Manual de utilizador – Sistema de Armazenamento Central AFS

O acesso ao sistema de armazenamento central AFS pode ser efetuado de duas formas diferentes:

- por cliente, através de um determinado sistema operativo (Windows, Linux, Mac OS)
- através do cluster sigma.

Acesso pelo cluster sigma

O cluster sigma utiliza como área de trabalho dos utilizadores a área de AFS central. Deste modo, o acesso à área de AFS é transparente para os utilizadores do cluster sigma, os quais têm acesso a esta área de forma análoga à que ocorre num acesso convencional aos diretórios de trabalho de um sistema Unix/Linux. Neste caso, temos acesso à área pessoal do AFS quando é feito login no cluster por ssh, sendo as configurações necessárias processadas de forma transparente durante o processo de login.

Este facto permite que qualquer utilizador com o serviço de shell ativo possa transferir ficheiros de/para a sua área de AFS através do comando scp ou equivalente, usando o cluster sigma como máquina de origem/destino.

Assim, o acesso à área de AFS pelo cluster sigma constitui a forma mais simples de obter um primeiro contacto com o sistema de AFS.

Em Linux, para aceder à sua área pessoal do sistema AFS através do cluster sigma, pode executar o seguinte comando:

- **ssh istxxxxxx@sigma.ist.utl.pt** – onde istxxxxxxx corresponde ao seu Técnico ID. De seguida insira a respetiva password.

Cópia de dados entre a área de AFS e outro computador

Pode optar por copiar ficheiros diretamente entre o seu computador e a sua área de AFS através do comando scp:

- **scp source target**

Para copiar, por exemplo, o ficheiro teste.txt do seu computador para a pasta “Documentos” da sua área de AFS, pode executar o comando:

- **scp teste.txt istxxxxx@sigma.ist.utl.pt:~/Documentos**

No sentido inverso, se pretender copiar o ficheiro teste.txt da pasta “Documentos” da sua área de AFS para o seu computador, pode executar o comando:

- **scp istxxxxx@sigma.ist.utl.pt:~/Documentos/teste.txt ./**

Se pretender copiar uma pasta em vez de um ficheiro, pode usar a flag **-r.**

Arquitetura do sistema AFS

Células e volumes

O sistema AFS está dividido em múltiplas células que existem num espaço global da Internet. Cada célula tem um nome que é geralmente derivado do domínio em que se encontra. Assim, a célula central correspondente ao IST é ist.utl.pt. Cada uma das células configuradas surge normalmente no sistema sob o diretório /afs. Assim, a célula do IST está sob a área /afs/ist.utl.pt. No cluster sigma a listagem das várias células configuradas pode ser acedida pelo comando:

- istxxxx@sigmayy:$ **ls /afs/**

A listagem das células que contêm ist no nome pode ser feita através do comando:

- istxxxx@sigmayy:$ **ls -ld /afs/*ist***

O sistema AFS divide igualmente o espaço físico em disco em unidades designadas volumes, cada um dos quais armazena uma subárvore de ficheiros e diretórios relacionados. Uma das vantagens da unidade lógica volume resulta de ser possível deslocar volumes e áreas associadas de um servidor para outro online, sem que tal transferência seja sentida a nível de utilizador.

Cada volume de AFS dispõe de uma quota definida pelo Administrador. A quota atribuída e disponível em cada momento pode ser consultada pelo comando fs listquota dir, onde o argumento opcional dir indica o diretório pretendido. Caso este seja omitido, é listada a quota do diretório corrente. Por exemplo:

- istxxxxx@sigmayy: $ **fs listquota**

Volume Name	Quota	Used	%Used	Partition
users.istxxxxx	153600	92	0%	0%

Autenticação

A disponibilização de um sistema distribuído de ficheiros, acessível a partir de qualquer parte, implica um sistema de segurança robusto. Por este motivo, o sistema de AFS dispõe de um sistema de autenticação forte, integrado com o sistema de autenticação Kerberos.

A autenticação em AFS é obtida por meio de um token. Um token pode ser visto como um “passe” de identificação, o qual permite acesso aos dados durante o período de validade. Os tokens na célula do IST têm atualmente uma duração de 10 horas.

Em muitos casos, os tokens são tratados de forma transparente, dispensando qualquer intervenção por parte do utilizador. No entanto, um utilizador pode em qualquer altura listar os tokens que foram emitidos em seu nome pelo comando tokens.

Os tokens de AFS são obtidos a partir de um ticket identificador de Kerberos. De forma análoga aos tokens, os tickets Kerberos podem ser interpretados como um "passe" de identificação do utilizador. Quando um utilizador se autentica no sistema Kerberos, obtém um ticket inicial, designado de ticket-granting tickets, emitido pelo KDC (Key Distribution Center) do Kerberos. Este ticket inicial identifica univocamente o utilizador e permite a obtenção de tickets específicos para determinados serviços, como sucede com os tokens de AFS (de facto, no sistema Kerberos, em utilização no IST, o ticket de Kerberos para o serviço AFS é usado diretamente como o token de identificação AFS).

No caso do login no cluster sigma, o ticket-granting ticket de Kerberos é obtido automaticamente durante o processo de login, o mesmo sucedendo com o token inicial de AFS. Tal como os tokens, a manipulação dos tickets de Kerberos é geralmente transparente, mas o utilizador pode obter uma listagem dos tickets emitidos através do comando klist.

A credentials cache é a localização do ficheiro onde se encontram os tickets. O Principal corresponde à identidade do utilizador e resulta basicamente da identidade do utilizador istxxxxx e do realm do domínio Kerberos (neste caso, IST.UTL.PT). De notar que o realm de Kerberos é geralmente representado em maiúsculas e é case sensitive. Segue-se a listagem dos tickets emitidos, cada com a data de início e a data de expiração. Neste caso, o primeiro ticket (krtbg) corresponde ao ticket-granting ticket relativo ao realm IST.UTL.PT (terá, obrigatoriamente, de ser em letras capitais), enquanto que o segundo corresponde ao token de AFS, relativo à célula de afs ist.utl.pt. Podem eventualmente surgir na lista outros tickets, caso existam outros serviços que requeiram a emissão de tickets Kerberos.

Pode consultar as instruções para obter um ticket Kerberos aqui.

Adicionalmente, pode consultar as instruções para obter um token AFS e aceder à sua área pessoal do AFS aqui.

Listas de controlo de acesso (ACLs)

Cada sistema operativo dispõe de sistemas de controlo de acesso específicos. Em sistemas Unix standard, por exemplo, as permissões de leitura, escrita e execução são controlados pelos chamados "bits de modo". Estes bits permitem definir níveis de acesso distintos de leitura, escrita e execução para o utilizador, grupos (definidos pelo administrador) e todos os utilizadores da máquina, para cada ficheiro individual. A alteração dos "bits de modo" é possível pelo comando chmod.

No sistema de ficheiros AFS, qualquer que seja o sistema operativo cliente, o controlo de acesso é mantido por ACLs (Access Control Lists ou Listas de Controlo de Acessos). O sistema de ACLs é mais sofisticado e flexível, embora só permita a definição de níveis de acesso a nível de diretórios e não dos ficheiros individuais. Este nível de granularidade é, no entanto, o mais frequentemente pretendido. Note-se que o sistema de ACLs não substitui totalmente o mecanismo habitual de chmod, o qual continua a ser necessário para definir ficheiros executáveis em sistemas Unix.

Em qualquer sistema operativo, o mecanismo de ACLs só se aplica aos ficheiros que estão sob a "diretoria/pasta/afs/". Para os restantes ficheiros mantém-se o sistema de controlo de acesso específico do sistema operativo.

As ACLs de AFS definem as seguintes permissões:

- lookup **l** - Permite examinar a ACL e os ficheiros disponíveis no diretório. Esta permissão é indispensável a muitos dos outros níveis de acesso.
- read **r** - Leitura dos ficheiros no diretório.
- insert **i** - Adicionar ficheiros ou sub-diretórios.
- write **w** - Modificar o conteúdo dos ficheiros. no diretório.
- delete **d** - Apagar ficheiros.
- lock **k** - Permite os programas usarem a chamada ao sistema flock() para acesso exclusivo ao ficheiro.
- administer **a** - Possibilita modificar (administrar) a ACL.

Uma ACL é representada ou definida pela combinação das letras da lista anterior. Assim, por exemplo, arw designa a ACL que combina as permissões de read, write e administer. É também possível usar as seguintes formas abreviadas, dado corresponderem a combinações frequentes:

- **read** - Abreviatura para rl, read e lookup.
- **write** - Abreviatura rlidwk, todas as permissões exceto administrar.
- **all** - Abreviatura para todas as permissões, rlidwka.
- **none** - Remove todas as permissões.

O comando de afs para examinar e manipular ACL encontra-se entre o conjunto de comandos fs, o qual é a base de várias operações em AFS. O comando fs tem a forma geral:

- user@my_pc:$ **fs comando argumentos**

onde comando designa uma dada operação. Em particular fs help ou fs comando help permitem listar todas operações disponíveis ou ajuda específica sobre uma dada operação.

Para listar a ACL de um dado diretório, pode ser usada a operação listacl do comando fs. No cluster sigma, por exemplo, pode ser experimentado o comando:

- istxxxxx@sigma03:$ **fs listacl ~**

Access list for /afs/.ist.utl.pt/users/a/b/istxxxxx/linux is

Normal rights:

system:administrators rlidwka

system: anyuser l

istxxxxx rlidwka

Neste caso, o utilizador istxxxxxx tem todas as permissões para a sua diretoria de omissão [~] do cluster sigma, o que sucede igualmente para o grupo system:administrators. Estas permissões são normalmente as permissões de omissão.

Cada utilizador pode manipular de forma autónoma as permissões à sua área de AFS, globalmente ou em subdiretório específico. Por exemplo, o utilizador istxxxxx pode permitir que o utilizador istyyyyy tenha acesso de leitura ao seu diretório:

- istxxxxx@sigma03 /afs/.ist.utl.pt/users/a/b/istxxxxx:$ **fs setacl ~ istyyyyy r**
- istxxxxx@sigma03 /afs/.ist.utl.pt/users/a/b/istxxxxx:$ **fs listacl ~**

Access list for /afs/.ist.utl.pt/users/a/b/istxxxxx/linux is

Normal rights:

system:administrators rlidwka

system: anyuser l

istxxxxx rlidwka

istyyyyy r

Para remover a permissão de leitura, basta fazer:

- istxxxxx@sigma03 /afs/.ist.utl.pt/users/a/b/istxxxxx:$ **fs setacl ~ istyyyyy none**
- istxxxxx@sigma03 /afs/.ist.utl.pt/users/a/b/istxxxxx:$ **fs listacl ~**

Access list for /afs/.ist.utl.pt/users/a/b/istxxxxx/linux is

Normal rights:

system:administrators rlidwka

system: anyuser l

istxxxxx rlidwka

Área de trabalho

Espaço em disco

Ao ativar o serviço de AFS, cada utilizador fica automaticamente com acesso a uma área em disco no sistema, que atualmente é de 10GB.

O diretório de raíz atribuído a cada utilizador é definido por:

- /afs/.ist.utl.pt/users/a/b/istnnnnn

em que “a” e “b” correspondem aos dois algarismos menos significativos do Técnico ID. Assim, por exemplo, no caso do utilizador ist12048, a área de raíz é definida por:

- /afs/.ist.utl.pt/users/4/8/ist12048/

O facto de surgir no caminho de diretórios o troço “/4/8/”, aparentemente desnecessário, destina-se apenas a hierarquizar e distribuir a estrutura de diretórios, impedindo que todos os diretórios de utilizador fiquem no mesmo nível. Caso assim não fosse, o diretório “/afs/.ist.utl.pt/users/” teria uma dimensão excessiva, reduzindo a eficiência dos acessos.

Diretórios pré-definidos

Um utilizador que faça login no cluster sigma e consulte a sua a área de trabalho de omissão, verificará que esta corresponde à sua área de raíz de AFS:

- user@my_pc:$ **ssh ist182048@sigma.ist.utl.pt**
- ist182048@sigma03:$ **pwd**

  /afs/.ist.utl.pt/users/4/8/ist182048/

Atualmente, quando a área de AFS é criada, são automaticamente criados os seguintes sub-diretórios:

- **public** - Área para partilha de ficheiros, acessível a todos os utilizadores do sistema. Todos os ficheiros colocados neste diretório ficam acessíveis por todos os utilizadores.
- **web** - Diretoria destinado à publicação de páginas web. Este diretório só é criado quando ativado o serviço de páginas web no serviço self-service.
- **yesterday** - Diretoria onde se encontram os ficheiros do dia anterior (imagem (cópia) efetuada entre as 21H e as 22H).

Seguranças relativa aos dados pessoais

Por omissão, todos os dados transmitidos entre o cliente e o servidor no sistema AFS são cifrados, mas essa cifra não é segura, o que significa que circulam em claro na rede e podem ser sujeitos a escuta ou "sniffing".

No caso de acessos pelo cluster sigma, o acesso mantém-se seguro apesar deste facto, dado que o servidor AFS e o cliente (cluster sigma) encontram-se no mesmo espaço físico e na mesma rede local, a qual se encontra reservada a servidores da DSI.

No entanto, em acessos remotos a partir de outros locais, é recomendável a utilização da VPN caso tenha informação sensível na sua área pessoal.

Instruções para a instalação e configuração da VPN do técnico podem ser consultadas aqui.