ERNW
providing security.

ERNW WHITEPAPER 67

ACTIVE DIRECTORY TRUST CONSIDERATIONS

Version:	1.0
Date:	11.12.2018
Classification:	Public
Author:	Christoph Kuderna (infoWAN) & Enno Rey

Friedw
art
Kuhn

Digitally signed
by Friedwart
Kuhn
Date: 2018.12.11
13:19:38 +01'00'

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

1 Introduction

End of November Will "harmj0y" Schroeder published an excellent technical post titled "Not A Security Boundary: Breaking Forest Trusts"[1] in which he lays out how a highly security-critical compromise can be achieved across a forest boundary, resulting from a combination of default Active Directory (security) settings and a new attack method.

As of his writing the basis for the attack path is an existing two-way trust between two Active Directory forests. Trusts and their security implications have been the topic of many discussions in the last years while at the same time many enterprise organizations have quite a few AD trusts in their environments, for historical reasons and due to mergers & acquisitions.

Christoph Kuderna from infoWAN and JD from ERNW's Active Directory Security team are currently working in an organization where this exact discussion is happening right now. One of the outcomes of said project is a document discussing the risks of AD trusts, together with some mitigation approaches.

We've decided to extract some parts of this document in order to contribute to well-informed decision taking in the context of AD trusts.

The document discusses security aspects of establishing Active Directory trust relationships between the customer's Active Directory forest and other domains/forests. The primary use case has users from an external AD domain accessing their Exchange mailboxes hosted on servers in the company domain ("dir.company.com") with Kerberos as the preferred authentication protocol. In Active Directory terminology the direction of trust is opposite to the direction of access, thus the company's forest ("dir.company.com") needs to trust the partner's AD domain. The document hence focuses on the scenario of a one-way trust where the dir.company.com (="company") AD-forest trusts the partner's AD forest, but not the other way around.

[1] *https://www.harmj0y.net/blog/redteaming/not-a-security-boundary-breaking-forest-trusts/*

The following picture shows the typical scenario where the trusting domain would be company AD on the left side and the trusted domain would be the partners AD on the right side:

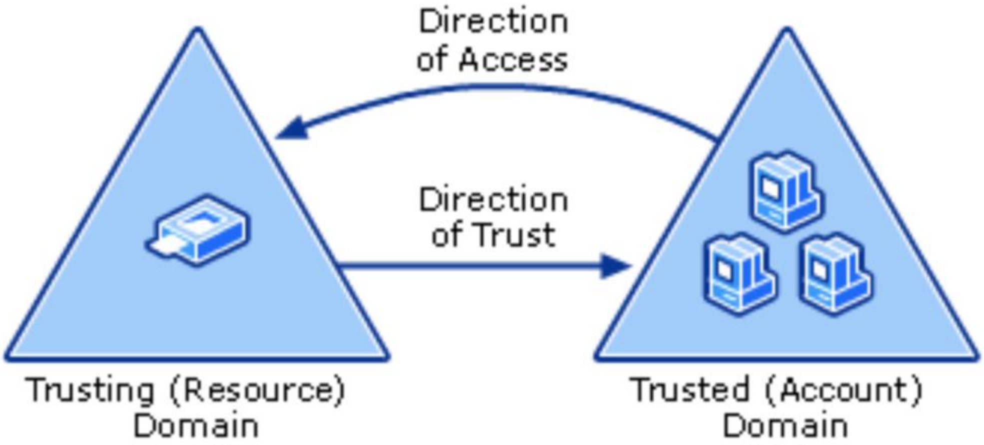


Figure 1: Direction of Access and Direction of Trust between Trusting (Resource) Domain and Trusted (Account) Domain

Even if dir.company.com trusts multiple other AD domains in this way, the trust relationships do not extend to the external domains themselves, meaning if dir.company.com trusts Domain A and Domain B, there is still no trust whatsoever between Domain A and Domain B.

Microsoft has outlined general trust considerations in a blog post: https://blogs.technet.microsoft.com/askpfeplat/2017/02/13/top-ten-issues-with-active-directory-trusts-and-corporate-mergers/

2 General Guidelines Regarding Active Directory Trusts

To avoid common risks resulting from trust relationships, the customer defined the following general guidelines for AD trusts in dir.company.com:

- Trust relationships must only be created on an as-needed basis and after prior approval.
- They **must** only be created in the required directions. Unidirectional trusts should always be preferred, each trust direction must be justified.
- SID Filtering **must** be enabled. This means that when a partner user wants to access a resource in dir.company.com over the trust relationship, the access token is filtered and all SIDs not originating from the partners domain are removed. This may lead to "access denied" issues, if a partner's AD forest consists of more than one domain or if SIDs from previous migrations are still required for resource access and that resource is migrated to the dir.company.com domain later.
  SID Filtering implicitly disables the use of SID-History.
- The trust should be configured for AES encryption.
- Trusts should be configured in such a way that Kerberos authentication is working, preferably as forest trusts instead of external trusts.
- As a default Selective Authentication **must** be turned on. Exceptions must be explicitly approved by company's Tier 0 administrators. Application owners need to provide Tier 0 administrators with the lists of systems where the ALLOWED TO AUTHENTICATE right must be configured for their service to be usable by users from trusted domains.
  Note: external Active Directory trusts and inter-forest Active Directory trusts are by default non-transitive, meaning that a trust created between a partner's Active Directory environment and the company AD never extends to any other domain of another forest trusted by dir.company.com or the partner's AD. The only possible exception would be other domains located in the same AD forest if the partner's AD forest consists of more than one domain.
- Since users from trusted domains are AUTHENTICATED USERS in the trusting domain, no matter from which trusted domain they originate, permissions in the trusting domain (dir.company.com) should not use the AUTHENTICATED USERS group for granting access.
- Any kind of administrative access to the dir.company.com domain, and the resources in it, must never be granted to accounts from partner directories. Administrative accounts must be in dir.company.com. The membership in administrative groups must be monitored, any unapproved members must be removed immediately. Without this limitation a compromise in the partners Active Directory could affect services in dir.company.com.

2.1 Monitoring of Trusts

Windows creates the required event log entries if the Audit Policy on Domain Controllers (defined in the Default Domain Controllers Policy) is configured correctly.

From Microsoft's "Windows 10 and Windows Server 2016 Security Auditing and Monitoring Reference" document: *"**Audit Authentication Policy Change** determines whether the operating system generates audit events when changes are made to authentication policy."*

Changes made to authentication policy include:

- Creation, modification, and removal of forest and domain trusts.
- Changes to Kerberos policy under Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy.
- When any of the following user logon rights is granted to a user or group:
  - Access this computer from the network
  - Allow logon locally
  - Allow logon through Remote Desktop
  - Logon as a batch job
  - Logon as a service
- Namespace collisions, such as when an added trust collides with an existing namespace name.

This setting is useful for tracking changes on domain-level and forest-level trust and privileges that are granted to user accounts or groups.

Event volume: Low.

Computer Type	General	Stronger	Comments
Domain Controller	Success Yes	Success Yes	On Domain Controllers, it is important to enable Success audit for this subcategory to be able to get information related to operations with domain and forest trusts, changes in Kerberos policy and some other events included in this subcategory.
	Failure No	Failure No	This subcategory doesn't have failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Table 1 Event Log configuration Domain Controller

The following events belong to this category:

- 4670: Permissions on an object were changed
- 4706: A new trust was created to a domain.
- 4707: A trust to a domain was removed.
- 4716: Trusted domain information was modified.
- 4713: Kerberos policy was changed.
- 4717: System security access was granted to an account.
- 4718: System security access was removed from an account.
- 4739: Domain Policy was changed.
- 4864: A namespace collision was detected.
- 4865: A trusted forest information entry was added.
- 4866: A trusted forest information entry was removed.
- 4867: A trusted forest information entry was modified.

Any changes in Active Directory forest trust settings must be monitored and alerts should be triggered for these events.

The Microsoft document also contains many details on the information in each of the events.

3 Creating a Trust Relationship in dir.company.com

A trust relationship can only be established with administrative rights on both sides of the trust. During the creation of the trust a trust password is agreed upon which is automatically changed on a regular basis (by default every 30 days). The current trust password must be known to Domain Controllers on both sides of the trust to create or consume the referral tickets required for resource access.

3.1 Trust Creation and Verification

DNS name resolution in both directions must already be in place. We recommend the use of Conditional Forwarders.

Since neither the old NETDOM command-line tool nor a PowerShell cmdlet can be used to create a forest trust, the GUI tool AD DOMAINS AND TRUSTS will be used.

The following screenshots show the setup with a sample partner domain called example.dir:

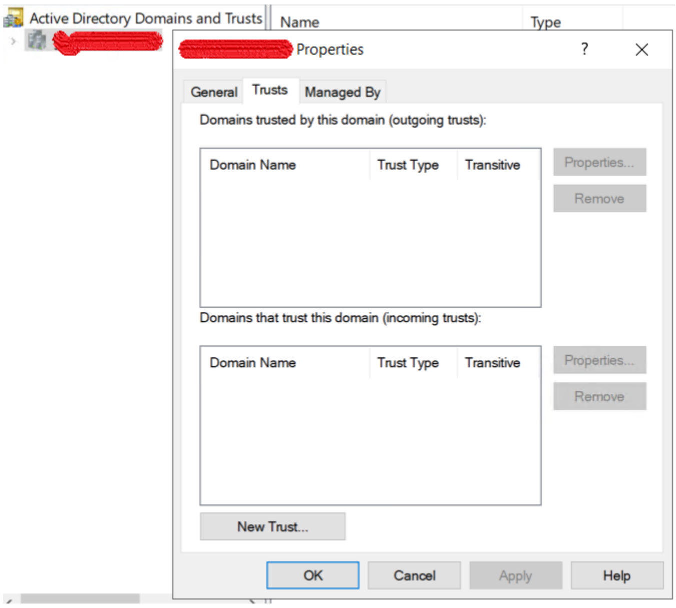
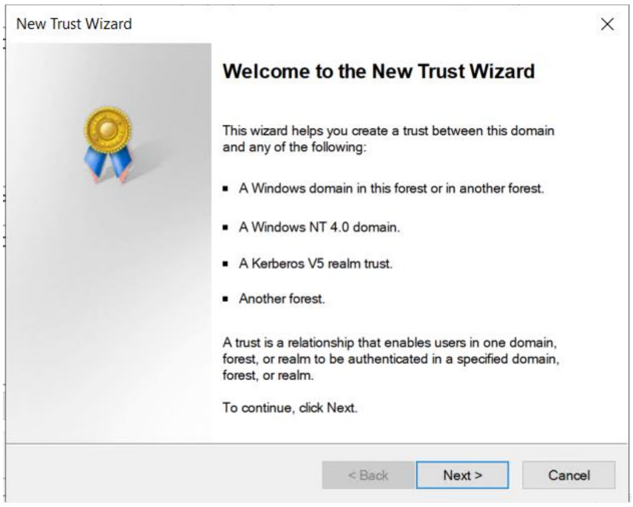


Figure 2: Screenshot setup with a sample partner domain called example.dir



New Trust Wizard

Welcome to the New Trust Wizard

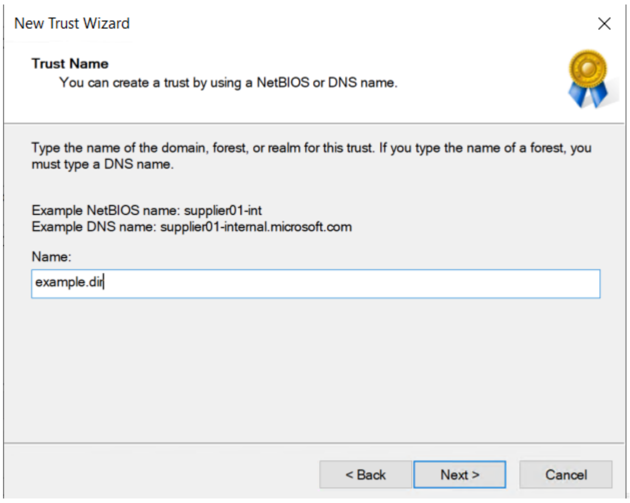
This wizard helps you create a trust between this domain and any of the following:

- A Windows domain in this forest or in another forest.
- A Windows NT 4.0 domain.
- A Kerberos V5 realm trust.
- Another forest.

A trust is a relationship that enables users in one domain, forest, or realm to be authenticated in a specified domain, forest, or realm.

To continue, click Next.

Figure 3: After clicking "New Trust"



New Trust Wizard

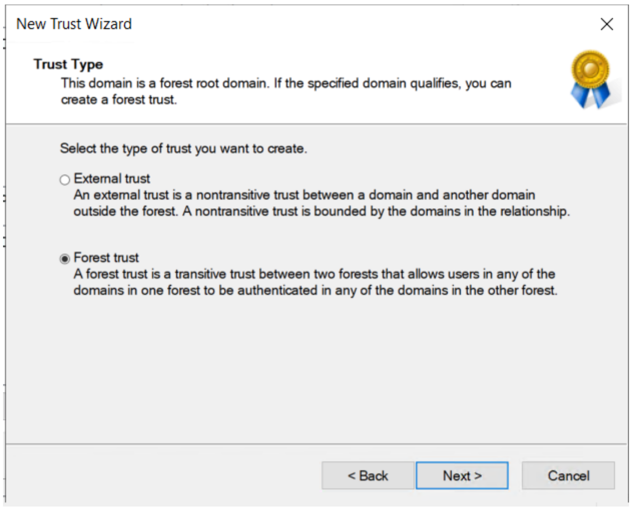
Trust Name
You can create a trust by using a NetBIOS or DNS name.

Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.

Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com

Name: example.dir

Figure 4: Specify the name of the domain to be trusted



New Trust Wizard

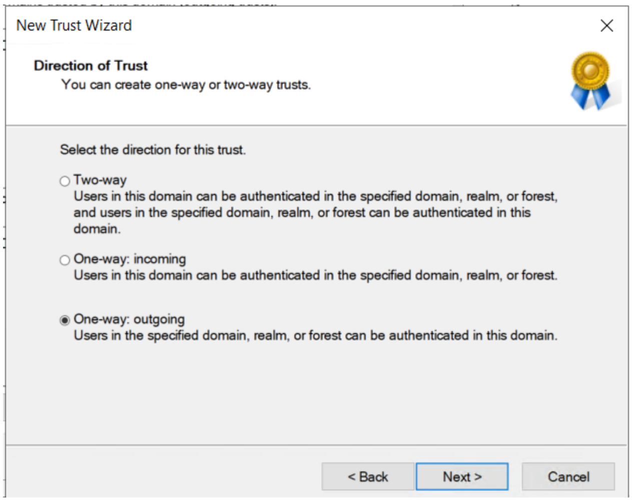
Trust Type
This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.

Select the type of trust you want to create.

○ External trust
An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.

● Forest trust
A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.

Figure 5: Change the setting to FOREST TRUST



New Trust Wizard

Direction of Trust
You can create one-way or two-way trusts.

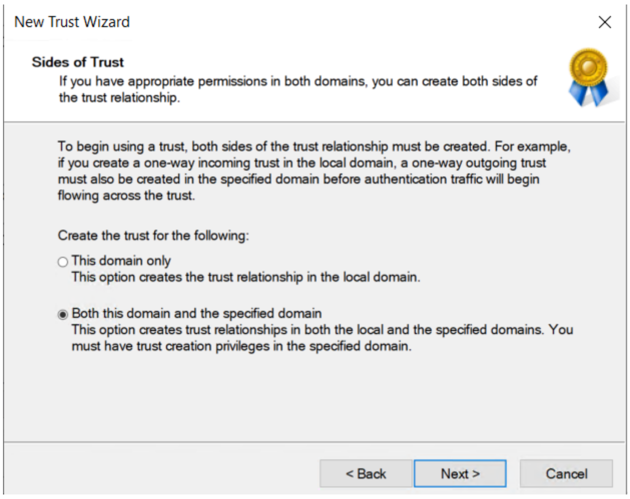
Select the direction for this trust.

○ Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.

○ One-way: incoming
Users in this domain can be authenticated in the specified domain, realm, or forest.

● One-way: outgoing
Users in the specified domain, realm, or forest can be authenticated in this domain.

Figure 6: Users from example.dir must be able to access resources in dir.company.com thus requiring a one-way outgoing trust



New Trust Wizard

Sides of Trust
If you have appropriate permissions in both domains, you can create both sides of the trust relationship.

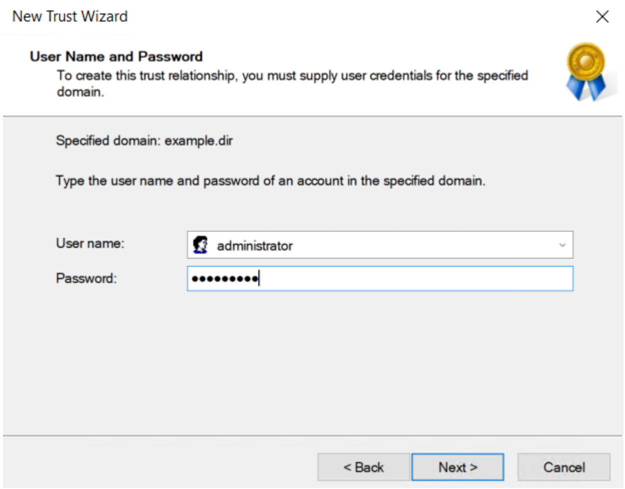
To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.

Create the trust for the following:

○ This domain only
This option creates the trust relationship in the local domain.

● Both this domain and the specified domain
This option creates trust relationships in both the local and the specified domains. You must have trust creation privileges in the specified domain.

Figure 7: For simplification, we assume that admin credentials from both domains are available. If that is not the case, the setup can be completed separately on both sides, if a required initial trust password is exchanged securely between the admins.



New Trust Wizard

User Name and Password
To create this trust relationship, you must supply user credentials for the specified domain.

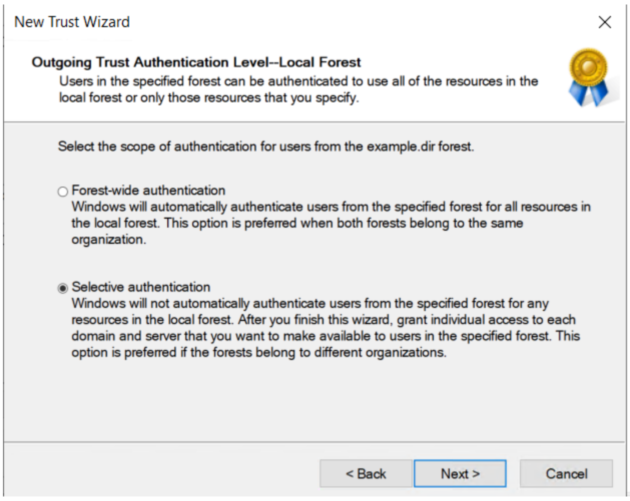
Specified domain: example.dir

Type the user name and password of an account in the specified domain.

User name: administrator

Password: •••••••••

Figure 8: Screenshot setup with a sample partner domain called example.dir



New Trust Wizard

Outgoing Trust Authentication Level--Local Forest

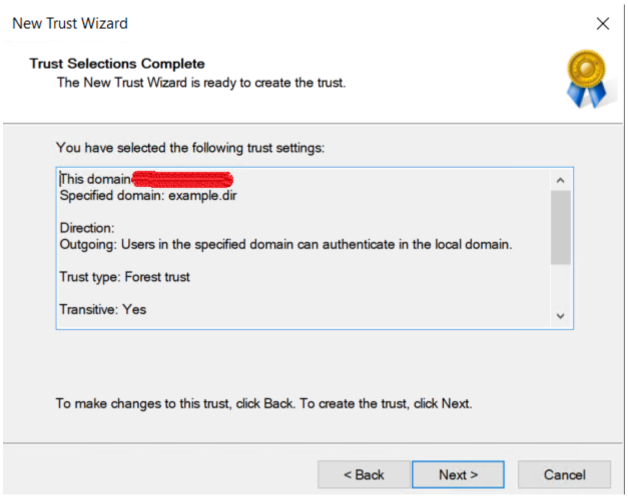
Users in the specified forest can be authenticated to use all of the resources in the local forest or only those resources that you specify.

Select the scope of authentication for users from the example.dir forest.

○ Forest-wide authentication
Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.

● Selective authentication
Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you finish this wizard, grant individual access to each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.

Figure 9: Authentication must be changed to Selective Authentication



New Trust Wizard

Trust Selections Complete

The New Trust Wizard is ready to create the trust.

You have selected the following trust settings:

This domain[redacted]
Specified domain: example.dir

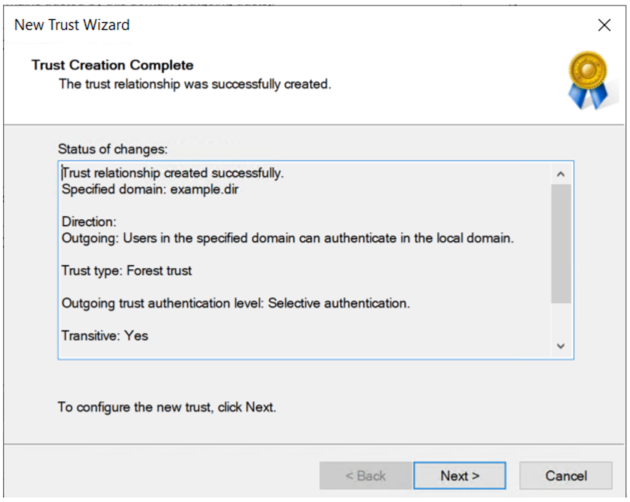
Direction:
Outgoing: Users in the specified domain can authenticate in the local domain.

Trust type: Forest trust

Transitive: Yes

To make changes to this trust, click Back. To create the trust, click Next.

Figure 10: Screenshot setup with a sample partner domain called example.dir



Trust Creation Complete
The trust relationship was successfully created.

Status of changes:

Trust relationship created successfully.
Specified domain: example.dir

Direction:
Outgoing: Users in the specified domain can authenticate in the local domain.

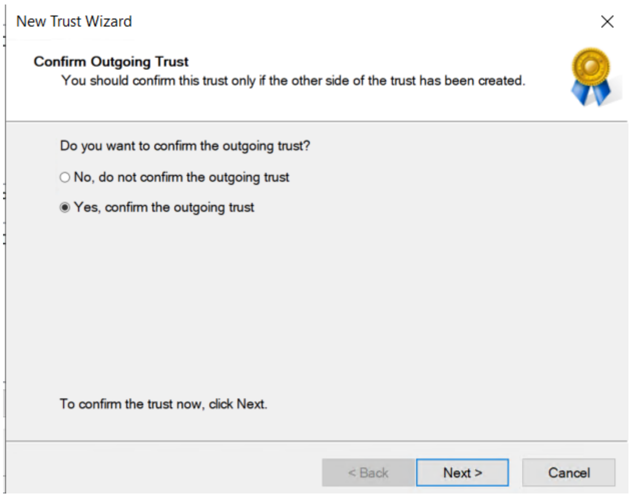
Trust type: Forest trust

Outgoing trust authentication level: Selective authentication.

Transitive: Yes

To configure the new trust, click Next.

Figure 11: Screenshot setup with a sample partner domain called example.dir



Confirm Outgoing Trust
You should confirm this trust only if the other side of the trust has been created.

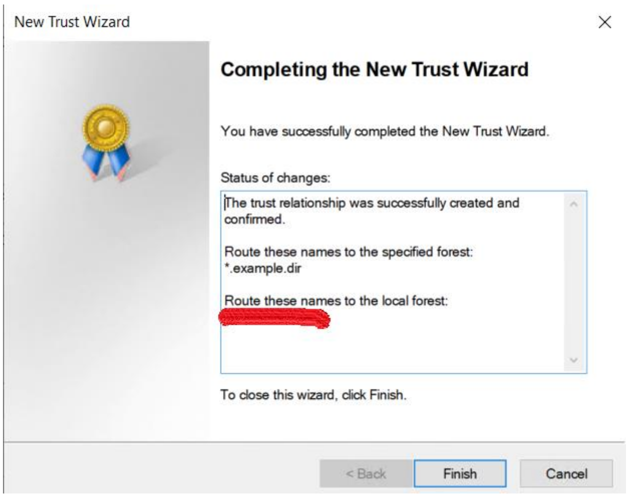
Do you want to confirm the outgoing trust?

○ No, do not confirm the outgoing trust

● Yes, confirm the outgoing trust

To confirm the trust now, click Next.

Figure 12: Screenshot setup with a sample partner domain called example.dir



New Trust Wizard

Completing the New Trust Wizard

You have successfully completed the New Trust Wizard.

Status of changes:

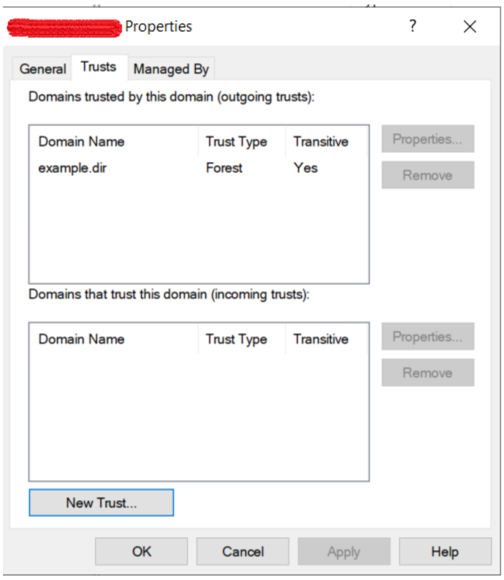
The trust relationship was successfully created and confirmed.

Route these names to the specified forest:
*.example.dir

Route these names to the local forest:
[redacted]

To close this wizard, click Finish.

Figure 13: Screenshot setup with a sample partner domain called example.dir



[redacted] Properties

Domains trusted by this domain (outgoing trusts):

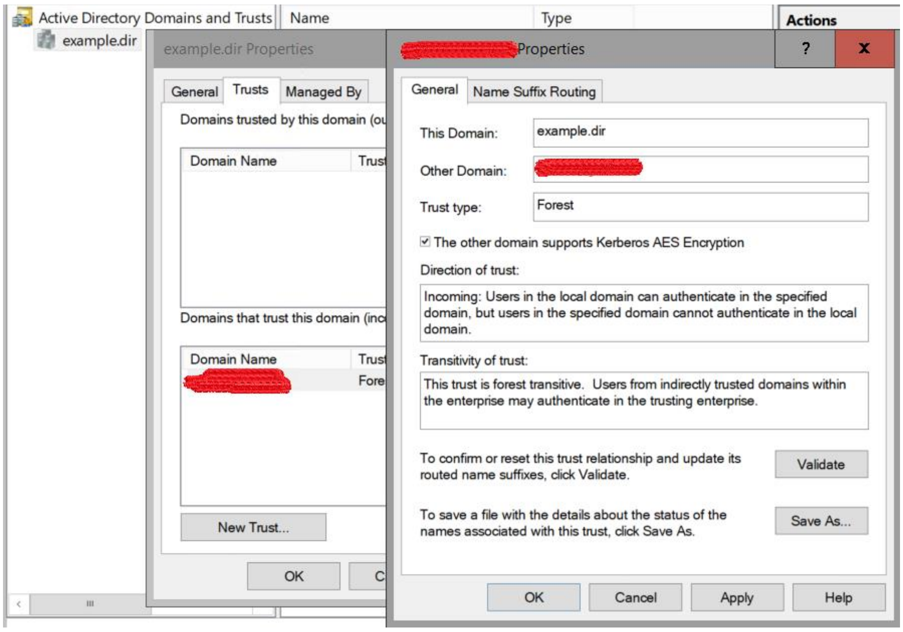
Domain Name	Trust Type	Transitive
example.dir	Forest	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive

Figure 14: Screenshot setup with a sample partner domain called example.dir

In the partner domain the trust properties should then be opened and the check box "The other domain supports Kerberos AES Encryption" should be checked. This requires Windows Server 2008 R2+ Domain Controllers and a Domain Functional Level of at least Windows Server 2008 R2, both of which are the case for dir.company.com.



Domains trusted by this domain (ou

Domains that trust this domain (inc

Domain Name: [redacted]

[redacted] Properties

This Domain: example.dir

Other Domain: [redacted]

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.

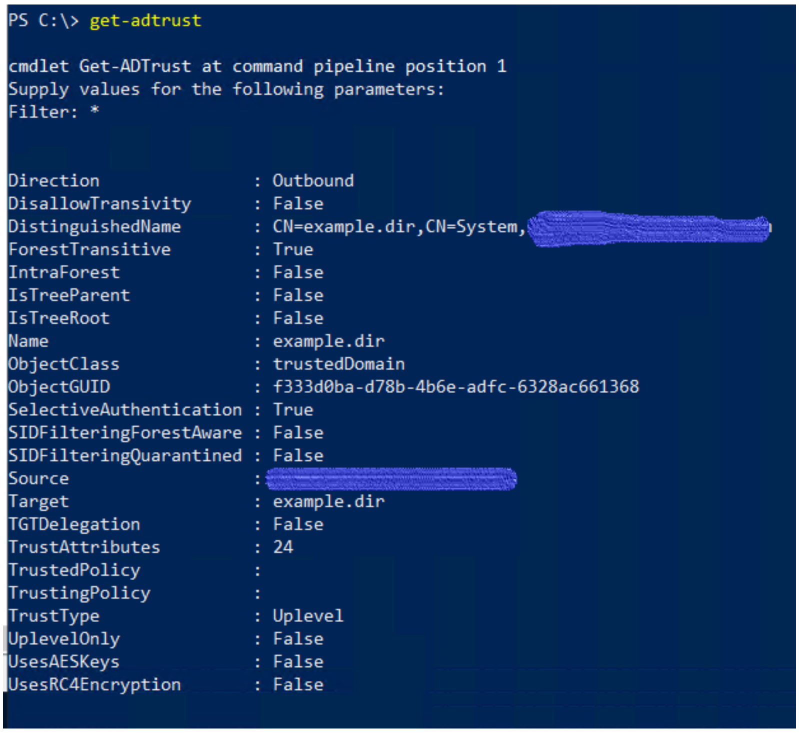
Transitivity of trust:

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.

To save a file with the details about the status of the names associated with this trust, click Save As.

Figure 15: Screenshot setup with a sample partner domain called example.dir

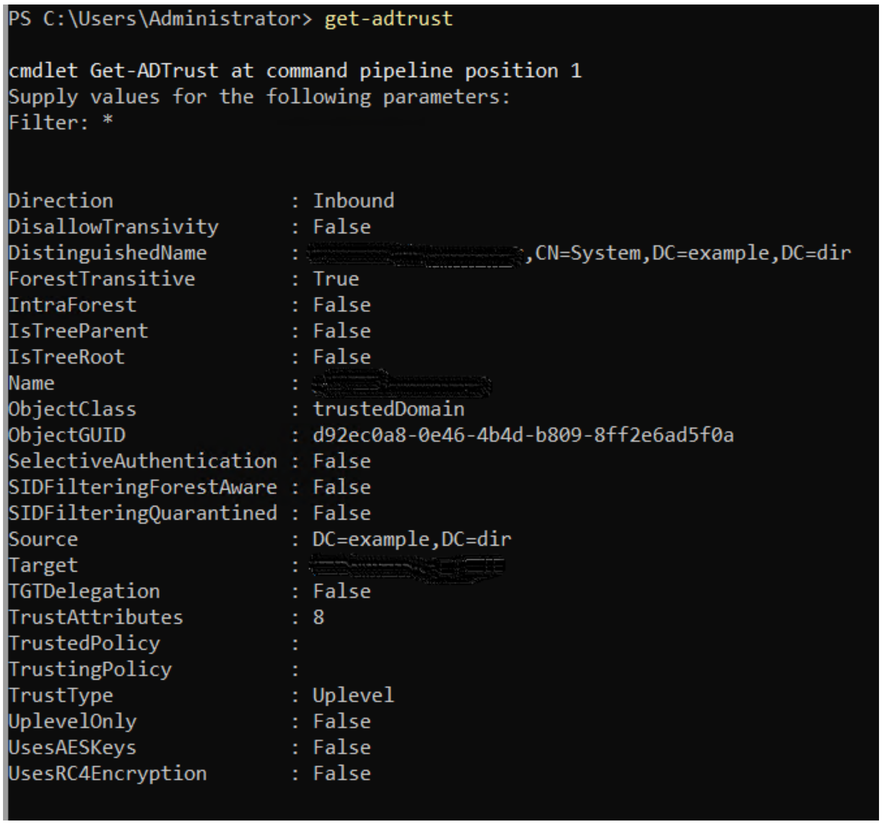


```
PS C:\> get-adtrust

cmdlet Get-ADTrust at command pipeline position 1
Supply values for the following parameters:
Filter: *


Direction                  : Outbound
DisallowTransivity         : False
DistinguishedName          : CN=example.dir,CN=System,[redacted]
ForestTransitive           : True
IntraForest                : False
IsTreeParent               : False
IsTreeRoot                 : False
Name                       : example.dir
ObjectClass                : trustedDomain
ObjectGUID                 : f333d0ba-d78b-4b6e-adfc-6328ac661368
SelectiveAuthentication    : True
SIDFilteringForestAware    : False
SIDFilteringQuarantined    : False
Source                     : [redacted]
Target                     : example.dir
TGTDelegation              : False
TrustAttributes            : 24
TrustedPolicy              :
TrustingPolicy             :
TrustType                  : Uplevel
UplevelOnly                : False
UsesAESKeys                : False
UsesRC4Encryption          : False
```

Figure 16: Verification of the configuration in dir.company.com

Note: SIDFilteringForestAware must be set to FALSE (=SID Filtering is active)

SIDFilteringQuarantined applies only to external trusts, but we are using forest trusts.



```
PS C:\Users\Administrator> get-adtrust

cmdlet Get-ADTrust at command pipeline position 1
Supply values for the following parameters:
Filter: *


Direction               : Inbound
DisallowTransivity      : False
DistinguishedName       : [redacted],CN=System,DC=example,DC=dir
ForestTransitive        : True
IntraForest             : False
IsTreeParent            : False
IsTreeRoot              : False
Name                    : [redacted]
ObjectClass             : trustedDomain
ObjectGUID              : d92ec0a8-0e46-4b4d-b809-8ff2e6ad5f0a
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
Source                  : DC=example,DC=dir
Target                  : [redacted]
TGTDelegation           : False
TrustAttributes         : 8
TrustedPolicy           :
TrustingPolicy          :
TrustType               : Uplevel
UplevelOnly             : False
UsesAESKeys             : False
UsesRC4Encryption       : False
```

Figure 17: The same trust viewed from the partner domain

Note: UsesAESKeys applies only to Kerberos Realm trusts. SelectiveAuthentication is set to false since the trust is not outbound.

3.2 Potential Risks and Mitigations

Without a detailed evaluation and permanent monitoring of the health state of a partner directory, the administrators of dir.company.com must assume the compromise of that partner's directory and have to consider the potential risks associated with that. The following paragraphs list relevant risks and how they are mitigated by the trust configuration guidelines described in section 2 (General Guidelines Regarding Active Directory Trusts).

3.2.1 Modification of the Trust Settings

A malicious actor in a partner directory could try to change the trust settings or create trusts to other domains. As trusts cannot be unilaterally created this is not an issue if an attacker has not compromised both sides. Weakening the security settings of the one-way trust, where COMPANY trusts the partner, can only be done from the COMPANY side.

Please also see section 2.1 (Monitoring of Trusts).

3.2.2 Creation of Fake Credentials

An attacker with admin rights in an account directory (partner directory) can manipulate the SID-History attribute of groups, computers and user accounts in such a way, that additional SIDs are added, potentially allowing access to resources to which they should not have access (e.g. different users mailbox). This scenario is especially dangerous if the added SIDs belong to other forests (other partners or COMPANY itself).

To mitigate this risk the trusts are configured with SID Filtering enabled, which means that all SIDs not belonging to the partners directory are automatically removed when using the trust.

For a very detailed technical description of SID Filtering see https://msdn.microsoft.com/en-us/library/cc237940.aspx.

This leaves the scenario, where the malicious actor adds SIDs from their own directory, thus potentially impersonating other users and accessing their resources in the Shared Services. This cannot be prevented but could be monitored.

Privilege escalation from the partner forest to dir.company.com is not possible, provided that

- users from the partner's directory are not given administrative rights in dir.company.com,
- dir.company.com has administrative tiers implemented and is operated according to security best practices

and unauthorized access from the partner forest to resources in dir.company.com is mitigated if Selective Authentication is implemented for the trust.

3.2.3 Manipulation of Directory Data

An attacker could manipulate or destroy data in the partner's directory, which may lead to denial-of-service issues for that environment. If a synchronization is implemented between the partner's directory and the company domain, the synchronization engine must implement mechanisms to handle these scenarios.

Otherwise this is an issue mainly for the partner, not for dir.company.com.

3.2.4 Enumeration of the COMPANY Domain

The use of the trust requires the right to access the Domain Controllers in dir.company.com and as the user is authenticated and trusted, they can enumerate most of the contents of the company environment.

If company considers enumeration a serious issue, additional measures can be considered, up to the activation of the LIST OBJECT mode in AD. Due to the negative impact on every day operations, compared to a low-risk created by enumeration, this setup is currently not implemented.

3.2.5 Enumeration of Other Trusted Domains

Multiple trust relationships between dir.company.com and different partners do not grant users from a partner domain any right to enumerate the domain of another partner, due to the direction of the trusts and the fact that they are not transitive.

Creating trust relationships requires a working DNS name resolution in both directions. This could enable someone from one partner AD to query the DNS zones of other partners, gathering information about computers in those domains.

If the company considers this problematic, additional measures can be implemented to mitigate this risk. We successfully tested replacing the READ permissions of the EVERYONE group on the conditional DNS forwarders in dir.company.com with more specific groups.

3.2.6 Privilege Escalation in the dir.company.com Domain

The use of SID Filtering prevents common attacks, e.g. using Mimikatz to add SIDs of dir.company.com accounts to tickets originating in the partner's directory.

Privilege escalation would then require misconfigurations or missing security patches etc. on dir.company.com servers, issues not directly related to trusts.

3.2.7 Access to Other Resources in dir.company.com

Users from trusted domains are automatically members of the AUTHENTICATED USERS group in a domain, potentially giving them access to resources, where that group has assigned permissions (even by default).

To mitigate this issue, we implement Selective Authentication (also called "authentication firewall"), where users from trusted domains must be explicitly assigned the ALLOWED TO AUTHENITCATE right on each resource in the trusting domain. This setting is configured on the computer objects in the trusting domain and is therefore controlled by administrators of dir.company.com.

We also recommended to replace the AUTHENTICATED USERS permission on objects and resources in the trusting domain with more specific groups, where necessary.

3.2.8 Attacks on Accounts

3.2.8.1 Kerberoasting

Users from a partner domain can request Kerberos Service Tickets for any account in dir.company.com which has a Service Principal Name associated with it. These Service Tickets can then be used for an offline password cracking attack since they are partially encrypted with the password of the target service account. If a user manages to request many Service Tickets for an account, the time to crack the password can be significantly reduced.[2,3]

The usual mitigations should be in place[3]:

- Service account passwords must be at least 32 characters long and must not be easily guessable
- Managed or Group Managed Service Accounts should be used whenever possible
- All administrative or service accounts should be monitored for changes to their Service Principal Name attribute
- Event ID 4769 on Domain Controllers should be monitored, especially with Encryption Type 0x17 (see the above-mentioned link[3])

[2] *http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/*

[3] *https://adsecurity.org/?p=2293*

[3] *https://adsecurity.org/?p=3458*

3.2.8.2 Lockout

Users may use the network connectivity that is required for resource access and try to lockout user accounts of other users. There are three scenarios to be considered:

- Locking out accounts of other users form the same partner domain
  This scenario already exists internally in each partner's AD with the trust
- Locking out accounts belonging to COMPANY
  This requires knowledge about account names, but would be possible, if account lockout is configured for COMPANY accounts. Microsoft does not recommend using account lockout, instead failed logins should be monitored
- Locking out accounts from other trusted partner domains
  This also requires knowledge about account names. To mitigate this scenario, account lockout should be configured appropriately in the partner directories.