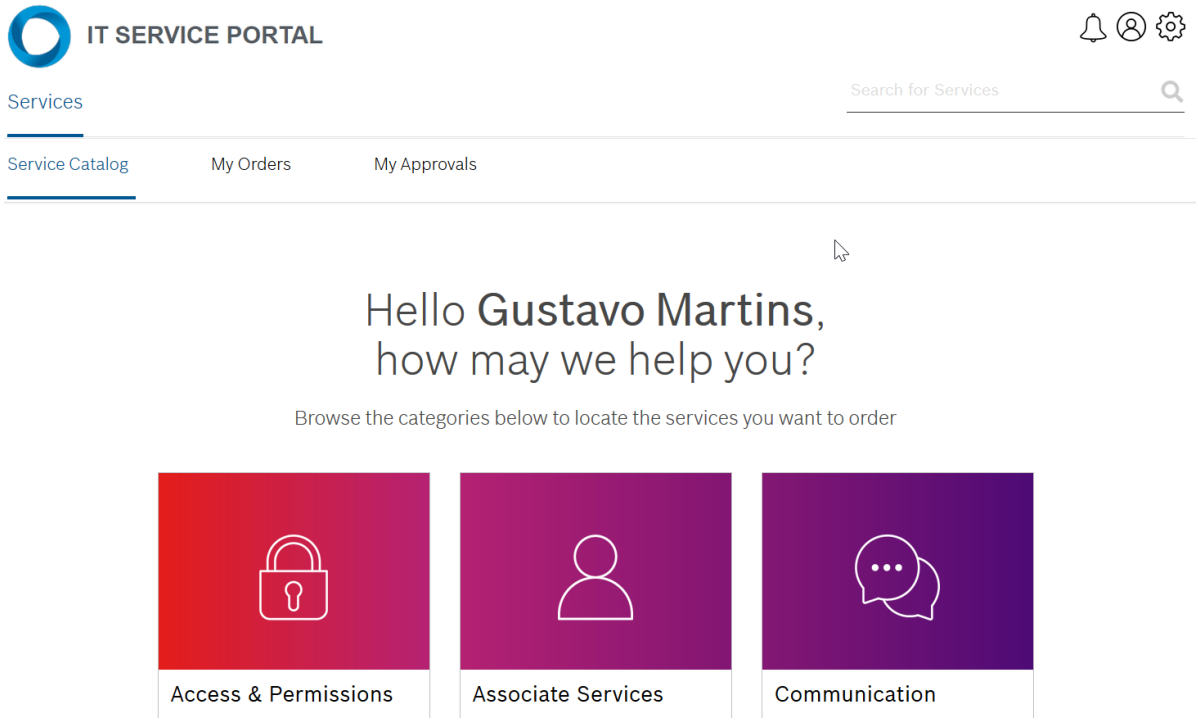
2.9 Portal de Serviços

O Portal de Serviços é uma plataforma *online* desenvolvida única e exclusivamente para a solicitação de serviços através de formulários, que capturam o conteúdo inserido pelo usuário e populam com estes dados tanto os *scripts* de automação em Powershell, quanto o banco de dados SQL.

Esta plataforma encontra-se na rede interna do cenário em análise mas poderia ser disponibilizada em uma rede interna com diferentes customizações.

Existe uma gama considerável de opções de serviço no portal e entre eles estão os serviços de arquivo. As opções variam de acordo com a necessidade do usuário e podem ser solicitadas massivamente em cenários específicos que serão descritos nos itens subsequentes. A tela inicial do Portal de Serviços pode ser visualizada na Figura 11.

Figura 11 – Portal de Serviços



Fonte: Próprio autor

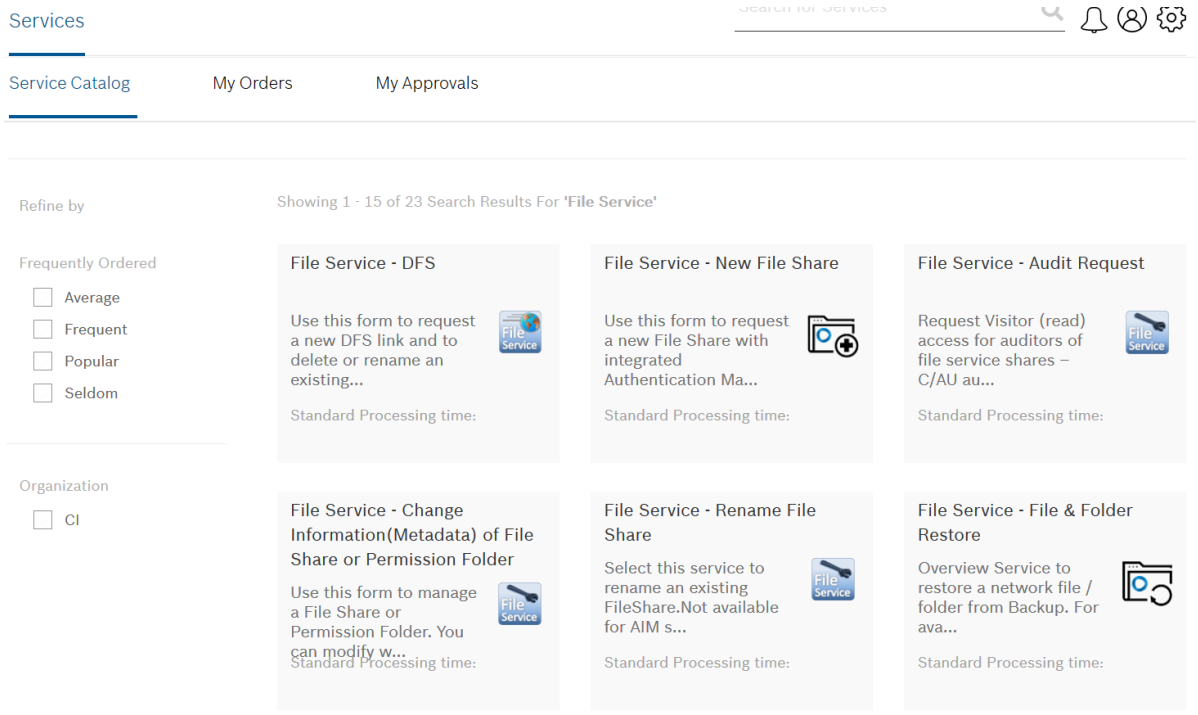
2.10 Solicitando um Serviço

Cada serviço possui um formulário único a ser preenchido com dados pertinentes à automação que o mesmo deve iniciar. Quando um usuário precisa de um serviço de arquivamento, o mesmo pode buscar pelos formulários no Portal de Serviços e solicitar pessoalmente.

Cada formulário possui um fluxo de inicialização diferente atrelado a sua criticidade e potencialidade de disrupção, ou seja, uma solicitação de serviço que possa alterar o modelo de negócio ou gerar algum impacto na produtividade da empresa passa por um fluxo de aprovação.

Após o a submissão da solicitação, um gatilho lógico aciona um *runbook* (um arquivo com uma sequência de *scripts* para pequenas tarefas) armazenado em uma ferramenta de automação conhecida como *Automation Bus*. Estes *scripts* são responsáveis pela execução das tarefas que levarão à entrega do serviço solicitado.

Figura 12 – Formulários de Serviços



Fonte: Próprio autor

2.11 Criação / Deleção de *File Share*

Para dar continuidade à análise da automação e suas funcionalidades, é preciso que haja compreensão do conceito de *File Share* e *Permission Folder.*

A função de um servidor de arquivo é disponibilizar caminhos de rede que possam ser acessados de maneira simultânea por múltiplas sessões e que possam ser gerenciáveis em diversos níveis, tais quais, segurança, capacidade e poder computacional.

Um *File Share* é um ponto de montagem que aponta para um espaço lógico alocado em um disco físico, ou seja, uma porção do disco é separada logicamente e disponibilizada através de um caminho de rede ao usuário ou aplicação. Em termos gerais, pode ser definido como uma pasta compartilhada.

Uma *Permission Folder* ou pasta de permissão é uma pasta comum criada em um sistema de arquivos que possui permissões de *New Technology File System* (NTFS) ou Unix atribuídas a ela. Nesse caso, mesmo que a pasta seja compartilhada, sua permissão de compartilhamento (*share*) e local podem ser completamente diferentes, predominando sempre a mais restritiva.

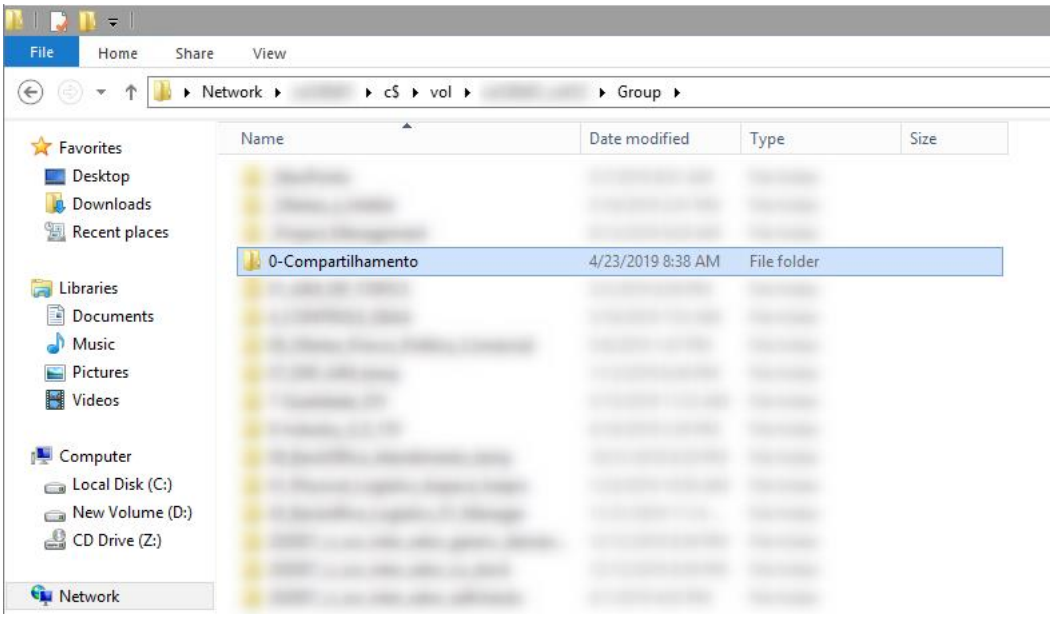
A Figura 13 mostra o caminho lógico de um *file share* criado no Netapp enquanto a Figura 14 traz um exemplo de uma pasta de permissão comum.

Figura 13 – *File Share* no Netapp

```
Vserver         Share          Path                Properties Comment  ACL
--------------- -------------- ------------------- ---------- -------- -----------
[redacted]      0-             /vol/[redacted]     oplocks    shared   Everyone / Change
                Compartilhame  vol12/Group/0-      browsable  by       [redacted] / No access
                nto$           Compartilhamento    changenotify
```

Fonte: Próprio autor

Figura 14 – Pasta de Permissão no Windows



Fonte: Próprio autor

Quando um *File Share* é solicitado através do portal de serviços, as informações são armazenadas em um arquivo de texto, enviadas para um caminho de leitura da aplicação e um gatilho de acionamento inicializa o *runbook* desta solicitação. Um e-mail de aprovação é enviado para o gestor da área para a qual a pasta compartilhada é solicitada. Caso a solicitação não seja aprovada, a condição de continuidade não é atingida e o processo no *Automation Bus* é interrompido enviando uma mensagem para o requisitante sobre a falha.

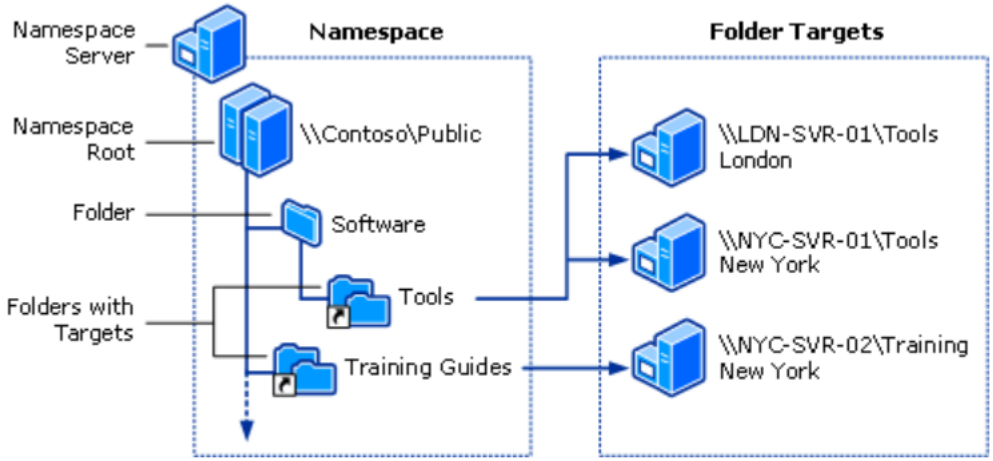
Uma requisição aprovada supre as condições de sequência e inicializa um *script* com comandos de *PowerShell* para a criação da Pasta de Permissão e do *File Share*.

Com a pasta e o *share* criados, um próximo *script* com comandos nativos do Windows interage com o *Active Directory* e crias dois grupos de permissão no domínio da rede, um de escrita e um de leitura. Existem outros tipos de permissões viáveis, porém, para simplificar a tratativa dos casos de problemas de acesso, é aconselhável que as opções sejam as mais limitadas possíveis. Dentro desses grupos são inseridos os usuários que terão acesso às pastas via

NTFS, uma vez que a permissão do compartilhamento permitiria acesso total a qualquer visitante.

Posterior à criação dos grupos de acesso, a pasta compartilhada recebe uma atribuição de um caminho virtual na estrutura de DFS. Está atribuição permite que a visualização do nome da pasta na rede seja diferente da nomenclatura dada à pasta anteriormente, ou seja, uma pasta de permissão com o nome “Teste_*Share*_1” pode ser visualizada como “Teste_1” na estrutura virtual de DFS. Esse recurso é utilizado para que mudanças nos caminhos de rede possam ser alterados superficialmente, sem afetar os compartimentos de dados. A Figura 15 demonstra algumas formas de atribuição de DFS *Links* a pastas de destino.

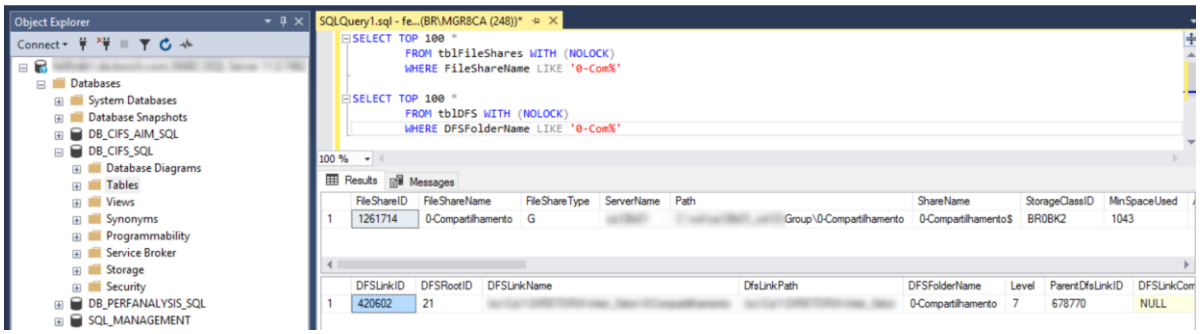
Figura 15 – Atribuição de DFS *Links* a Pastas



Fonte: Microsoft, 2018

Todas as informações geradas através da execução dos *scripts* são armazenadas e salvas diretamente em um banco de dados SQL para futuras consultas. A Figura 16 mostra a execução de uma busca especifica no banco de dados SQL que resulta na exposição de um registro válido dentro de uma tabela.

Figura 16 – Demonstração de registro no banco SQL



Fonte: Próprio autor

Além da criação, também é possível que a deleção seja executada de maneira automática. O gatilho que inicializa as instruções também é a baseado na submissão da solicitação por parte do requisitante e da aprovação do responsável pela pasta que será deletada. A quantidade de *scripts* que são executados de forma sequencial é semelhante à da criação, pois o processo é operado de modo reverso.

O registro de um *File Share* nunca é deletado do banco de dados SQL, permitindo que toda a estrutura de arquivo seja passiva de auditoria.

2.12 Criação / Deleção / Renomeação de DFS Link

Conforme mencionado anteriormente, a premissa de uso de uma camada adicional de estrutura de arquivo baseia-se na possibilidade de realizar alterações no caminho de rede sem gerar impacto para a continuidade do negócio.

É comum que durante o processo de organização de uma estrutura de dados, erros sejam cometidos. Por vezes o DFS *Link* é criado em uma parte errônea do caminho de rede e precisa ser excluído para ser recriado em seguida, porém a automação em estudo não trata esta situação como uma ocorrência única.

Para que um DFS *Link* seja recriado, duas solicitações de serviço são necessárias. Uma para que o *link* seja deletado e outra para que o mesmo seja recriado corretamente. Existe também a possibilidade de renomear o *link* caso o mesmo esteja atribuído ao cominho de rede correto.

Os *scripts* para requisições de DFS operam principalmente com comandos da própria aplicação (dfscmd). Utilizando as informações providas pelo requisitante o comando de associação ou remoção do DFS *Link* é criado e iniciado.

Os passos de renomeação de um DFS *Link* também envolvem excluir e recriar o mesmo, porém o fato de não alterar seu caminho, permite que todos os passos sejam executados dentro de um mesmo bloco de programação.

2.13 Criação / Deleção de Permission Folder

As *Permission Folders* ou as pastas de permissão possuem uma característica própria relacionada à atribuição das permissões NTFS no nível da própria pasta e não de seu compartilhamento. Essas pastas também são conhecidas como pontos de controle de acesso, pois determinam em qual nível do caminho da rede os acessos serão determinados.

A função das pastas de permissão na estrutura deste estudo de caso é voltada ao conceito de organização do ambiente de arquivo.

O Netapp permite que múltiplos pontos de compartilhamento (*shares*) sejam criados para uma mesma pasta ou para pastas em níveis inferiores no caminho da rede, o que, do ponto de vista organizacional dificulta a identificação e a auditoria dos dados que são inseridos na rede. Por exemplo, se há uma pasta de permissão com dois compartilhamentos apontados para ela, pode-se ter dados de finalidades distintas sendo inseridos em caminhos virtuais diferentes, mas sendo escritos em uma mesma compartição lógica do *Storage*.

Para que não haja problemas de duplicidade ou qualquer outro problema derivado da pluralidade de opções organizacionais disponíveis, a automação estabelece uma regra de criação de pastas de permissão sem atribuição de DFS *Links* no caminho da rede e sem *share* associado a elas. Quando um usuário acessa um *share* ou um DFS *Link* na rede, as pastas de permissão abaixo dos mesmos são apresentadas e operam como ponto de controle de acesso. Dentro das pastas de permissão, todas as permissões são herdadas da pasta “pai”.

O *script* de criação de uma pasta de permissão baseia-se em comandos nativos do sistema operacional tanto para a criação, quanto para a atribuição dos acessos as pastas. Quando o usuário submete uma solicitação via Portal de Serviços a mesma é aprovada pelo dono da área à qual a pasta será atribuída.

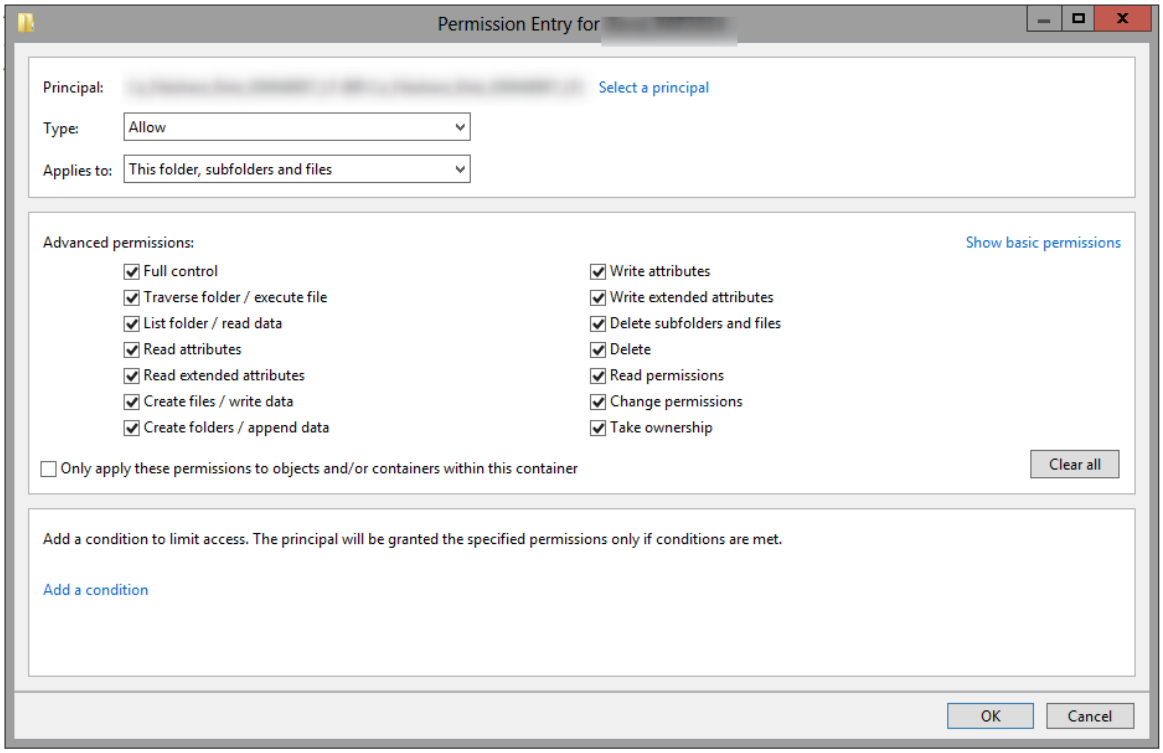
Para deletar uma pasta de permissão o procedimento pode ser iniciado pelo Portal de Serviços através da automação (recomendado), porém é possível que o usuário com acesso à pasta também possa deletá-la. O problema é que para a automação não há registro de um *script* rodando, portanto, a única evidência restante passa a ser um escaneamento do banco de dados antes e depois da deleção.

2.14 Inclusão / Remoção de Acesso a *File Share* ou *Permission Folder*

A inclusão ou remoção de acesso NTFS (não do nível do *share* em si) de um *File Share* ou *Permission Folder* podem ser solicitadas concomitantemente, ou seja, a automação permite que através do preenchimento de um único formulário no Portal de Serviços, acessos possam ser removidos ou atribuídos a qualquer usuário ou grupo de acesso presente no domínio da rede.

Conforme mencionado anteriormente, as permissões podem variar de muitas maneiras caso não haja uma restrição proposital. A Figura 17 traz todas as opções disponibilizadas na tela de permissões avançadas do Windows. Cada uma das opções marcadas representa uma característica de acesso, possibilitando combinações variadas que supram as mais diversas necessidades de negócio.

Figura 17 – Tela de permissões avançadas do Windows



Fonte: Próprio autor

Cientes da dificuldade de gerenciamento e identificação de problemas de um ambiente mais complexo, a automação permite apenas que dois tipos de permissão comuns sejam atribuídos aos usuários, “leitura e execução” ou “modificação”. No formulário, as definições foram renomeadas para visitantes e membros, no intuito de facilitar a interpretação de usuários leigos.

Exclusivamente para os administradores do sistema é permitido acesso total e irrestrito aos objetos da rede de arquivos. Apesar de operações manuais serem possíveis devido a essa liberação, apenas em casos extremos as permissões não serão gerenciadas por *scripts*.

No formulário de requisição ainda existe a possibilidade de definir datas de expiração para acessos temporários, que utiliza o horário da localidade interpretada pelo banco de dados SQL, ou seja, é possível utilizar o horário local e

não apenas um fuso horário, o que se torna muito útil para auditorias, que demandam acessos aos auditores por períodos determinados para análise.

O *script* de atribuição de permissões às pastas e *shares* fazia uso de comandos como "*subnacl*" e "*icacls*" para uma rápida alteração na pasta solicitada via formulário, porém devido à reestruturação de segurança que compõe a automação aqui descrita, o *script* foi alterado para que o mesmo seja capaz de fazer alterações internamente em grupos do *Active Directory*, utilizando comandos como "*ADD-ADGroupMember*".

Este serviço também solicita a aprovação do responsável pela pasta na qual o acesso está sendo solicitado.

2.15 *Restore* de Arquivos ou Pastas

Uma das automações mais complexas é a de *restore* e para que haja compreensão de sua funcionalidade é necessário que sejam explicadas as políticas de *backup* que permitem o uso deste recurso.

O Netapp permite formas variadas de *backup* que não serão objetos deste estudo em sua totalidade, portanto, as formas pertinentes de análise são através de *snapshots* e *snapmirrors*.

Todo dado armazenado no *Storage* é replicado para uma localidade remota, que apesar de não estar discriminado explicitamente na ISO 22301, orienta-se que esteja a pelo menos 50Km de distância da localidade primária do dado de origem. O método de movimentação de dado que permite este tipo de replicação é chamado de *snapmirror* pela Netapp.

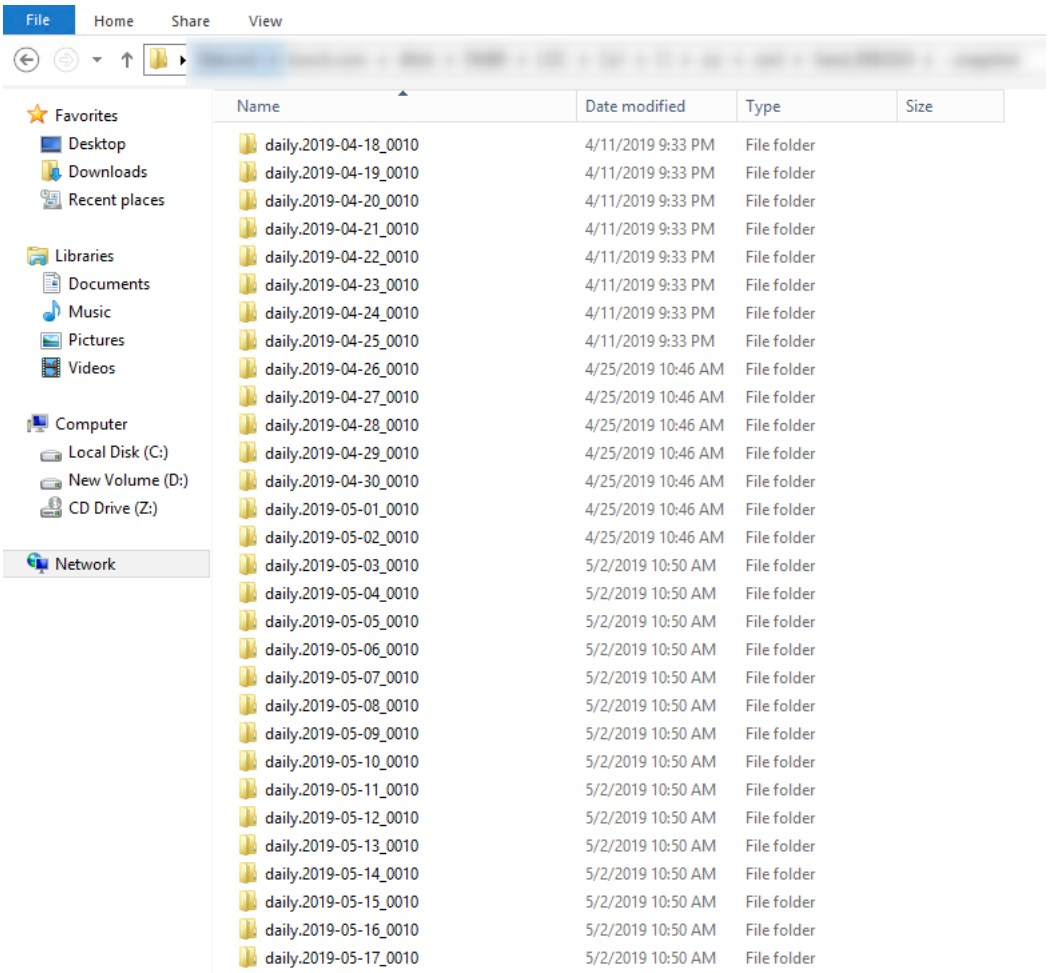
Além da replicação para outras localidades, existe uma função de cópia interna chamada *snapshot*. O *snapshot* não copia os dados literalmente, na verdade o que é copiado são os ponteiros para os blocos com determinada informação no disco, portanto, as cópias possuem um consumo de espaço relativamente baixo.

A automação é capaz de utilizar qualquer uma das cópias, tanto a remota quanto a local, porém a remota só será utilizada em caso de algum desastre, fazendo com que a cópia local seja a principal ferramenta para a execução automática de uma restauração de dados neste cenário.

A quantidade de cópias de um determinado volume de dados no Netapp pode ser de até 255, porém é comum que sejam determinadas quantidades menores, como 30, 60 ou 90. Isso ocorre, pois, a maioria das cópias locais são criadas com o intuito de possibilitar a restauração de dados que foram removidos ou alterados nos últimos 3 meses. Os *snapshots* podem ser únicos ou podem ser agendados para rodar de hora em hora, diariamente, semanalmente, etc...

Para o estudo de caso, considera-se a criação de cópias diárias dos últimos 30 dias, conforme a listagem de snapshots apresentada na Figura 18.

Figura 18 – Lista de cópias de *Snapshot*



Fonte: Próprio autor

Como o caminho e a nomenclatura dos *snapshots* são padronizados, é possível para a automação que através de uma análise comparativa no banco de dados, a mesma identifique o arquivo ou pasta que deve ser restaurado.

No formulário de restauração de Portal de Serviços, os únicos dados solicitados são o nome do arquivo ou pasta a ser restaurado e o caminho na rede onde o dado estava anteriormente à deleção ou modificação do mesmo. Com estes dados, a automação é capaz de utilizar uma ferramenta de cópia do Windows chamada "*robocopy*" para restaurar o dado na mesma localidade sem sobrescreve-lo.

3 Resultados

O estudo de caso descrito no presente documento, demonstra a viabilidade do processo de automação de um ambiente de serviços de arquivamento.

Além de esclarecer um possível método de implementação é possível obter valores numéricos de melhoria relacionados a tempo e qualidade do serviço.

Antes da implementação do processo de automação, os serviços variavam de 30 minutos a 24 horas para implementação em um fluxo normal de aprovação, porém esse tempo podia tornar-se ainda maior devido a quantidade de interações humanas que eram necessárias e dependiam da disponibilidade dos profissionais. Com o processo automático em vigência, qualquer um dos serviços aqui apresentados, podem ser realizados em 10 minutos e quase sem interação humana.

Além da redução de tempo, a automação do serviço de arquivamento possibilitou a otimização de um padrão do ambiente, que facilita tanto a compreensão do usuário requisitante quanto do administrador do sistema. A centralização do canal de solicitação de serviço também diminui a quantidade de possíveis pontos de falha durante a requisição de um recurso.

O tempo de análise de problemas também foi reduzido exponencialmente, liberando os administradores do sistema para funções que possuem real necessidade intelectual, como o desenvolvimento de novas aplicações e a criação de novos serviços que beneficiem o cliente.

4 Conclusões e considerações finais

Os processos automáticos tendem a facilitar a interação do usuário com a máquina e garantem um nível maior de satisfação com o serviço prestado, portanto é de extrema valia que o conteúdo deste documento não seja visto como regra e que outros recursos estejam sob constante análise para o desenvolvimento de novas soluções.

O estudo foi viabilizado através de um ambiente físico, o que em um cenário real de implementação parte do pressuposto da existência da infraestrutura necessária, porém, é totalmente viável que uma solução semelhante a exposta seja desenvolvida em um ambiente de nuvem.

A migração de processos manuais para processos automatizados é uma realidade na maioria das empresas. Um dos maiores desafios é enxergar a aplicabilidade de um processo automático, portanto, é notório o crescimento da busca por profissionais capazes, que tenham conhecimentos em áreas como *design thinking, big data* e computação em nuvem.

Perante a análise final dos dados provenientes da criação deste documento, é possível afirmar que o desenvolvimento de novos serviços está baseado na interpretação de necessidades e na exploração de todos os seus vieses, gerando protótipos de melhorias que possam ser traduzidos em processos automáticos que entreguem valor ao cliente.

Conforme expressado no intuito inicial deste documento, toda a arquitetura desenvolvida para elucidar a aplicabilidade das automações nos processos de solicitação e execução de serviços de arquivos foi explorada, demonstrando a especificidade e eficiência do estudo embasado em pesquisa e posterior estudo de caso relacionado.

REFERÊNCIAS BIBLIOGRÁFICAS:

CertBR - Disponível em https://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#subsubsec4.4.3 Acesso em: 15 maio 2019

MICROSOFT - Disponível em https://docs.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview Acesso em: 13 de abr. 2019

MICROSOFT – Disponível em https://docs.microsoft.com/pt-br/powershell/scripting/getting-started/getting-started-with-windows-powershell?view=powershell-6 Acesso em: 14 abr. 2019

MICROSOFT - Disponível em https://support.microsoft.com/pt-br/help/17463/windows-7-connect-to-another-computer-remote-desktop-connection Acesso em: 16 maio 2019

MICROSOFT - Disponível em https://docs.microsoft.com/pt-br/windows-server/storage/dfs-namespaces/dfs-overview Acesso em: 22 maio 2019

NETAPP - Disponível em https://hwu.netapp.com/Resources/Posters/HWU-2017-NA00-0494-000-000.pdf Acesso em: 22 maio 2019

NETAPP - Disponível em https://blog.netapp.com/blogs/netapp-oncommand-unified-manager-7-2-data-management-simplified/ Acesso em: 25 mar. 2019

NETAPP - Disponível em https://www.netapp.com/us/documentation/fas-storage-systems.aspx Acesso em: 16 maio 2019

SEAGATE - Disponível em https://www.seagate.com/br/pt/tech-insights/what-is-nas-master-ti/ Acesso em: 22 abr. 2019

SNIA - Disponível em https://www.snia.org/sites/default/education/tutorials/2007/fall/storage/WolfgangSinger_%20NAS_and_ISCSI_Technology.pdf Acesso em: 22 abr. 2019

SYMANTEC - Disponível em https://www.symantec.com/connect/blogs/basic-concepts Acesso em: 05 maio 2019

VIANNA, William Barbosa; DUTRA, Moisés Lima; FRAZZON, Enzo Morosini. Big data e gestão da informação: modelagem do contexto decisional apoiado pela sistemografia. **Informação & Informação**, v. 21, n. 1, 2016.