Administração de Sistemas (ASIST)

Aula Teórico Prática 08 - 2018/2019

Integração Windows – Linux
Software Samba.
Registos de Eventos (*Event Logs*)

Integração Linux - Windows

A interoperacionalidade entre servidores Windows e servidores Linux através da rede é na atualidade facilitada pelo facto de os servidores Windows integrarem cada vez mais protocolos standard suportados pelos servidores Linux como o DNS, LDAP, iSCSI, NFS, SMB/CIFS e Kerberos 5, entre outros.

Apesar deste suporte ao nível de protocolos de aplicação básicos, a forma como eles são usados difere substancialmente entre servidores Windows e Servidores Linux, essencialmente devido as diferenças de conceção entre os sistemas operativos subjacentes.

Desde logo, a maioria dos conceitos de domínios do *Active Directory* dos servidores Windows está ausente nos servidores Linux.

O **Samba** (**https://www.samba.org/**) é um conjunto de componentes de software para Linux que inclui serviços de rede e aplicações clientes. Permite a um servidor Linux simular muitas das funcionalidades dos servidores Windows e constitui a ferramenta base de qualquer integração mais séria entre estes dois tipos de sistemas em ambiente de rede.

Contas de utilizadores e grupos

Enquanto em Linux os utilizadores e grupos são identificados, respetivamente, através de um UID e GID únicos, em Windows são identificados através de um SID (*Security Identifier*) único.

Desde logo a compatibilização vai exigir o estabelecimento de um mecanismo de mapeamento (UID <-> SID) e (GID <-> SID).

Além deste aspeto as incompatibilidades são diversas começando pelos nomes de utilizadores e grupos que são muito mais restritivos em Linux do que em Windows.

Uma forma de resolver as incompatibilidades de nomes é criar mapeamentos estáticos, entre nomes Windows que não são válidos em Linux, e nomes válidos em Linux. Por exemplo fazendo corresponder ao grupo Windows **Domain Users** o grupo Linux **dom_users**.

Note-se também que a maioria das restrições relativas a nomes de utilizadores e grupos em Linux não existem de facto, são restrições de retro compatibilidade, genericamente os nomes suportados em Windows são diretamente suportados em Linux.

Em Linux cada utilizador pertence obrigatoriamente a pelo menos um grupo (grupo primário), o mesmo se aplica a utilizadores Windows. No Windows cada utilizador também é obrigatoriamente membro de um grupo primário (compatibilidade POSIX). No entanto, enquanto em Linux apenas utilizadores podem ser membros de grupos, no *Active Directory*, grupos podem ser membros de grupos.

Partilha de ficheiros (NAS)

Sob o ponto de vista de SAN (iSCSI), nunca existem problemas de integração porque os discos lógicos são formatados e utilizados pelo sistema operativo que os recebe como se fossem discos locais.

Ao nível de partilha de ficheiros em rede (NAS), os servidores Windows são orientados para a utilização de SMB/CIFS enquanto os servidores Linux são orientados para a utilização de NFS.

Embora os servidores Windows possam operar como clientes e servidores NFS, a melhor solução de integração consiste em adicionar o suporte de SMB/CIFS aos servidores Linux através do Samba.

O Samba permite partilhar pastas e impressoras através de SMB/CIFS de forma totalmente compatível com as máquinas Windows, as incompatibilidades surgem sob o ponto de vista das caraterísticas dos sistemas de ficheiros subjacentes à partilha.

No Linux as ACL base (Posix) apenas suportam três entidades: owner, group e others. Com apenas três permissões possíveis para cada um deles: read, write e execute.

Desde que o UID (owner) associado ao objeto corresponda a um utilizador Windows (SID) e o GID (group) associado ao objeto corresponda um grupo Windows (SID), estas duas entidades são diretamente colocadas na ACL Windows. A entidade Linux **others** é normalmente associada ao SID do grupo Windows **everybody**.

Linux - *Extended Permissions* (ACL)

Nos sistemas Linux atuais, as ACL base podem ser expandidas através da utilização dos comandos **getfacl/setfacl**. Continuam a existir apenas as três permissões das ACL base (rwx), mas as entidades deixam de estar limitadas a (owner/group/others). Além destas três entidades das ACL base, podem ser acrescentados outros utilizadores e grupos.

Usando o comando setfacl é possível definir para uma pasta a "Default ACL", essa ACL será herdada pelos objetos colocados dentro dessa pasta. Também é possível definir uma mascara de permissões efetivas máximas que podem ser atribuídas pelas várias entradas da ACL.

Tanto as partilhas de rede via Samba (SMB/CIFS) como via NFS suportam as *extended permissions* do Linux, relativamente às ACL Windows permitem uma melhor integração através do Samba.

Numa partilha de rede realizada através do Samba, as ACL definidas são armazenadas sob a forma de *extended permissions* no Linux, assim deixam de estar limitadas a apenas três entidades.

Note-se que se o Samba estiver a exercer a função de DC de domínio AD, as ACL das partilhas serão ACLs nativas Windows e não são armazenadas sob a forma de *extended permissions* no Linux. Por essa razão aconselha-se a que o DC Samba *Active Directory* não exerça a função de File Server (servidor de partilhas) e essa função seja transferida para um *domain member*.

Samba – *Atributos do MS-DOS*

Algumas aplicações ainda utilizam os atributos dos ficheiros herdados do MS-DOS: System; Hidden, Archive e Read-only. Esses atributos não existem nos sistemas de ficheiros Linux subjacentes às partilhas de rede realizadas através do Samba.

O problema pode ser colmatado através do seu armazenamento na ACL de *extended permissions* do Linux ou através do seu mapeamento para permissões execute de owner, group e others.

Samba – *Partilha de impressoras*

A partilha de impressoras (Print Server) é integralmente suportada pelo Samba, incluindo a instalação automática de drivers nos sistemas operativos Windows clientes (Workstations).

O Samba pode disponibilizar impressoras configuradas localmente através do CUPS (*Common UNIX Printing System*) ou do LPRng, ou usar diretamente impressoras de rede.

Também é possível criar uma impressora virtual PDF que cria automaticamente ficheiros em formato PDF numa pasta partilhada na rede.

Integração Linux/Windows - Samba

Desde a versão 4, o Samba pode assumir a função *Domain Controller Active Directory*, isso significa que pode fazer praticamente tudo o que o Windows Server faz como DC no *Active Directory*. É mesmo possível ter no mesmo domínio *Domain Controllers*, Windows Server 2016 a trabalhar conjuntamente com *Domain Controllers* Samba.

Este será o papel mais avançado que o Samba suporta, no entanto existem muitos cenários de integração nos quais pode ser usado.

Samba – *Standalone Server*

O Samba configurado como ***Standalone Server*** permite disponibilizar partilhas de rede. Não estando integrado em nenhum domínio, será necessária a autenticação do utilizador perante o servidor para aceder às partilhas.

As contas de utilizador válidas serão todas as contas Linux válidas (NSS) desde que tenham sido acrescentadas à base de dados de contas Windows do Samba.

O Samba tem de manter uma base de dados sombra de contas de utilizadores e grupos Linux para armazenar atributos que, sendo necessários nas contas Windows, não existem nas contas Linux.

Neste tipo de configuração (***Standalone Server***) o Samba tem de simular contas de utilizadores e grupos Windows a partir das contas Linux.

O único atributo das contas Linux que é diretamente transferido para as contas Windows é o **login-name,** tudo o resto tem de ser definido pelo Samba e armazenado num repositório sombra. Os SID dos utilizadores e grupos são definidos com base respetivamente no UID e GID e são armazenados juntamente com todos os outros atributos das contas Windows.

O Windows realiza a autenticação dos utilizadores através de ***hashes*** designados **NT-password** e **LM-password** (este último apenas é mantido para compatibilidade com clientes antigos). Estes ***hashes*** ficam também guardados nas contas de utilizadores Windows.

A password Linux e a password Windows são totalmente independentes, no entanto o Samba inclui um mecanismo através do qual sempre que o utilizador altera a password através do Windows, a respetiva password Linux é alterada da mesma forma.

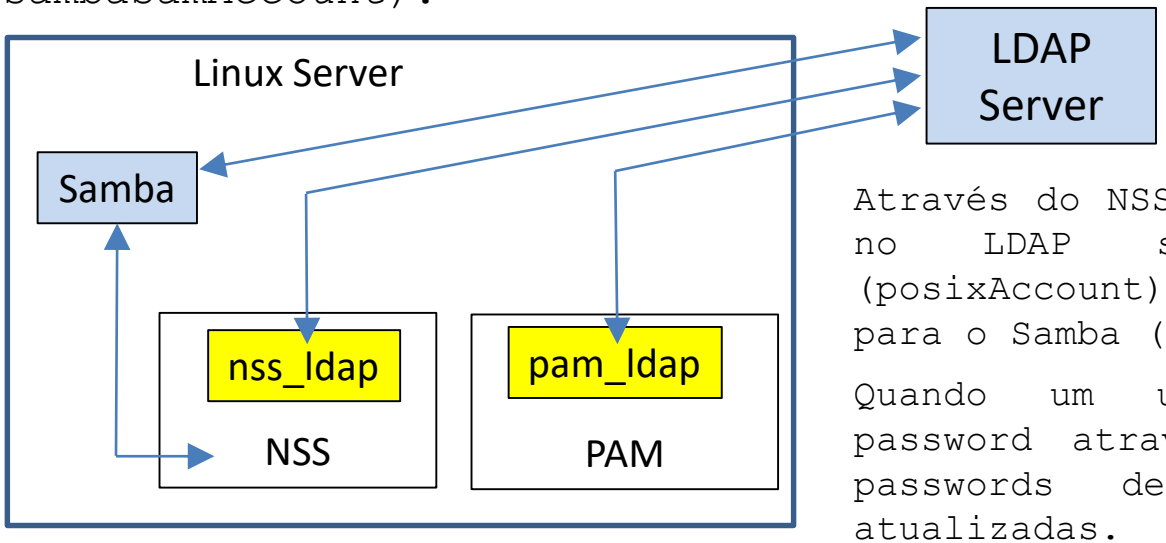
Uma conta de utilizador ou grupo só é válida sob o ponto de vista do Samba/Windows se for um utilizador/grupo válido no Linux e existir no repositório sombra do Samba (contas Windows).

Samba - Utilização do LDAP como repositório

Em qualquer configuração do Samba em que seja necessário gerir contas locais de utilizadores Windows, o *default* é o Samba armazenar esses dados em bases de dados internas (**tdbsam**). Neste caso, temos armazenados em locais diferentes a conta Linux (NSS) e a conta sombra Windows (**tdbsam**), usar LDAP permite resolver este problema com algumas vantagens.

No LDAP podemos definir objetos que pertencem a várias classes (desde que apenas uma seja estrutural e as restantes auxiliares).

Por exemplo, no caso das contas de utilizadores podem ser usadas as classes LDAP **posixAccount** e **sambaSamAccount**. Isto permite armazenar no mesmo objeto os atributos do Linux (posixAccount) e do Windows (sambaSamAccount).



Através do NSS, os utilizadores definidos no LDAP são válidos no Linux (posixAccount) e são igualmente válidos para o Samba (sambaSamAccount).

Quando um utilizador altera a sua password através do Windows/Samba, as passwords de ambas as contas são atualizadas.

Samba – *Active Directory Domain Member*

O Samba pode ser um ***Domain Member Server*** de um domínio *Active Directory* ou de um domínio Windows NT, independentemente do domínio operar com *Domain Controllers* Windows Server ou Samba.

Isto significa que todos os objetos do domínio, incluindo utilizadores e grupos passarão a ser válidos no sistema Linux e consequentemente no Samba. Deste modo, os utilizadores autenticados num domínio da floresta terão acesso direto às partilhas de rede disponibilizadas pelo Samba sem necessidade de autenticação adicional.

Adaptar as contas de utilizadores e grupos, tal como estão definidas no domínio Windows, ao que o Linux espera que sejam contas de utilizadores e grupos exige algum esforço. Existe um serviço local dedicado a essa tarefa designado **Winbind.**

O Winbind é o responsável por dar um aspeto Linux às contas Windows e tem vários desafios pela frente. O mais importante é realizar o mapeamento entre os SID dos utilizadores e grupos Windows para UID e GID em Linux.

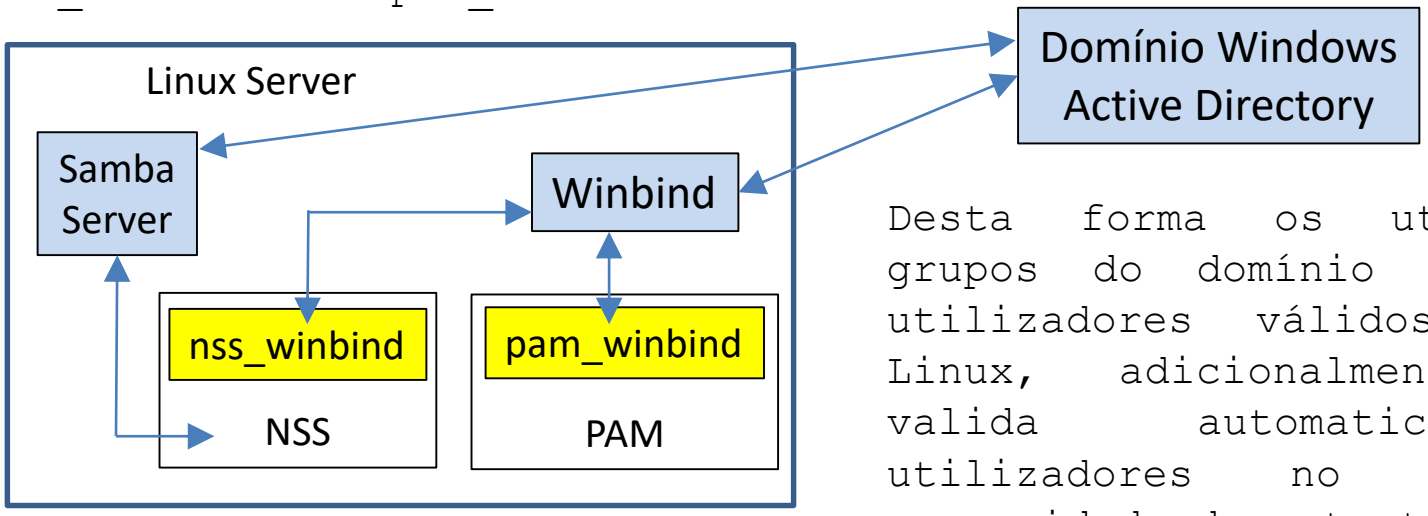
Neste tipo de configuração é atribuída uma gama de UIDs e GIDs para o Winbind gerir, cada vez que se depara com um SID desconhecido associa-lhe de forma persistente um novo UID ou GID das gamas estabelecidas, conforme se trate de um utilizador ou grupo.

Samba *domain member* – *Winbind*

O Winbind mantém os mapeamentos estabelecidos numa base de dados interna, assim quando atribui um UID ou GID a um determinado SID, o utilizador ou grupo correspondente vai ter sempre o mesmo UID ou GID.

No entanto, se existirem vários *domain members* configurados desta forma nada garante que em todos eles o Winbind atribua o mesmo UID ou GID ao mesmo SID. Para resolver este problema é possível configurar o Winbind para guardar os mapeamentos num repositório centralizado LDAP, desta forma garante-se que um utilizador ou grupo Windows terá o mesmo UID ou GID em todos os servidores Linux que são membros do domínio.

A integração dos utilizadores e grupos do Winbind no sistema Linux é feita à custa de módulos NSS e PAM apropriados, nomeadamente o nss_winbind e o pam_winbind:

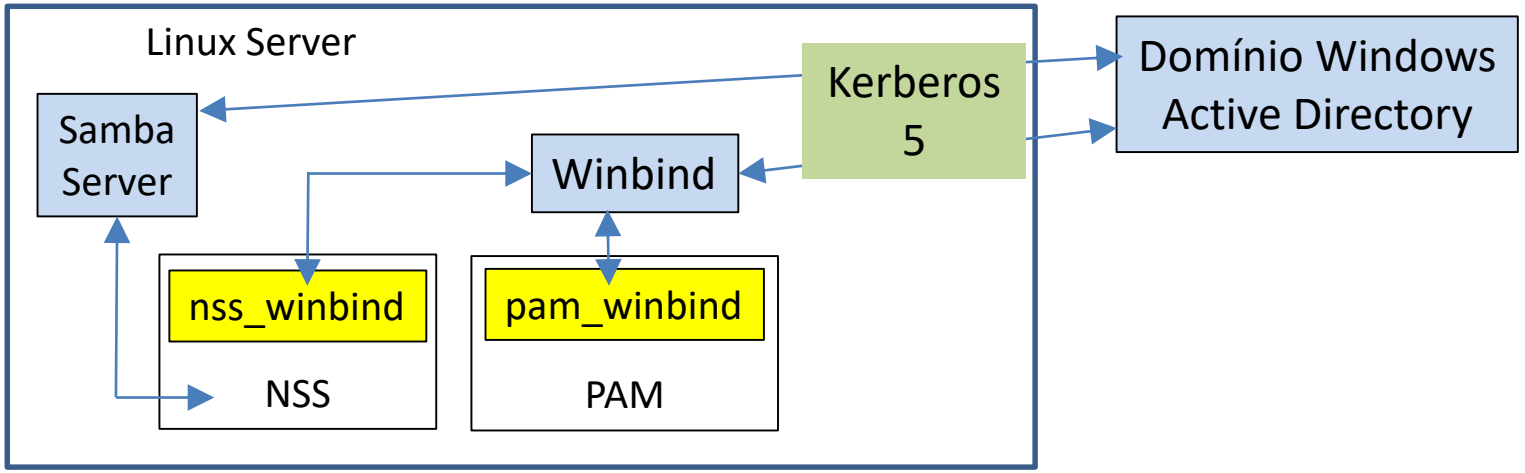


Desta forma os utilizadores e grupos do domínio passam a ser utilizadores válidos no sistema Linux, adicionalmente o Samba valida automaticamente os utilizadores no domínio sem necessidade de autenticação manual.

Samba *domain member* – *Kerberos 5*

O funcionamento do *Active Directory* exige que todas as transações entre membros do domínio sejam protegidas e autenticadas através do *Kerberos 5*, os *Domain Controllers* possuem um servidor *Kerberos 5*, incluindo um KDC (*Key Distribution Center*).

Assim, **os *domain members* de um domínio *Active Directory*** necessitam de ter um cliente *Kerberos 5* configurado para usar esse KDC.



Para evitar ataques de ***replay***, as mensagens usadas pelo *Kerberos* transportam ***timestamps***, normalmente uma mensagem torna-se invalida se a diferença horária é superior a 300 segundos.

É portanto fundamental assegurar a sincronização horária entre as máquinas de um domínio *Active Directory*, no caso do Linux, a melhor forma de assegurar isso é utilizar o serviço NTP (***Network Time Protocol***).

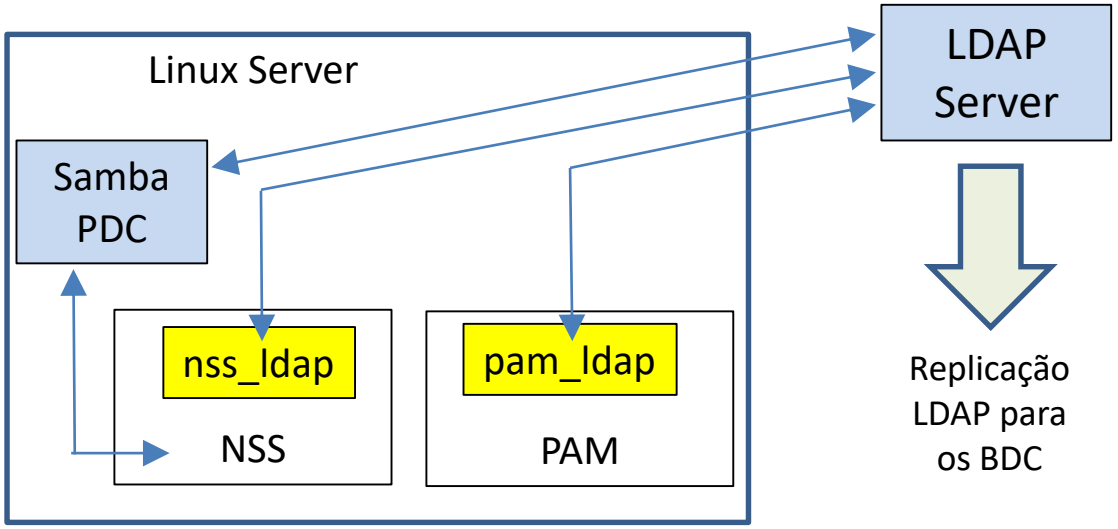
Samba *domain controller NT*

O Samba pode funcionar como PDC (*Primary Domain Controller*) de um domínio Windows em modo de compatibilidade NT (pré *Active Directory*).

A configuração é semelhante ao modo de funcionamento ***Standalone Server***, ou seja são usadas as contas locais do Linux apoiadas numa base de dados com informação complementar de atributos Windows.

A solução mais interessante é a utilização de uma base de dados LDAP para armazenar a informação relativamente a contas de forma integrada.

São suportadas todas as funcionalidades presentes nos domínios NT nativos, nomeadamente: Single Sign-On no domínio, home directory, roaming profiles, logon script e políticas de domínio.



Sendo usado o LDAP, também é simples definir BDCs (*Backup Domain Controllers*), para esse feito devem ser usados os mecanismos de replicação do LDAP para garantir a replicação da base de dados LDAP do PDC para as que são usadas pelos vários BDC.

Samba *Active Directory Domain Controller*

A Samba também pode operar como *Domain Controller Active Directory*, atualmente isso exige algumas condições na configuração do servidor Linux.

Devido às especificidades do *Active Directory*, terá de ser usado um servidor LDAP interno do Samba e terá de ser também usado um servidor DNS integrado no Samba. Pode ser usado o servidor *Kerberos* MIT do sistema operativo ou em alternativa um servidor *Kerberos* interno do Samba.

O facto de se usarem servidores integrados no Samba significa que toda a gestão de utilizadores, grupos e DNS terá de ser realizada através do Samba/Windows.

O servidor LDAP integrado é puramente *Active Directory*, não contém atributos de contas Linux. Por exemplo para que os utilizadores e grupos do domínio sejam válidos no Linux é necessário usar o Winbind e configurar o Linux como *domain member* como se tratasse de um domínio Windows *Active Directory* nativo. Não é possível usar diretamente o servidor LDAP integrado.

Num domínio *Active Directory*, devem existir pelo menos dois DC, neste modo de funcionamento o Samba assegura a replicação automática da base de dados *Active Directory* entre todos os *Domain Controllers* do domínio.

Registos de atividades (*Event Logs*)

Os sistemas operativos e aplicações produzem mensagens representativas dos eventos que ocorrem, essas mensagem são guardadas persistentemente em ficheiros de log.

A análise dos ficheiros de log pelos administradores deve ser o primeiro passo quando algo não funciona como pretendido. A inspeção dos ficheiros de log permite ainda detetar situações anómalas que apesar de não afetarem o funcionamento aparente dos sistemas podem ser importantes, por exemplo sob o ponto de vista da segurança.

Se forem usadas ferramentas de monitorização automática dos sistemas, um dos aspetos que deve ser monitorizado são os ficheiros de log.

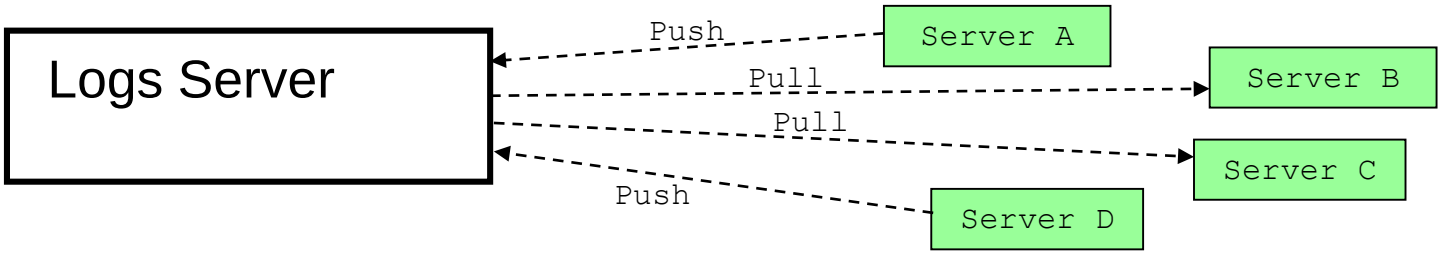
Cada mensagem de log gerada por uma aplicação, serviço ou pelo sistema operativo contém normalmente um **nível de gravidade**, uma identificação da **origem** (quem a produziu – computador, aplicação, serviço, subsistema, etc.) e um **texto descritivo** do evento.

A quantidade de informação de log gerada por cada origem pode ser geralmente configurada nessa origem, tipicamente um serviço ou aplicação. Se um serviço ou aplicação não está a funcionar corretamente podemos muitas vezes configura-la para aumentar a quantidade de informação de log que ela gera (nível de log), uma vez detetado e resolvido o problema, devemos reduzir novamente o nível de log para o normal para não afetar a sua performance.

Registos de eventos centralizado

Num ambiente de rede distribuído em que existem vários servidores e outros equipamentos, podemos centralizar o registo de eventos. Para esse efeito será escolhido um servidor (servidor de log) que vai obter através da rede os eventos produzidos em todos os outros equipamentos. Desta forma o administrador dispõe de um local único onde pode consultar os eventos relativos a todos os equipamentos da infraestrutura.

A centralização de log pode ser implementada de duas formas PUSH (*Source Computer Initiated*) ou PULL (*Collector Initiated*).



PULL: O servidor de logs toma a iniciativa de estabelecer uma sessão para transferência de logs, para isso será necessário definir no servidor de logs um a um todos os equipamentos dos quais se pretende obter eventos.

PUSH: O equipamento de origem do evento toma a iniciativa de contactar o servidor de logs. Em cada um dos equipamentos é necessário definir o mesmo servidor de logs correto.

Windows Event Logs

Nos sistemas Windows, os eventos são guardados em ficheiros distintos de acordo com a sua origem. A aplicação ***Event Viewer*** permite consultar e gerir esses registos de eventos.

Os logs estão organizados por temas de acordo com a sua origem (sistema, aplicações, serviços, etc.) existindo um log distinto para cada, nestes logs são registados todos os eventos independentemente da sua gravidade. Também podem ser adicionados novos ficheiros de log.

No ***Event Viewer*** podemos criar ***Custom Views*** de logs, numa ***Custom View*** podemos agregar conjuntos de eventos de vários logs, definir os níveis de gravidade que pretendemos incluir na ***Custom View*** e outros critérios de filtragem.

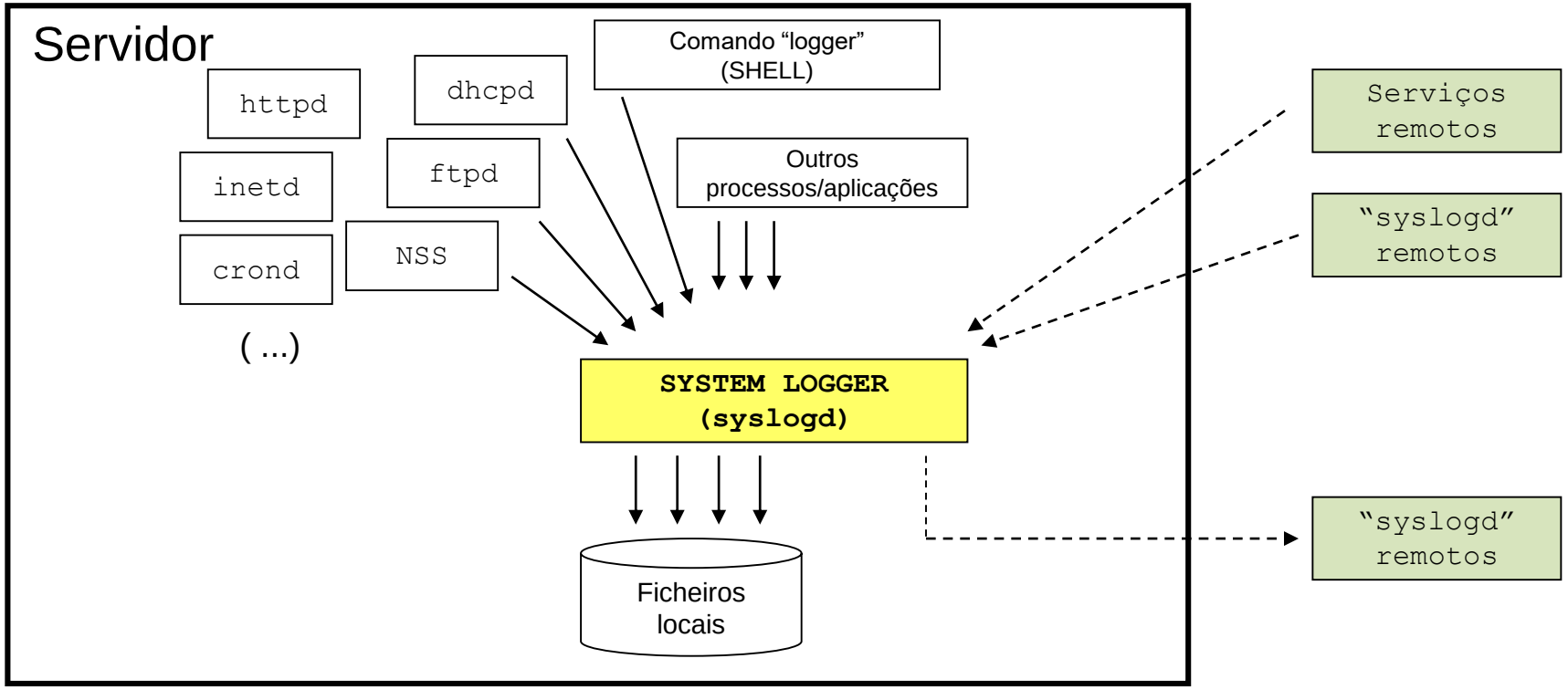
Podemos centralizar os logs através da criação de uma ***Subscription*** na qual definimos as máquinas de onde queremos obter o eventos, o log onde depositar esses eventos, e critérios de filtragem.

Numa ***Subscription*** podemos obter os eventos por iniciativa do servidor que os pretende recolher (*Collector Initiated*) ou por iniciativa das máquinas de origem (*Source Computer Initiated*). Neste último caso a máquina de origem terá de ser configurada para o efeito. A transferência de logs entre máquinas usa o protocolo HTTP/HTTPS dirigido para números de porto especiais.

Linux - *System Logger* (syslog)

O Linux utiliza um sistema *standard* de log conhecido por Syslog, através de uma API apropriada, as aplicações e serviços enviam ao Syslog os seus eventos.

De acordo com os atributos definidos na origem o Syslog classifica os eventos e através das configurações definidas pelo administrador realiza uma ou várias ações sobre eles. Normalmente uma das ações mais comums é acrescentar (append) o evento a um ficheiro de texto que é usado como repositório, normalmente na pasta **/var/log/**.



System Logger – Classificação das mensagens

Embora as versões mais avançadas como o RSYSLOG (*the rocket-fast system for log processing*) permitam usar uma grande variedade de critérios para classificar os eventos, incluindo através do conteúdo do respetivo texto, a forma mais tradicional de classificação é através dos atributos ***facility*** e ***severity*** definidos na origem.

O atributo ***facility*** serve para identificar o tipo de origem, pode ter um dos valores seguintes: *auth*, *authpriv*, *cron*, *daemon*, *kern*, *lpr*, *mail*, *mark*, *news*, *security* (o mesmo que *auth*), *syslog*, *user*, *uucp* e *local0* a *local7*.

O atributo ***severity*** define o nível de gravidade do evento, por ordem crescente de gravidade, os valores possíveis são: debug, info, notice, warning, warn (igual ao anterior), err, error (igual ao anterior), crit, alert, emerg, panic (igual ao anterior).

Estes dois atributos são frequentemente apresentados na forma agrupada: ***facility.severity***

A missão fundamental do Syslog é analisar estes dois atributos e em função do seu valor definir o que fazer com o evento. Algumas ações standard são: acrescentar (append) a um ficheiro local; enviar para um servidor Syslog remoto; enviar diretamente para o terminais de utilizadores ativos; executar um programa externo e passar-lhe a mensagem através do stdin.

Linux System Logger – Configuração

Nas versões tradicionais do Syslog o ficheiro de configuração é o **/etc/syslog.conf** e a classificação dos eventos baseia-se exclusivamente nos atributos ***facility.severity***, o ficheiro contém uma sequência de padrões destes atributos e a ação a desencadear para os eventos que lhe correspondam. Para cada evento, todas as ações definidas para padrões que lhe correspondam serão executadas, não apenas a primeira correspondência.

Exemplo:

```
kern.*                          /var/adm/kernel
mail.*;mail.!=info              -/var/adm/mail
*.alert                         root,admin
mail.=info                      @server2.ipp.pt
mail,news.=info                 *
kern.info;kern.!err             |/root/kern-info
```

Os valores de ***severity*** no padrão fazem correspondência com eventos com nível de gravidade superior ou igual. Para cada padrão é especificada uma ação, se a ação começa por / significa que se trata de um ficheiro de logs onde o evento deve ser registado, pode ser precedido do sinal – para indicar é necessário executar o sync (caso contrário pode não ser imediatamente escrito no ficheiro).

```
*.alert                         root,admin
mail.=info                      @server2.ipp.pt
mail,news.=info                 *
kern.info;kern.!err             |/root/kern-info
```

A ação também pode ser um ou uma lista de utilizadores, nesse caso se os utilizadores estiverem ativos em sessões de terminal recebem uma mensagem com o evento no seu terminal. O símbolo * permite o envio da referida mensagem a todos os utilizadores ativos em sessões de terminal. A barra vertical (pipe) identifica um comando externo a ser executado que recebe no stdin o evento.

O símbolo @ permite identificar através de um endereço IP ou nome DNS uma máquina para a qual pretendemos enviar o registo de evento. É necessário que na máquina remota esteja em funcionamento um Syslog configurado para aceitar eventos da rede no número de porto UDP 514.

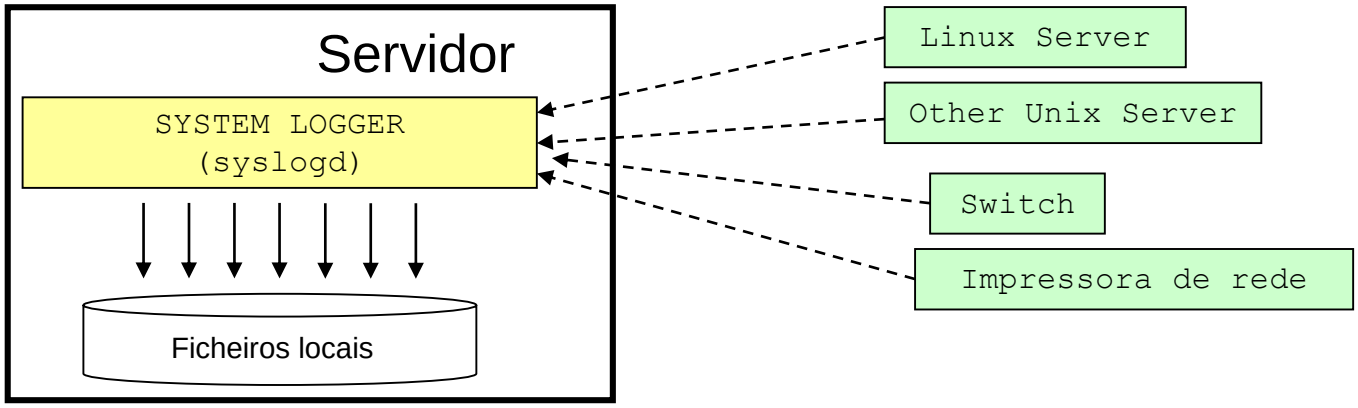
Algumas versões do Syslog também suportam a utilização de TCP e outros números de porto, nesse caso a ação deve ser identificada por @@ e o número de porto pode ser definido, por omissão será 514.

Exemplo:

```
*.*             @@server1.example.net:10514
*.info          @192.168.5.7:23000
*.!=info        @@192.168.5.1
```

Linux System Logger – Centralização

Um vantagem do Syslog é que se trata de um standard (RFC5424), que entre outros aspetos define como requisitos mínimos o transporte dos eventos através de UDP. Uma grande diversidade de equipamentos de rede simples como impressoras, switches, routers e outros, suportam o protocolo Syslog.



É mesmo possível através de DHCP fornecer aos equipamentos da rede a indicação de qual é o endereço do servidor Syslog que devem usar (atributo **log-servers** do DHCP).

O protocolo de transferência de eventos através da rede do Syslog não dispõe de mecanismos de autenticação e segurança, assim deve ser usado através de redes seguras, de preferência usando TCP e permitindo o acesso apenas para os endereços de origem correspondentes aos equipamentos dos quais se pretende receber os eventos (filtragem).

Embora o protocolo Syslog não seja suportado pela Microsoft nos sistemas Windows, existem implementações disponíveis não Microsoft, incluindo uma versão do RSYSLOG.

Linux System Logger – Ficheiros de log

Em última instância, a maioria dos eventos processados pelo Syslog acabam em ficheiros de log. Tratam-se de ficheiros de texto e como tal podem ser consultados usando vários comandos disponíveis no Linux para esse efeito como por exemplo: cat, less, tail, more, grep e cut.

Logrotate

A dimensão de cada ficheiro de log vai crescer sucessivamente, para organizar estes ficheiros pode ser usado o comando ***logrotate***.

Tipicamente o ***logrotate*** é executado diariamente pelo CRON para consolidar os ficheiros de log segundo as configurações definida no ficheiro **/etc/logrotate.conf**. A consolidação consiste numa rotação do ficheiro de log, ou seja transferir o conteúdo atual para um ficheiro de arquivo e esvaziar o ficheiro de log, os ficheiros de arquivo possuem o mesmo nome do log com um sufixo numérico de ordem ou de data.

Através desta consolidação podemos definir para cada ficheiro de log: a periodicidade da rotação, se os ficheiros de arquivo devem ser comprimidos e o número máximo de rotações a partir do qual se começa a eliminar as cópias de arquivo mais antigas.

Em lugar de uma rotação periódica também podemos definir que a rotação será realizada quando a dimensão do log ultrapassa um dado limite. Pode ainda ser configurado um endereço de email para o qual as copias de arquivo que ultrapassam o número máximo de rotações serão enviadas antes de serem eliminadas.

Linux – registo de entradas e saídas

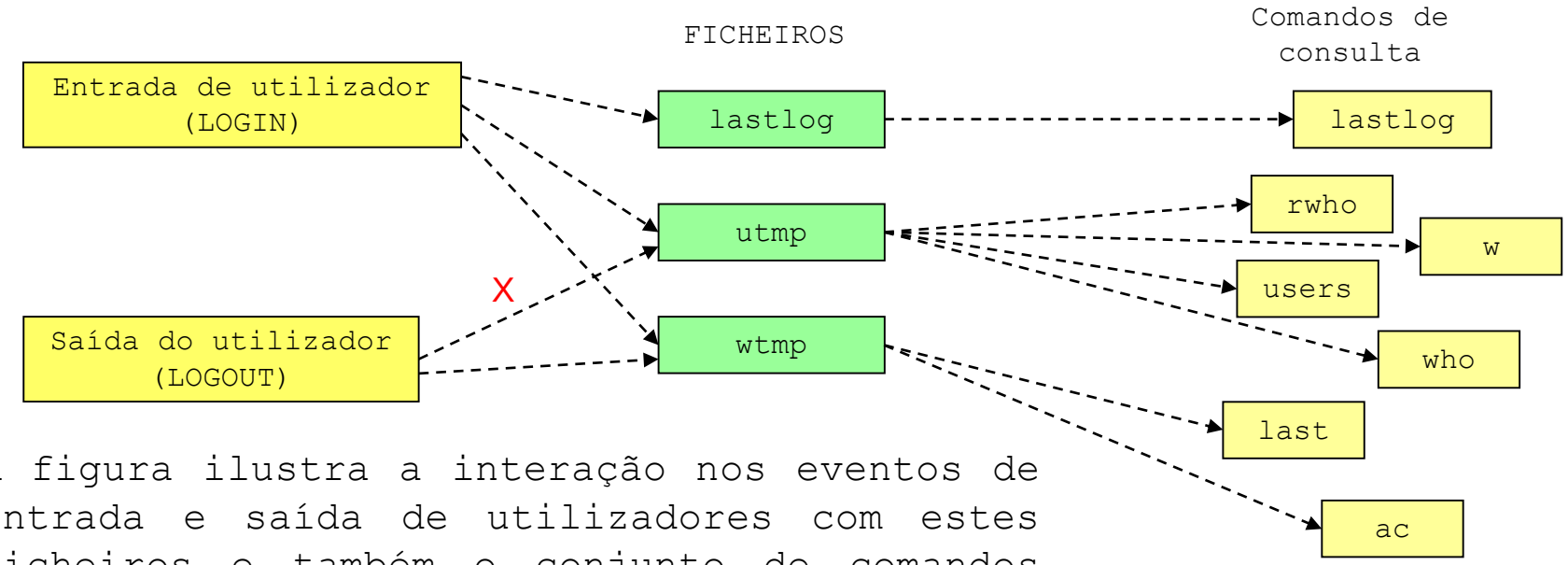
Embora os eventos de entrada (login/logon) e saída (logout/logoff) de utilizadores no sistema sejam registados sob a forma de eventos através do Syslog (incluindo tentativas de acesso falhadas), no Unix existem registos adicionais para este efeito. Os programas que lidam com estes eventos têm a responsabilidade de os registar através de uma API distinta do Syslog. Estes registos são baseados em três ficheiros que não se encontram em formato de texto legível:

- **utmp** (normalmente **/var/run/utmp**) – contém, para cada terminal, o nome do terminal, o nome do utilizador atual, a origem do utilizador (máquina remota/endereço) e a data/hora a que efetuou o login. Quando o utilizador saí, o registo é eliminado.

- **lastlog** (normalmente **/var/log/lastlog**) – contém, para cada UID, a hora e local (terminal/máquina remota/endereço) da última entrada no sistema (login).

- **wtmp** (normalmente **/var/log/wtmp**) – contém o registo histórico de todas as entradas e saídas no sistema.

Linux – registo de entradas e saídas



A figura ilustra a interação nos eventos de entrada e saída de utilizadores com estes ficheiros e também o conjunto de comandos usados para os consultar. Exemplo de resultado do comando last:

```
[root@server ~]# last -5
andre    pts/0        beavis.dei.isep. Wed Nov 12 16:35   still logged in
dei      pts/0        beavis.dei.isep. Wed Nov 12 11:46 - 14:12  (02:25)
i090763  pts/4        srv3.dei.isep.ip Wed Nov 12 09:36 - 09:54  (00:17)
i080751  pts/3        srv3.dei.isep.ip Wed Nov 12 08:52 - 10:02  (01:10)
i040478  pts/2        srv2.dei.isep.ip Wed Nov 12 08:51 - 10:03  (01:11)

wtmp begins Sat Nov  1 12:59:40 2004
```