Trusted Domain Support

as Active Directory Domain Controller

Stefan Metzmacher <metze@samba.org>

Samba Team / SerNet

2018-06-07

https://samba.org/~metze/presentations/2018/SambaXP/

Talks at SambaXP/SDC 2017

- Last year I gave talks about concepts and details of trusted domains
- "The Important Details Of Windows Authentication" at SambaXP.
- https://samba.org/~metze/presentations/2017/SambaXP/
- "Windows Authentication With Multiple Domains and Forests" at Storage Developer Conference.
- https://samba.org/~metze/presentations/2017/SDC/

(draft)

Topics

- The long road to trust support (4.3.0, 4.7.0, 4.8.0, master)
- samba-tool domain trust commands
- wbinfo -m –verbose changes
- Automatic creation of foreignSecurityPrincipal objects
- Implementing SID expanding/filtering
- Forest/Domain-wide Authentication
- Selective Authentication (Cross Organization Trusts)
- Future Improvements / Open Bugs
- Questions?

The long road to trust support (Part1, before 4.3.0)

- It started with a Red Hat project to support Forest Trusts to FreeIPA:
  - Red Hat sponsored my work (via SerNet)
  - The initial target was only Kerberos
  - NTLMSSP was not required and got deferred
- Preparation work:
  - The Windows GUI should be able to create/manage trusts
  - It was required to fix/implement several LSA and Netlogon RPC calls
  - The most challenging was the forest information conflict detection
- Our own tools:
  - 'samba-tool domain trust *' commands were added
  - It uses very similar network request as the Windows GUI
  - They manage trust for the local domain by default
  - But they can also run against a remote servers

The long road to trust support (Part1, before 4.3.0)

- It started with a Red Hat project to support Forest Trusts to FreeIPA:
  - Red Hat sponsored my work (via SerNet)
  - The initial target was only Kerberos
  - NTLMSSP was not required and got deferred
- Preparation work:
  - The Windows GUI should be able to create/manage trusts
  - It was required to fix/implement several LSA and Netlogon RPC calls
  - The most challenging was the forest information conflict detection
- Our own tools:
  - 'samba-tool domain trust *' commands were added
  - It uses very similar network request as the Windows GUI
  - They manage trust for the local domain by default
  - But they can also run against a remote servers

The long road to trust support (Part1, before 4.3.0)

- It started with a Red Hat project to support Forest Trusts to FreeIPA:
  - Red Hat sponsored my work (via SerNet)
  - The initial target was only Kerberos
  - NTLMSSP was not required and got deferred
- Preparation work:
  - The Windows GUI should be able to create/manage trusts
  - It was required to fix/implement several LSA and Netlogon RPC calls
  - The most challenging was the forest information conflict detection
- Our own tools:
  - 'samba-tool domain trust *' commands were added
  - It uses very similar network request as the Windows GUI
  - They manage trust for the local domain by default
  - But they can also run against a remote servers

Management: samba-tool domain trust

```
dc1:~$ samba-tool domain trust help
Usage: samba-tool domain trust <subcommand>

Domain and forest trust management.

Options:
  -h, --help  show this help message and exit

Available subcommands:
  create       - Create a domain or forest trust.
  delete       - Delete a domain trust.
  list         - List domain trusts.
  namespaces   - Manage forest trust namespaces.
  show         - Show trusted domain details.
  validate     - Validate a domain trust.
For more help on a specific subcommand,
please type: samba-tool domain trust <subcommand> (-h|--help)
```

The long road to trust support (Part2, before 4.3.0)

- We added code to manage and use a trust routing table:
  - Utility (dsdb_trust_*) functions made it easier for high level code
  - They load the forest information of the local forest
  - They load the forest information of all trusted domain/forests
  - Some put everything together to form a routing table
- Implementing INCOMING and OUTGOING trust support for Kerberos:
  - The KDC was changed to use the routing table
  - AS-Requests may refer clients to the correct KDC with WRONG_REALM referrals
  - TGS-Requests may result in cross realm referral tickets
- Regression selftests:
  - We established trust relationships between several environments
  - It was relatively easy by using the new 'samba-tool domain trust' commands
  - The rest was done with some blackbox tests using kinit or smbclient

The long road to trust support (Part2, before 4.3.0)

- We added code to manage and use a trust routing table:
  - Utility (dsdb_trust_*) functions made it easier for high level code
  - They load the forest information of the local forest
  - They load the forest information of all trusted domain/forests
  - Some put everything together to form a routing table
- Implementing INCOMING and OUTGOING trust support for Kerberos:
  - The KDC was changed to use the routing table
  - AS-Requests may refer clients to the correct KDC with WRONG_REALM referrals
  - TGS-Requests may result in cross realm referral tickets
- Regression selftests:
  - We established trust relationships between several environments
  - It was relatively easy by using the new 'samba-tool domain trust' commands
  - The rest was done with some blackbox tests using kinit or smbclient

The long road to trust support (Part2, before 4.3.0)

- We added code to manage and use a trust routing table:
  - Utility (dsdb_trust_*) functions made it easier for high level code
  - They load the forest information of the local forest
  - They load the forest information of all trusted domain/forests
  - Some put everything together to form a routing table
- Implementing INCOMING and OUTGOING trust support for Kerberos:
  - The KDC was changed to use the routing table
  - AS-Requests may refer clients to the correct KDC with WRONG_REALM referrals
  - TGS-Requests may result in cross realm referral tickets
- Regression selftests:
  - We established trust relationships between several environments
  - It was relatively easy by using the new 'samba-tool domain trust' commands
  - The rest was done with some blackbox tests using kinit or smbclient

The long road to trust support (Part3, 4.3.0)

- 4.3.0 was released (in September 2015) with the improvements, but had limitations:
  - It's not possible to add users groups of a trusted domain into domain groups.
  - NTLMSSP and LSA LookupNames Sids were not implemented for outgoing trusts
- There were also security limitations:
  - No SID filtering rules are applied at all!
  - Both sides of the trust need to fully trust each other!
  - This means DCs of domain A can grant domain admin rights in domain B!
- There was a lot of usefull work happening:
  - But it was still only be usable for some rare usecases
  - The project was stopped at that point

The long road to trust support (Part3, 4.3.0)

- 4.3.0 was released (in September 2015) with the improvements, but had limitations:
  - It's not possible to add users groups of a trusted domain into domain groups.
  - NTLMSSP and LSA LookupNames Sids were not implemented for outgoing trusts

- There were also security limitations:
  - No SID filtering rules are applied at all!
  - Both sides of the trust need to fully trust each other!
  - This means DCs of domain A can grant domain admin rights in domain B!

- There was a lot of usefull work happening:
  - But it was still only be usable for some rare usecases
  - The project was stopped at that point

The long road to trust support (Part3, 4.3.0)

- 4.3.0 was released (in September 2015) with the improvements, but had limitations:
  - It's not possible to add users groups of a trusted domain into domain groups.
  - NTLMSSP and LSA LookupNames Sids were not implemented for outgoing trusts
- There were also security limitations:
  - No SID filtering rules are applied at all!
  - Both sides of the trust need to fully trust each other!
  - This means DCs of domain A can grant domain admin rights in domain B!
- There was a lot of usefull work happening:
  - But it was still only be usable for some rare usecases
  - The project was stopped at that point

The long road to trust support (Part4, after 4.5.0)

- After 4.5.0 was released in September 2016
  - SerNet got more and more customers asking for trust support
  - This was often the only reason they had to keep using Windows servers
- Other customers had a lot of problems with trusts on member servers
  - We knew that support for trusted domains on a member server faces very similar problems than on a domain controller
- By selling the SAMBA+ subscriptions
  - We had the opportunity to think about sponsoring our own projects
  - So we decided to bring trust support for DCs to a level were customers can really make useful use of it
  - As a side effect we were also able to solve urgent problems on domain members

The long road to trust support (Part4, after 4.5.0)

- After 4.5.0 was released in September 2016
  - SerNet got more and more customers asking for trust support
  - This was often the only reason they had to keep using Windows servers
- Other customers had a lot of problems with trusts on member servers
  - We knew that support for trusted domains on a member server faces very similar problems than on a domain controller
- By selling the SAMBA+ subscriptions
  - We had the opportunity to think about sponsoring our own projects
  - So we decided to bring trust support for DCs to a level were customers can really make useful use of it
  - As a side effect we were also able to solve urgent problems on domain members

The long road to trust support (Part4, after 4.5.0)

- After 4.5.0 was released in September 2016
  - SerNet got more and more customers asking for trust support
  - This was often the only reason they had to keep using Windows servers
- Other customers had a lot of problems with trusts on member servers
  - We knew that support for trusted domains on a member server faces very similar problems than on a domain controller
- By selling the SAMBA+ subscriptions
  - We had the opportunity to think about sponsoring our own projects
  - So we decided to bring trust support for DCs to a level were customers can really make useful use of it
  - As a side effect we were also able to solve urgent problems on domain members

The long road to trust support (Part4, 4.7.0 and more)

- The new "map untrusted to domain = auto" option
  - Was introduced to improve member server setups
  - It lets the domain controllers of the primary domain do its job
  - The member server doesn't have to know about trusted domains
  - There is just an outgoing transitive trust to the primary domain
- The "map untrusted to domain" and "auth methods" options
  - Got deprecated in 4.7.0 and removed in 4.8.0
  - The (new) default behaviour (as of 4.7.0) was kept for 4.8.0
- The "winbind scan trusted domains" option
  - With "map untrusted to domain" being removed there is no need to have a list of trusted domain available in winbindd
  - We no longer try list all trusted domain recursively
  - The option was added in 4.8.0, but the default is still "yes"
  - But the old (default) is only required for domain specific idmap backend configurations
  - As domain controller the behaviour is hardcoded to "no"

The long road to trust support (Part4, 4.7.0 and more)

- The new ”map untrusted to domain = auto” option
  - Was introduced to improve member server setups
  - It lets the domain controllers of the primary domain do its job
  - The member server doesn’t have to know about trusted domains
  - There is just an outgoing transitive trust to the primary domain
- The ”map untrusted to domain” and ”auth methods” options
  - Got deprecated in 4.7.0 and removed in 4.8.0
  - The (new) default behaviour (as of 4.7.0) was kept for 4.8.0
- The ”winbind scan trusted domains” option
  - With ”map untrusted to domain” being removed there is no need to have a list of trusted domain available in winbindd
  - We no longer try list all trusted domain recursively
  - The option was added in 4.8.0, but the default is still ”yes”
  - But the old (default) is only required for domain specific idmap backend configurations
  - As domain controller the behaviour is hardcoded to ”no”

The long road to trust support (Part4, 4.7.0 and more)

- The new "map untrusted to domain = auto" option
  - Was introduced to improve member server setups
  - It lets the domain controllers of the primary domain do its job
  - The member server doesn't have to know about trusted domains
  - There is just an outgoing transitive trust to the primary domain
- The "map untrusted to domain" and "auth methods" options
  - Got deprecated in 4.7.0 and removed in 4.8.0
  - The (new) default behaviour (as of 4.7.0) was kept for 4.8.0
- The "winbind scan trusted domains" option
  - With "map untrusted to domain" being removed there is no need to have a list of trusted domain available in winbindd
  - We no longer try list all trusted domain recursively
  - The option was added in 4.8.0, but the default is still "yes"
  - But the old (default) is only required for domain specific idmap backend configurations
  - As domain controller the behaviour is hardcoded to "no"

The long road to trust support (Part5, 4.7.0 and more)

- The most challenging task was a rewrite of gensec processing
  - Async authentication is required for to trusted domains
  - The complexity of spnego.c relied on recursing into the sync 'gensec_update()' implementation
- It took a while to create a patchset for upstream inclusion:
  - In total 31 files changed, 3774 insertions(+), 1954 deletions(-)
  - It took about 150 (relatively small) commits to make auth/gensec fully async
  - 82 patches just for spnego.c
  - The aim was to allow a reviewer to understand and verify each single commit
  - Some changes went into 4.7.0, while the rest made it into 4.8.0

The long road to trust support (Part5, 4.7.0 and more)

- The most challenging task was a rewrite of gensec processing
  - Async authentication is required for to trusted domains
  - The complexity of spnego.c relied on recursing into the sync 'gensec_update()' implementation
- It took a while to create a patchset for upstream inclusion:
  - In total 31 files changed, 3774 insertions(+), 1954 deletions(-)
  - It took about 150 (relatively small) commits to make auth/gensec fully async
  - 82 patches just for spnego.c
  - The aim was to allow a reviewer to understand and verify each single commit
  - Some changes went into 4.7.0, while the rest made it into 4.8.0

The long road to trust support (Part6, 4.8.0)

- Trusted domain support requires winbindd in 4.8.0
  - On domain members the primary domain is also a trusted domain
  - The AD DC already required and used winbindd internally
- winbindd loads the full domain topology as AD DC
  - We also load all domains of forest trusts
  - Internally we remember a "routing domain" for transitive trusts
  - Only uses NETLOGON and LSA with Netlogon Secure Channel
  - Only anonymous DCERPC transports (tcp or unauthenticated smb)
  - No NTLMSSP, no Kerberos!
  - No SAMR, no LDAP!
- LookupNames and LookupSids are routed via winbindd as AD DC
  - There are various scopes for LookupNames/Sids
  - Predefined, Builtin, Account Domain, Trusts
  - We use abstracted view tables for this
  - At the end winbindd is the last resort routing
  - Samba member servers can make use of the trust now

The long road to trust support (Part6, 4.8.0)

- Trusted domain support requires winbindd in 4.8.0
  - On domain members the primary domain is also a trusted domain
  - The AD DC already required and used winbindd internally
- winbindd loads the full domain topology as AD DC
  - We also load all domains of forest trusts
  - Internally we remember a ”routing domain” for transitive trusts
  - Only uses NETLOGON and LSA with Netlogon Secure Channel
  - Only anonymous DCERPC transports (tcp or unauthenticated smb)
  - No NTLMSSP, no Kerberos!
  - No SAMR, no LDAP!
- LookupNames and LookupSids are routed via winbindd as AD DC
  - There are various scopes for LookupNames/Sids
  - Predefined, Builtin, Account Domain, Trusts
  - We use abstracted view tables for this
  - At the end winbindd is the last resort routing
  - Samba member servers can make use of the trust now

The long road to trust support (Part6, 4.8.0)

- Trusted domain support requires winbindd in 4.8.0
  - On domain members the primary domain is also a trusted domain
  - The AD DC already required and used winbindd internally
- winbindd loads the full domain topology as AD DC
  - We also load all domains of forest trusts
  - Internally we remember a "routing domain" for transitive trusts
  - Only uses NETLOGON and LSA with Netlogon Secure Channel
  - Only anonymous DCERPC transports (tcp or unauthenticated smb)
  - No NTLMSSP, no Kerberos!
  - No SAMR, no LDAP!
- LookupNames and LookupSids are routed via winbindd as AD DC
  - There are various scopes for LookupNames/Sids
  - Predefined, Builtin, Account Domain, Trusts
  - We use abstracted view tables for this
  - At the end winbindd is the last resort routing
  - Samba member servers can make use of the trust now

The long road to trust support (Part7, 4.8.0)

- 4.8.0 was released (in March 2018) with the improvements, but had limitations:
  - It's still not possible to add users groups of a trusted domain into domain groups
- There are still security limitations:
  - No SID filtering rules are applied at all!
  - Both sides of the trust need to fully trust each other!
  - This means DCs of domain A can grant domain admin rights in domain B!

The long road to trust support (Part7, 4.8.0)

- 4.8.0 was released (in March 2018) with the improvements, but had limitations:
  - It's still not possible to add users groups of a trusted domain into domain groups
- There are still security limitations:
  - No SID filtering rules are applied at all!
  - Both sides of the trust need to fully trust each other!
  - This means DCs of domain A can grant domain admin rights in domain B!

Admin visible changes in 4.8.0 (Part1)

- Previously ”wbinfo -m –verbose” produced confusing results
  - It mixed the views recursively of all reachable domains
  - The trust types and directions don’t match the view of the local system
- This changed to be more useful in 4.8.0
  - The trust properties printed have been changed to correctly reflect the view of the system where wbinfo is executed (only!)
  - This is only correct with ”winbind scan trusted domains” effectively ”no”
  - On a domain member trusted domains are learned on the fly if used

Admin visible changes in 4.8.0 (Part1)

- Previously "wbinfo -m –verbose" produced confusing results
  - It mixed the views recursively of all reachable domains
  - The trust types and directions don't match the view of the local system
- This changed to be more useful in 4.8.0
  - The trust properties printed have been changed to correctly reflect the view of the system where wbinfo is executed (only!)
  - This is only correct with "winbind scan trusted domains" effectively "no"
  - On a domain member trusted domains are learned on the fly if used

Admin visible changes in 4.8.0 (Part2)

- Example, on a AD DC (SDOM1):

```
dc1:~$ wbinfo -m --verbose
Domain Name DNS Domain          Trust Type  Transitive  In   Out
BUILTIN                         Local
SDOM1       sdom1.site          RWDC
WDOM3       wdom3.site          Forest      Yes         No   Yes
WDOM2       wdom2.site          Forest      Yes         Yes  Yes
SUBDOM31    subdom31.wdom3.site Routed (via WDOM3)
SUBDOM21    subdom21.wdom2.site Routed (via WDOM2)
```

- Indirect (transitive) trusts are shown as "Routed" including the routing domain

Admin visible changes in 4.8.0 (Part2)

- Example, on a AD DC (SDOM1):

```
dc1:~$ wbinfo -m --verbose
Domain Name DNS Domain          Trust Type  Transitive  In   Out
BUILTIN                         Local
SDOM1       sdom1.site          RWDC
WDOM3       wdom3.site          Forest      Yes         No   Yes
WDOM2       wdom2.site          Forest      Yes         Yes  Yes
SUBDOM31    subdom31.wdom3.site Routed (via WDOM3)
SUBDOM21    subdom21.wdom2.site Routed (via WDOM2)
```

- Indirect (transitive) trusts are shown as "Routed" including the routing domain

Admin visible changes in 4.8.0 (Part3)

- Same setup, on a member of WDOM2:

```
member1:~$ wbinfo -m --verbose
Domain Name DNS Domain          Trust Type  Transitive  In   Out
BUILTIN                         Local
TITAN                           Local
WDOM2       wdom2.site          Workstation Yes         No   Yes
WDOM1       wdom1.site          Routed (via WDOM2)
WDOM3       wdom3.site          Routed (via WDOM2)
SUBDOM21    subdom21.wdom2.site Routed (via WDOM2)
SDOM1       sdom1.site          Routed (via WDOM2)
SUBDOM11    subdom11.wdom1.site Routed (via WDOM2)
```

- The list of trusts may be incomplete
- Additional domains may appear as "Routed" if a user of an unknown domain is successfully authenticated

Admin visible changes in 4.8.0 (Part3)

- Same setup, on a member of WDOM2:

```
member1:~$ wbinfo -m --verbose
Domain Name DNS Domain          Trust Type  Transitive  In   Out
BUILTIN                         Local
TITAN                           Local
WDOM2       wdom2.site          Workstation Yes         No   Yes
WDOM1       wdom1.site          Routed (via WDOM2)
WDOM3       wdom3.site          Routed (via WDOM2)
SUBDOM21    subdom21.wdom2.site Routed (via WDOM2)
SDOM1       sdom1.site          Routed (via WDOM2)
SUBDOM11    subdom11.wdom1.site Routed (via WDOM2)
```

- The list of trusts may be incomplete
- Additional domains may appear as "Routed" if a user of an unknown domain is successfully authenticated

foreignSecurityPrincipal objects (Part 1)

- Domain local (resource) groups
  - Should be able to have users/group of trusted domains as members
  - We only support one domain in our forest (yet)
  - So we have to care about just about foreignSecurityPrincipal objects (FPO)
- The ”member” attribute
  - Requires a full extended dn of an object in the local forest
  - Is an FPO-enabled attribute (as well as msDS-MembersForAzRole, msDS-NeverRevealGroup and msDS-RevealOnDemandGroup)
  - It automatically creates an FPO if a foreign extended dn sid is added
  - E.g. '<SID=S-1-5-21-123-456-789-512>' or '<SID=S-1-5-11>' does not belong to any domain in the local forest
  - CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=example,DC=com
- samba-tool group addmembers
  - Allows members to be specifiet as SID-string
  - E.g. 'S-1-5-21-123-456-789-512'
  - In master, will be in 4.9.0

foreignSecurityPrincipal objects (Part 1)

- Domain local (resource) groups
  - Should be able to have users/group of trusted domains as members
  - We only support one domain in our forest (yet)
  - So we have to care about just about foreignSecurityPrincipal objects (FPO)
- The "member" attribute
  - Requires a full extended dn of an object in the local forest
  - Is an FPO-enabled attribute (as well as msDS-MembersForAzRole, msDS-NeverRevealGroup and msDS-RevealOnDemandGroup)
  - It automatically creates an FPO if a foreign extended dn sid is added
  - E.g. '<SID=S-1-5-21-123-456-789-512>' or '<SID=S-1-5-11>' does not belong to any domain in the local forest
  - CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=example,DC=com
- samba-tool group addmembers
  - Allows members to be specifiet as SID-string
  - E.g. 'S-1-5-21-123-456-789-512'
  - In master, will be in 4.9.0

foreignSecurityPrincipal objects (Part 1)

- Domain local (resource) groups
  - Should be able to have users/group of trusted domains as members
  - We only support one domain in our forest (yet)
  - So we have to care about just about foreignSecurityPrincipal objects (FPO)
- The ”member” attribute
  - Requires a full extended dn of an object in the local forest
  - Is an FPO-enabled attribute (as well as msDS-MembersForAzRole, msDS-NeverRevealGroup and msDS-RevealOnDemandGroup)
  - It automatically creates an FPO if a foreign extended dn sid is added
  - E.g. '<SID=S-1-5-21-123-456-789-512>' or '<SID=S-1-5-11>' does not belong to any domain in the local forest
  - CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=example,DC=com
- samba-tool group addmembers
  - Allows members to be specifiet as SID-string
  - E.g. 'S-1-5-21-123-456-789-512'
  - In master, will be in 4.9.0

foreignSecurityPrincipal objects (Part 2)

Get some details of the trust

```
dc1:~$ samba-tool domain trust list
Type[Forest]   Transitive[Yes] Direction[BOTH]     Name[addom.samba.example.com]
```

```
dc1:$ samba-tool domain trust show addom.samba.example.com
LocalDomain Netbios[SAMBA2008R2] DNS[samba2008r2.example.com] SID[S-1-5-21-123-456-789]
TrustedDomain:

NetbiosName:    ADDOMAIN
DnsName:        addom.samba.example.com
SID:            S-1-5-21-987-654-321
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[4] TDO[addom.samba.example.com]:
TLN: Status[Enabled] DNS[*.ADDOM.SAMBA.EXAMPLE.COM.upn]
TLN: Status[Enabled] DNS[*.ADDOM.SAMBA.EXAMPLE.COM.spn]
TLN: Status[Enabled] DNS[*.addom.samba.example.com]
DOM: Status[Enabled] DNS[addom.samba.example.com] Netbios[ADDOMAIN]
                     SID[S-1-5-21-987-654-321]
```

foreignSecurityPrincipal objects (Part 2)

Get some details of the trust

```
dc1:~$ samba-tool domain trust list
Type[Forest]   Transitive[Yes] Direction[BOTH]     Name[addom.samba.example.com]
```

```
dc1:$ samba-tool domain trust show addom.samba.example.com
LocalDomain Netbios[SAMBA2008R2] DNS[samba2008r2.example.com] SID[S-1-5-21-123-456-789]
TrustedDomain:

NetbiosName:    ADDOMAIN
DnsName:        addom.samba.example.com
SID:            S-1-5-21-987-654-321
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[4] TDO[addom.samba.example.com]:
TLN: Status[Enabled] DNS[*.ADDOM.SAMBA.EXAMPLE.COM.upn]
TLN: Status[Enabled] DNS[*.ADDOM.SAMBA.EXAMPLE.COM.spn]
TLN: Status[Enabled] DNS[*.addom.samba.example.com]
DOM: Status[Enabled] DNS[addom.samba.example.com] Netbios[ADDOMAIN]
                     SID[S-1-5-21-987-654-321]
```

foreignSecurityPrincipal objects (Part 3)

How to add 'ADDOMAIN\Domain Admins' to 'SAMBA2008R2\Domain Admins'

```
dc1:$ wbinfo --name-to-sid 'ADDOMAIN\Domain␣Admins'
S-1-5-21-987-654-321-512 SID_DOM_GROUP (2)
```

```
dc1:$ samba-tool group listmembers 'Domain␣Admins'
Administrator
```

```
dc1:$ samba-tool group addmembers 'Domain␣Admins' S-1-5-21-987-654-321-512
Added members to group Domain Admins
```

```
dc1:$ samba-tool group listmembers 'Domain␣Admins'
Administrator
S-1-5-21-987-654-321-512
```

foreignSecurityPrincipal objects (Part 3)

How to add 'ADDOMAIN\Domain Admins' to 'SAMBA2008R2\Domain Admins'

```
dc1:$ wbinfo --name-to-sid 'ADDOMAIN\Domain␣Admins'
S-1-5-21-987-654-321-512 SID_DOM_GROUP (2)
```

```
dc1:$ samba-tool group listmembers 'Domain␣Admins'
Administrator
```

```
dc1:$ samba-tool group addmembers 'Domain␣Admins' S-1-5-21-987-654-321-512
Added members to group Domain Admins
```

```
dc1:$ samba-tool group listmembers 'Domain␣Admins'
Administrator
S-1-5-21-987-654-321-512
```

foreignSecurityPrincipal objects (Part 3)

How to add 'ADDOMAIN\Domain Admins' to 'SAMBA2008R2\Domain Admins'

```
dc1:$ wbinfo --name-to-sid ’ADDOMAIN\Domain␣Admins’
S-1-5-21-987-654-321-512 SID_DOM_GROUP (2)
```

```
dc1:$ samba-tool group listmembers ’Domain␣Admins’
Administrator
```

```
dc1:$ samba-tool group addmembers ’Domain␣Admins’ S-1-5-21-987-654-321-512
Added members to group Domain Admins
```

```
dc1:$ samba-tool group listmembers ’Domain␣Admins’
Administrator
S-1-5-21-987-654-321-512
```

foreignSecurityPrincipal objects (Part 3)

How to add 'ADDOMAIN\Domain Admins' to 'SAMBA2008R2\Domain Admins'

```
dc1:$ wbinfo --name-to-sid 'ADDOMAIN\Domain␣Admins'
S-1-5-21-987-654-321-512 SID_DOM_GROUP (2)
```

```
dc1:$ samba-tool group listmembers 'Domain␣Admins'
Administrator
```

```
dc1:$ samba-tool group addmembers 'Domain␣Admins' S-1-5-21-987-654-321-512
Added members to group Domain Admins
```

```
dc1:$ samba-tool group listmembers 'Domain␣Admins'
Administrator
S-1-5-21-987-654-321-512
```

SID-Expanding (Part1)

- Domain local (resource) groups
  - Need to be expanded before using the received authorization token
  - Before expanding the BUILTIN groups for local authentication
  - Before returning netr_LogonSamLogon[{WithFlags,Ex}]()
  - Before returning CROSS-REALM Kerberos Tickets

- We have this in authsam_update_user_info_dc()
  - Called from source4/auth/ntlm/auth_winbind.c
  - Called from source4/kdc/pac-glue.c
  - In master, will be in 4.9.0

- Some TODOs...
  - We don't add SE_GROUP_RESOURCE yes
  - We don't use resource group compression for Kerberos
  - We pass resource / domain local groups via the trust

SID-Expanding (Part1)

- Domain local (resource) groups
  - Need to be expanded before using the received authorization token
  - Before expanding the BUILTIN groups for local authentication
  - Before returning netr_LogonSamLogon[{WithFlags,Ex}]()
  - Before returning CROSS-REALM Kerberos Tickets

- We have this in authsam_update_user_info_dc()
  - Called from source4/auth/ntlm/auth_winbind.c
  - Called from source4/kdc/pac-glue.c
  - In master, will be in 4.9.0

- Some TODOs...
  - We don't add SE_GROUP_RESOURCE yes
  - We don't use resource group compression for Kerberos
  - We pass resource / domain local groups via the trust

SID-Expanding (Part1)

- Domain local (resource) groups
  - Need to be expanded before using the received authorization token
  - Before expanding the BUILTIN groups for local authentication
  - Before returning netr_LogonSamLogon[{WithFlags,Ex}]()
  - Before returning CROSS-REALM Kerberos Tickets
- We have this in authsam_update_user_info_dc()
  - Called from source4/auth/ntlm/auth_winbind.c
  - Called from source4/kdc/pac-glue.c
  - In master, will be in 4.9.0
- Some TODOs...
  - We don't add SE_GROUP_RESOURCE yes
  - We don't use resource group compression for Kerberos
  - We pass resource / domain local groups via the trust

SID-Expanding (Part2)

The fully expanded token of a authentication of a user from a trusted domain

```
dc1:$ ldbsearch -H ldap://dc1.samba2008r2.example.com -UADDOMAIN\Administrator" -b "" -s
     base tokenGroups
# record 1
dn:
tokenGroups: S-1-5-21-987-654-321-500
tokenGroups: S-1-5-21-987-654-321-513
tokenGroups: S-1-5-21-987-654-321-512
tokenGroups: S-1-5-21-987-654-321-572
tokenGroups: S-1-5-21-987-654-321-518
tokenGroups: S-1-5-21-987-654-321-519
tokenGroups: S-1-5-21-987-654-321-520
tokenGroups: S-1-5-21-123-456-789-1109
tokenGroups: S-1-5-21-123-456-789-512
tokenGroups: S-1-5-21-123-456-789-572
tokenGroups: S-1-1-0
tokenGroups: S-1-5-2
tokenGroups: S-1-5-11
tokenGroups: S-1-5-64-10
tokenGroups: S-1-5-32-544
tokenGroups: S-1-5-32-545
tokenGroups: S-1-5-32-554
```

Resource / domain local groups (type 4) should not be passed, needs to be fixed!

```
dc1:$ wbinfo --sid-to-name S-1-5-21-987-654-321-572
ADDOMAIN\Denied RODC Password Replication Group 4
```

SID-Expanding (Part2)

The fully expanded token of a authentication of a user from a trusted domain

```
dc1:$ ldbsearch -H ldap://dc1.samba2008r2.example.com -UADDOMAIN\Administrator" -b "" -s
     base tokenGroups
# record 1
dn:
tokenGroups: S-1-5-21-987-654-321-500
tokenGroups: S-1-5-21-987-654-321-513
tokenGroups: S-1-5-21-987-654-321-512
tokenGroups: S-1-5-21-987-654-321-572
tokenGroups: S-1-5-21-987-654-321-518
tokenGroups: S-1-5-21-987-654-321-519
tokenGroups: S-1-5-21-987-654-321-520
tokenGroups: S-1-5-21-123-456-789-1109
tokenGroups: S-1-5-21-123-456-789-512
tokenGroups: S-1-5-21-123-456-789-572
tokenGroups: S-1-1-0
tokenGroups: S-1-5-2
tokenGroups: S-1-5-11
tokenGroups: S-1-5-64-10
tokenGroups: S-1-5-32-544
tokenGroups: S-1-5-32-545
tokenGroups: S-1-5-32-554
```

Resource / domain local groups (type 4) should not be passed, needs to be fixed!

```
dc1:$ wbinfo --sid-to-name S-1-5-21-987-654-321-572
ADDOMAIN\Denied RODC Password Replication Group 4
```

SID-Filtering (Part 1)

- A trusted domain could spoof an authorization token
  - Local admin privileges could be gained
  - Very critical in case of cross organization trusts
  - See [MS-PAC] 4.1.2 Authorization Validation and Filtering
- Based on the documentation (and some further thinking)
  - I added dom_sid_filter_token_sid() and dom_sid_filter_{domain,upn}_name()
  - They operate on just one sid or name
  - They take the local domain/forest information
  - They take the used secure channel type
  - They take the remote domain/forest information
- authsam_update_user_info_dc() also filters
  - We filter SIDs as well as names using the helper functions
  - Used in source4/kdc/pac-glue.c
  - source4/auth/ntlm/auth_winbind.c can't filter, uses SEC_CHAN_BDC
  - only winbindd has the remote domain/forest information

SID-Filtering (Part 1)

- A trusted domain could spoof an authorization token
  - Local admin privileges could be gained
  - Very critical in case of cross organization trusts
  - See [MS-PAC] 4.1.2 Authorization Validation and Filtering
- Based on the documentation (and some further thinking)
  - I added dom_sid_filter_token_sid() and dom_sid_filter_{domain,upn}_name()
  - They operate on just one sid or name
  - They take the local domain/forest information
  - They take the used secure channel type
  - They take the remote domain/forest information
- authsam_update_user_info_dc() also filters
  - We filter SIDs as well as names using the helper functions
  - Used in source4/kdc/pac-glue.c
  - source4/auth/ntlm/auth_winbind.c can't filter, uses SEC_CHAN_BDC
  - only winbindd has the remote domain/forest information

SID-Filtering (Part 1)

- A trusted domain could spoof an authorization token
  - Local admin privileges could be gained
  - Very critical in case of cross organization trusts
  - See [MS-PAC] 4.1.2 Authorization Validation and Filtering
- Based on the documentation (and some further thinking)
  - I added dom_sid_filter_token_sid() and dom_sid_filter_{domain,upn}_name()
  - They operate on just one sid or name
  - They take the local domain/forest information
  - They take the used secure channel type
  - They take the remote domain/forest information
- authsam_update_user_info_dc() also filters
  - We filter SIDs as well as names using the helper functions
  - Used in source4/kdc/pac-glue.c
  - source4/auth/ntlm/auth_winbind.c can't filter, uses SEC_CHAN_BDC
  - only winbindd has the remote domain/forest information

SID-Filtering (Part 2)

- Filtering in winbindd...
  - netr_LogonSamLogon[{WithFlags,Ex}]() results are filtered
  - lsa_Lookup{Sids,Names}() results are filtered
  - pdb_filter_hints() and pdb_update_validation() are added
  - pdb_samba_dsdb implements this for the AD DC
  - All non AD DC roles still get local SAM, BUILTIN protection

- Work in progress...
  - git://git.samba.org/metze/samba/wip.git
  - master3-trusts-ok
  - master3-trusts-tmp
  - master3-trusts
  - Planed to be ready before 4.9.0

SID-Filtering (Part 2)

- Filtering in winbindd...
  - netr_LogonSamLogon[{WithFlags,Ex}]() results are filtered
  - lsa_Lookup{Sids,Names}() results are filtered
  - pdb_filter_hints() and pdb_update_validation() are added
  - pdb_samba_dsdb implements this for the AD DC
  - All non AD DC roles still get local SAM, BUILTIN protection
- Work in progress...
  - git://git.samba.org/metze/samba/wip.git
  - master3-trusts-ok
  - master3-trusts-tmp
  - master3-trusts
  - Planed to be ready before 4.9.0

Forest/Domain-wide Authentication

- Forest/Domain-wide Authentication (the default) allows:
  - Authentication of each principal of the trusted forest/domain
  - Authentication to each service in the trusting forest/domain

- Authorization is handled by:
  - Using ACLs on individual resources (objects, files, ...)
  - Access might be granted just by "Authenticated Users" ACEs

- One-way trusts:
  - Often used to limit the authentication between organizations
  - Make the use of S4U2Self impossible

Forest/Domain-wide Authentication

- Forest/Domain-wide Authentication (the default) allows:
  - Authentication of each principal of the trusted forest/domain
  - Authentication to each service in the trusting forest/domain
- Authorization is handled by:
  - Using ACLs on individual resources (objects, files, ...)
  - Access might be granted just by "Authenticated Users" ACEs
- One-way trusts:
  - Often used to limit the authentication between organizations
  - Make the use of S4U2Self impossible

Forest/Domain-wide Authentication

- Forest/Domain-wide Authentication (the default) allows:
  - Authentication of each principal of the trusted forest/domain
  - Authentication to each service in the trusting forest/domain
- Authorization is handled by:
  - Using ACLs on individual resources (objects, files, ...)
  - Access might be granted just by "Authenticated Users" ACEs
- One-way trusts:
  - Often used to limit the authentication between organizations
  - Make the use of S4U2Self impossible

Selective Authentication (Cross Organization Trusts) (Part1)

- Trusts can be marked for selective authentication:
  - Using LSA_TRUST_ATTRIBUTE_CROSS_ORGANIZATION
  - The trusting end adds the OTHER_ORGANIZATION SID (S-1-5-1000) to any token
  - By default authentication of trusted principals to trusting services is rejected with STATUS_AUTHENTICATION_FIREWALL_FAILED
- Selective authentication checking:
  - Only done if the token contains S-1-5-1000
  - The "AllowedToAuthenticateTo" extended access right is required on the AD object of the service
- Advantages of selective authentication:
  - It is much more flexible than the all or nothing of one-way trusts
  - It allows S4U2Self to work

Selective Authentication (Cross Organization Trusts) (Part1)

- Trusts can be marked for selective authentication:
    - Using LSA_TRUST_ATTRIBUTE_CROSS_ORGANIZATION
    - The trusting end adds the OTHER_ORGANIZATION SID (S-1-5-1000) to any token
    - By default authentication of trusted principals to trusting services is rejected with STATUS_AUTHENTICATION_FIREWALL_FAILED
- Selective authentication checking:
    - Only done if the token contains S-1-5-1000
    - The "AllowedToAuthenticateTo" extended access right is required on the AD object of the service
- Advantages of selective authentication:
    - It is much more flexible than the all or nothing of one-way trusts
    - It allows S4U2Self to work

Selective Authentication (Cross Organization Trusts) (Part1)

- Trusts can be marked for selective authentication:
  - Using LSA_TRUST_ATTRIBUTE_CROSS_ORGANIZATION
  - The trusting end adds the OTHER_ORGANIZATION SID (S-1-5-1000) to any token
  - By default authentication of trusted principals to trusting services is rejected with STATUS_AUTHENTICATION_FIREWALL_FAILED
- Selective authentication checking:
  - Only done if the token contains S-1-5-1000
  - The "AllowedToAuthenticateTo" extended access right is required on the AD object of the service
- Advantages of selective authentication:
  - It is much more flexible than the all or nothing of one-way trusts
  - It allows S4U2Self to work

Selective Authentication (Cross Organization Trusts) (Part2)

- authsam_update_user_info_dc() also "selects"
  - We pass 'struct ldb_dn *local_service_dn' is the target is within the local domain
  - authsam_extract_local_service_dn() gets it from auth_usersupplied_info
  - We need Heimdal changes to pass the required information to the pac [re-]generation hooks
  - We may need Heimdal/MIT changes to return STATUS_AUTHENTICATION_FIREWALL_FAILED blobs to TGS requests
- Work in progress...
  - git://git.samba.org/metze/samba/wip.git
  - master3-trusts-ok
  - master3-trusts-tmp
  - master3-trusts
  - Needs 'samba-tool' commands for "AllowedToAuthenticateTo" ACEs
  - Planed to be ready before 4.9.0

Selective Authentication (Cross Organization Trusts) (Part2)

- authsam_update_user_info_dc() also ”selects”
  - We pass 'struct ldb_dn *local_service_dn' is the target is within the local domain
  - authsam_extract_local_service_dn() gets it from auth_usersupplied_info
  - We need Heimdal changes to pass the required information to the pac [re-]generation hooks
  - We may need Heimdal/MIT changes to return STATUS_AUTHENTICATION_FIREWALL_FAILED blobs to TGS requests
- Work in progress...
  - git://git.samba.org/metze/samba/wip.git
  - master3-trusts-ok
  - master3-trusts-tmp
  - master3-trusts
  - Needs 'samba-tool' commands for ”AllowedToAuthenticateTo” ACEs
  - Planed to be ready before 4.9.0

Future Improvements / Open Bugs

- Open bugs...
  - Bug 11362: GPO security filtering based on the groups in Kerberos PAC (but primary group is missing)
  - Bug 11517: Samba 4.3 GPO issue when Trust is enabled
- TODOs...
  - Fix some NETLOGON calls which return details about trusted domains
  - A lot more tests to verify we construct the PAC exactly like Windows
  - A low level kerberos testsuite (most likely as python bindings)
  - More Kerberos features from Windows 2012 and higher
  - See the last years slides for more topics and references

Future Improvements / Open Bugs

- Open bugs...
  - Bug 11362: GPO security filtering based on the groups in Kerberos PAC (but primary group is missing)
  - Bug 11517: Samba 4.3 GPO issue when Trust is enabled
- TODOs...
  - Fix some NETLOGON calls which return details about trusted domains
  - A lot more tests to verify we construct the PAC exactly like Windows
  - A low level kerberos testsuite (most likely as python bindings)
  - More Kerberos features from Windows 2012 and higher
  - See the last years slides for more topics and references

Questions?

- Stefan Metzmacher, `metze@samba.org`
- https://www.sernet.com