Deploying Shielded Virtual Machines – Part2

michaelfirsov.wordpress.com/deploying-shielded-virtual-machines-part2

June 14, 2018

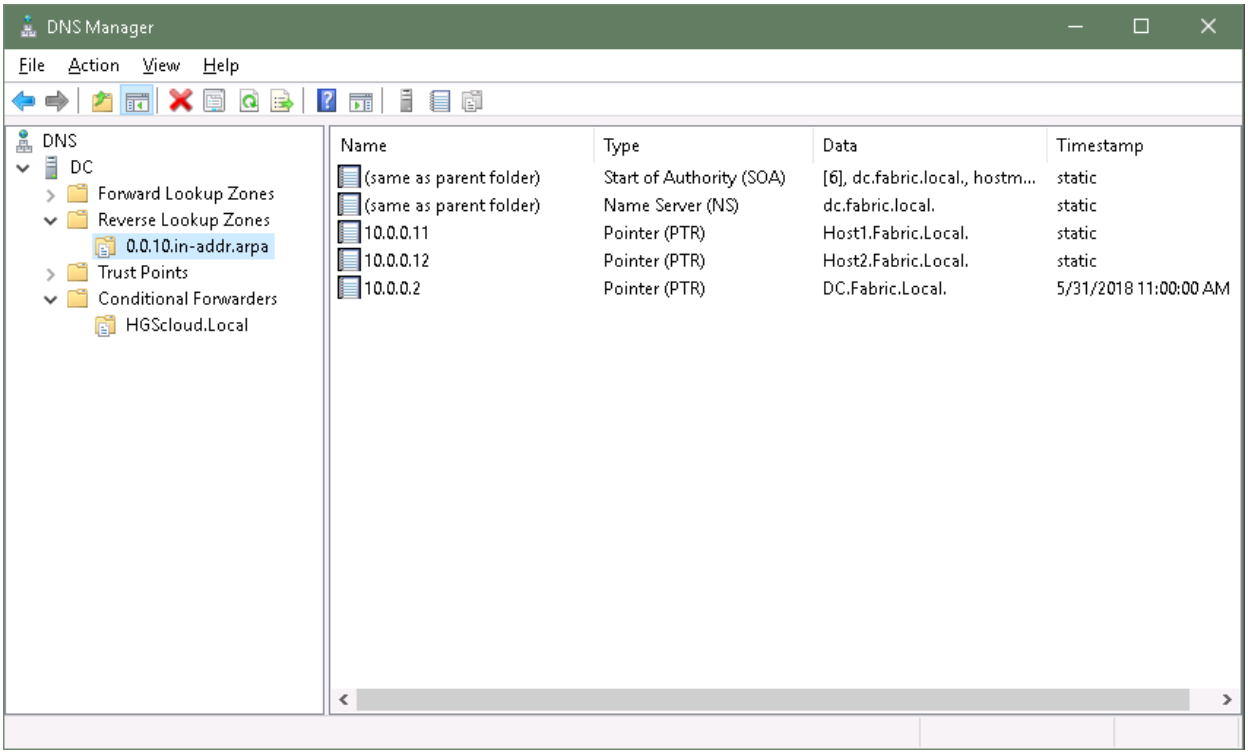
Part1

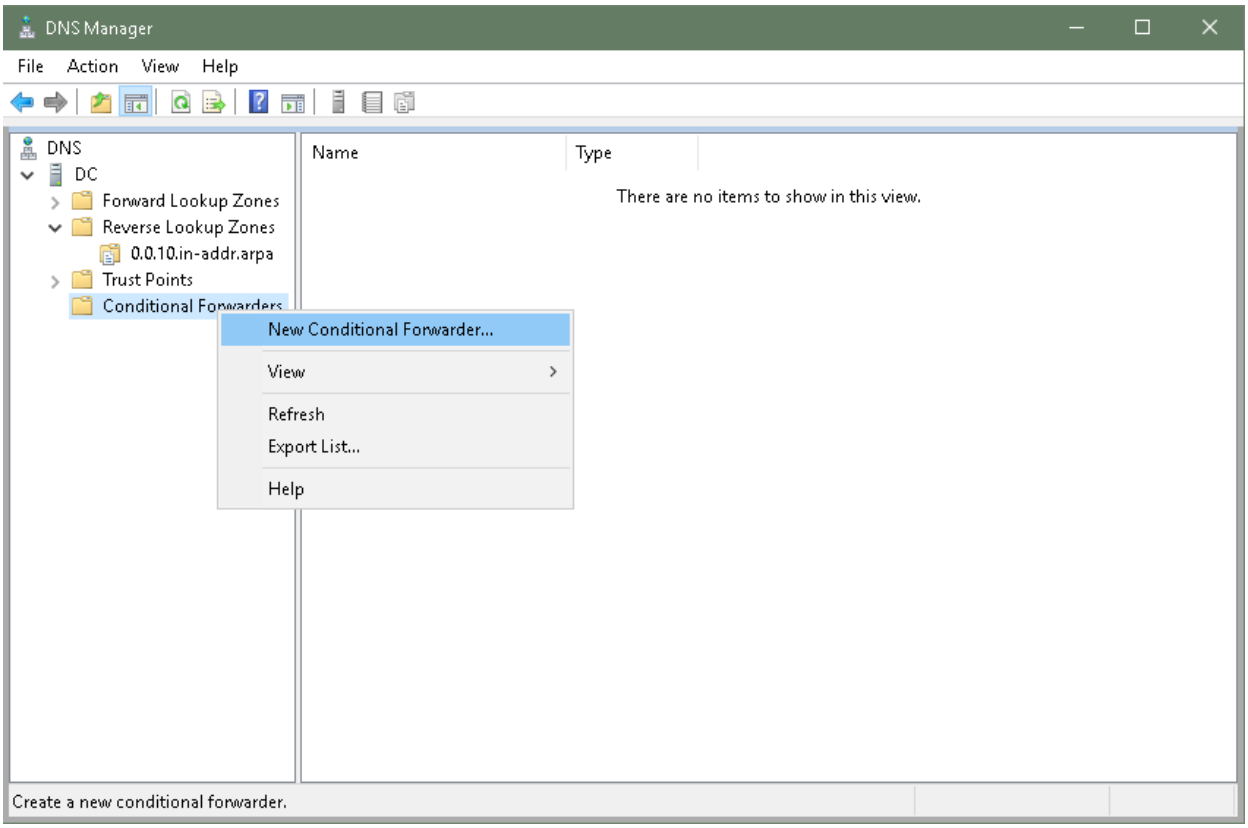
Part 2: Deploying guarded hosts

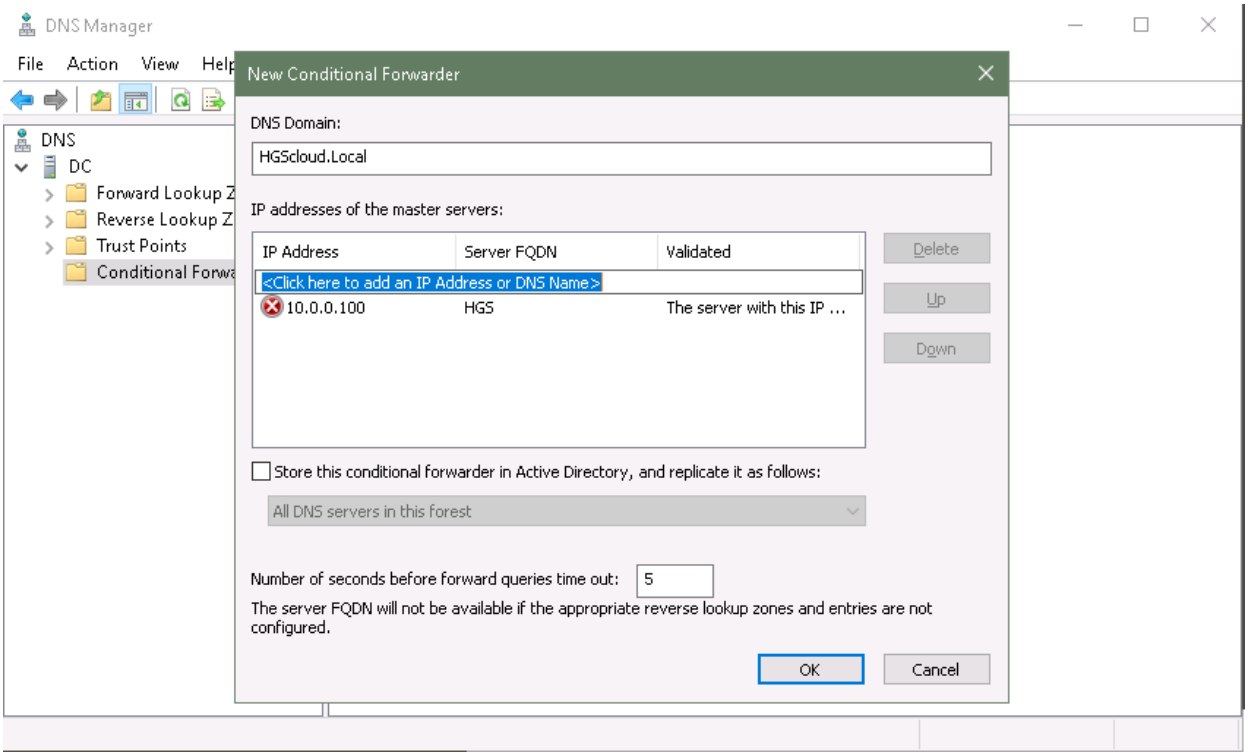
Before we proceed to configuring guarded hosts there are several steps that should be taken.

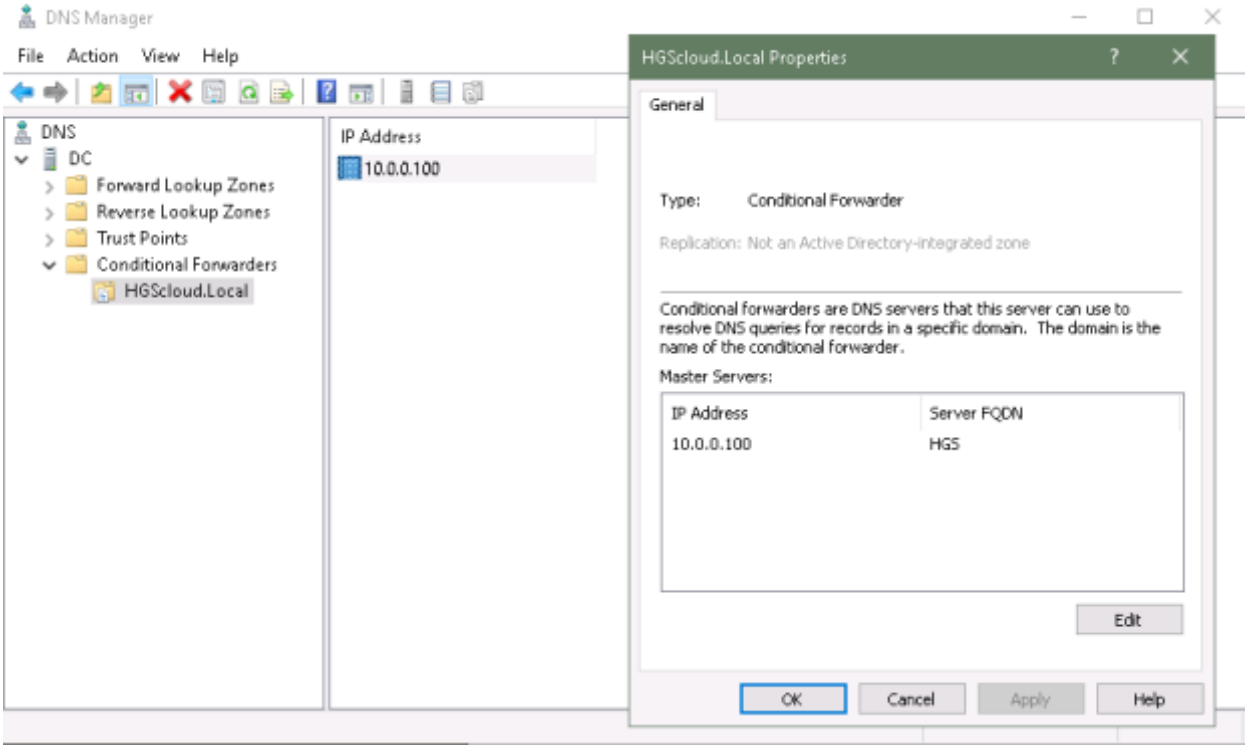
1) For guarded hosts to be able to retreive information from the HGS server and vice versa I'll have to create the DNS forwarders in both domains. Before I do that I'll create the reverse lookup zones on both domain controllers:

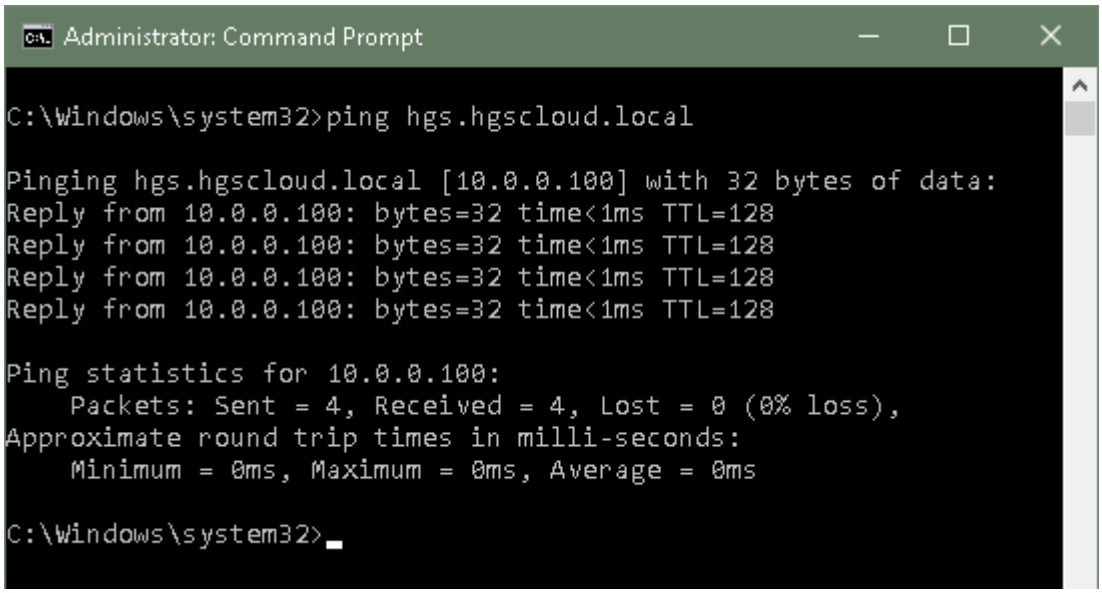
In the *Fabric.Local* domain



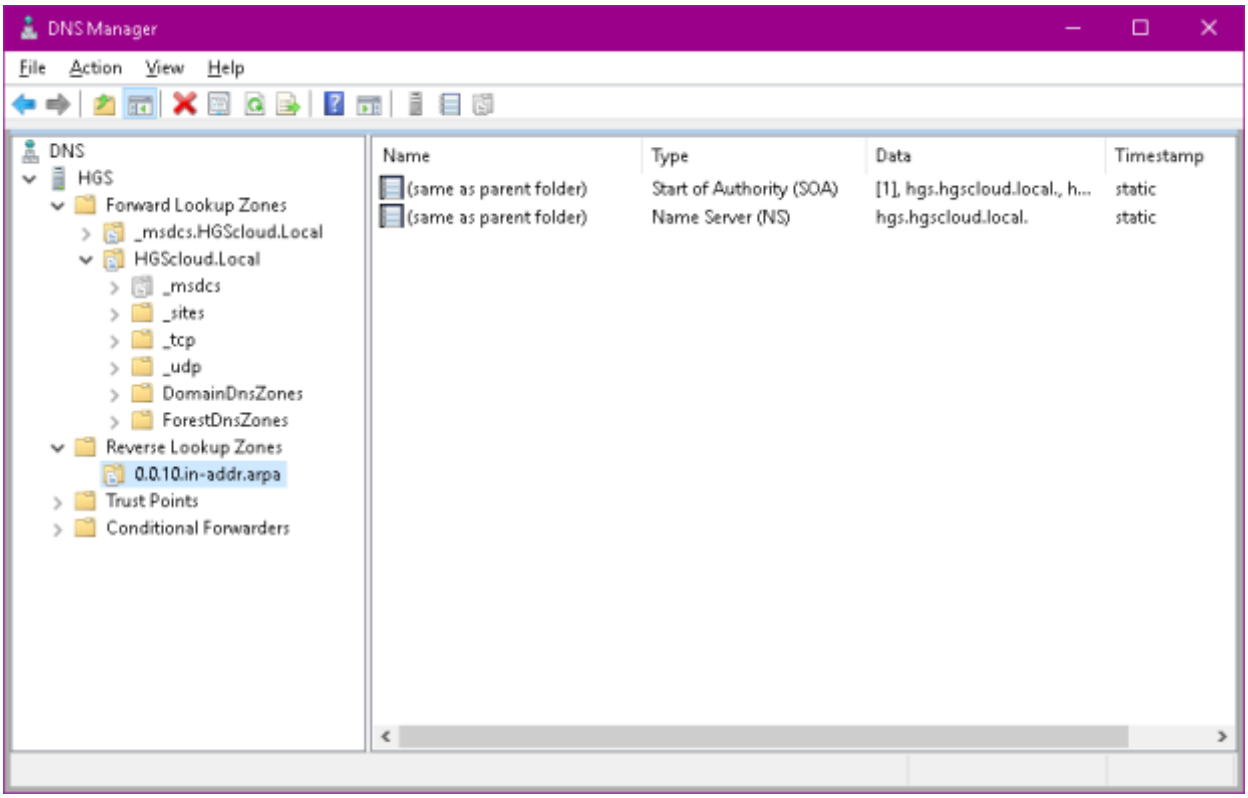

DNS Manager
File Action View Help
DNS
DC
Forward Lookup Zones
Reverse Lookup Zones
0.0.10.in-addr.arpa
Trust Points
Conditional Forwarders
Name
Type
There are no items to show in this view.
New Conditional Forwarder...
View
Refresh
Export List...
Help
Create a new conditional forwarder.

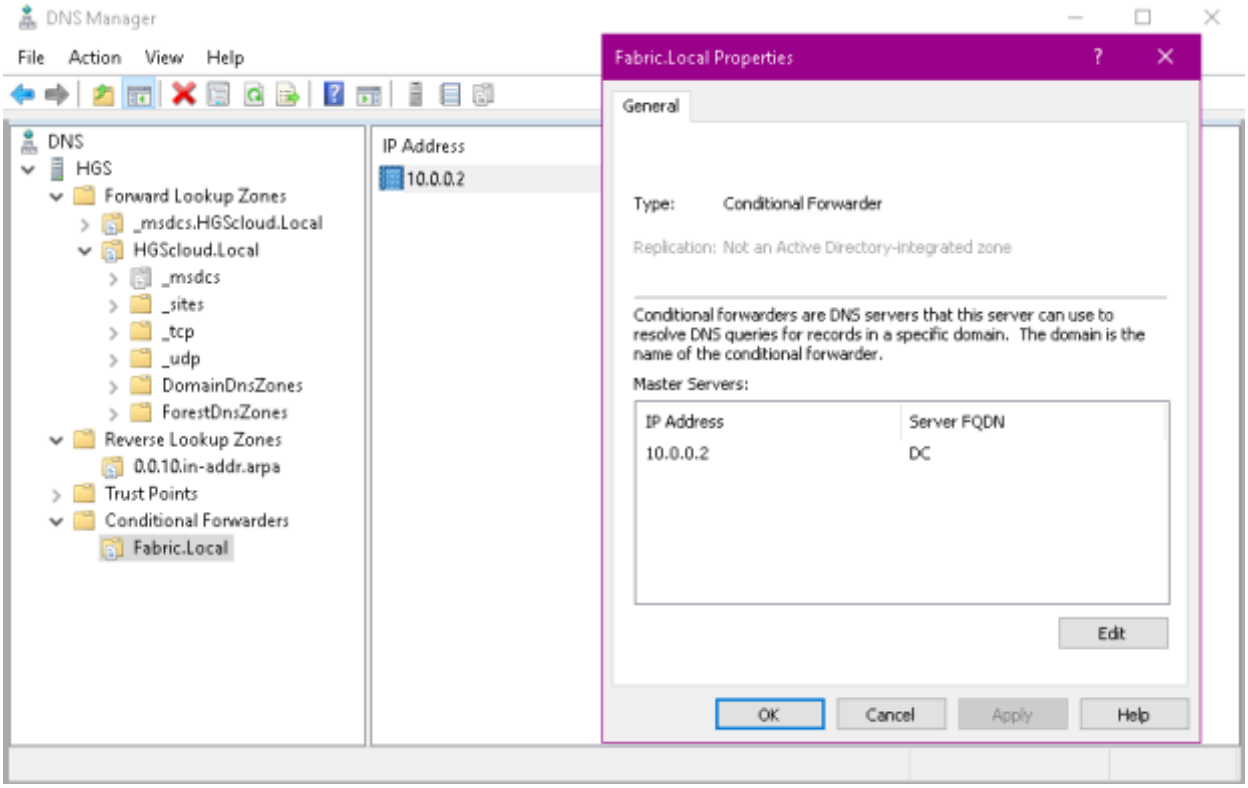

DNS Manager
File Action View Help
DNS
DC
Forward Lookup Z
Reverse Lookup Z
Trust Points
Conditional Forwa
New Conditional Forwarder
DNS Domain:
HGScloud.Local
IP addresses of the master servers:
IP Address
Server FQDN
Validated
<Click here to add an IP Address or DNS Name>
10.0.0.100
HGS
The server with this IP ...
Delete
Up
Down
Store this conditional forwarder in Active Directory, and replicate it as follows:
All DNS servers in this forest
Number of seconds before forward queries time out:
5
The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.
OK
Cancel

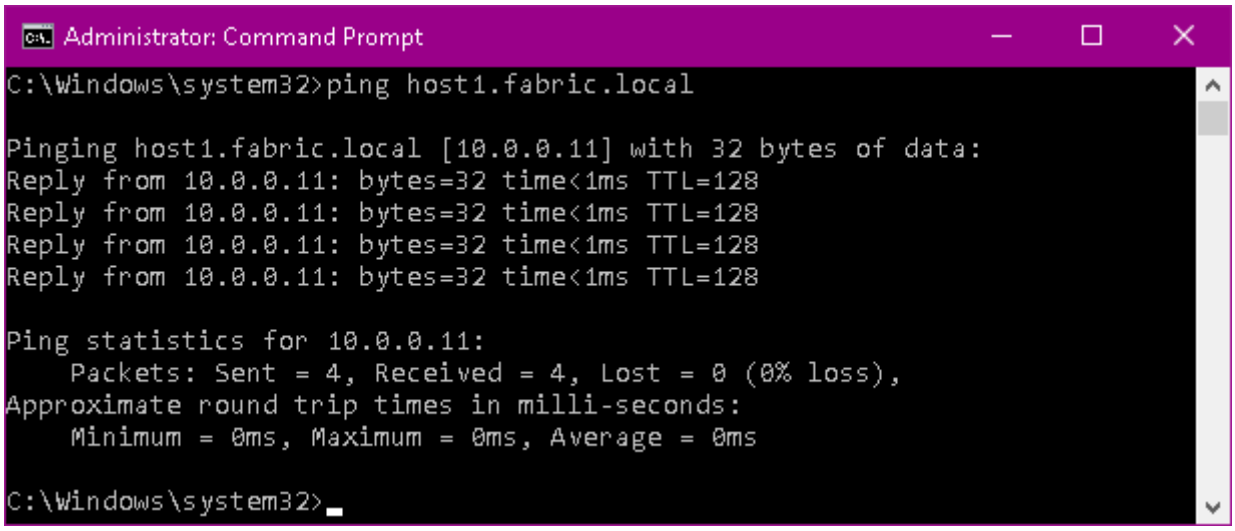




In the *HGScloud.Local* domain:

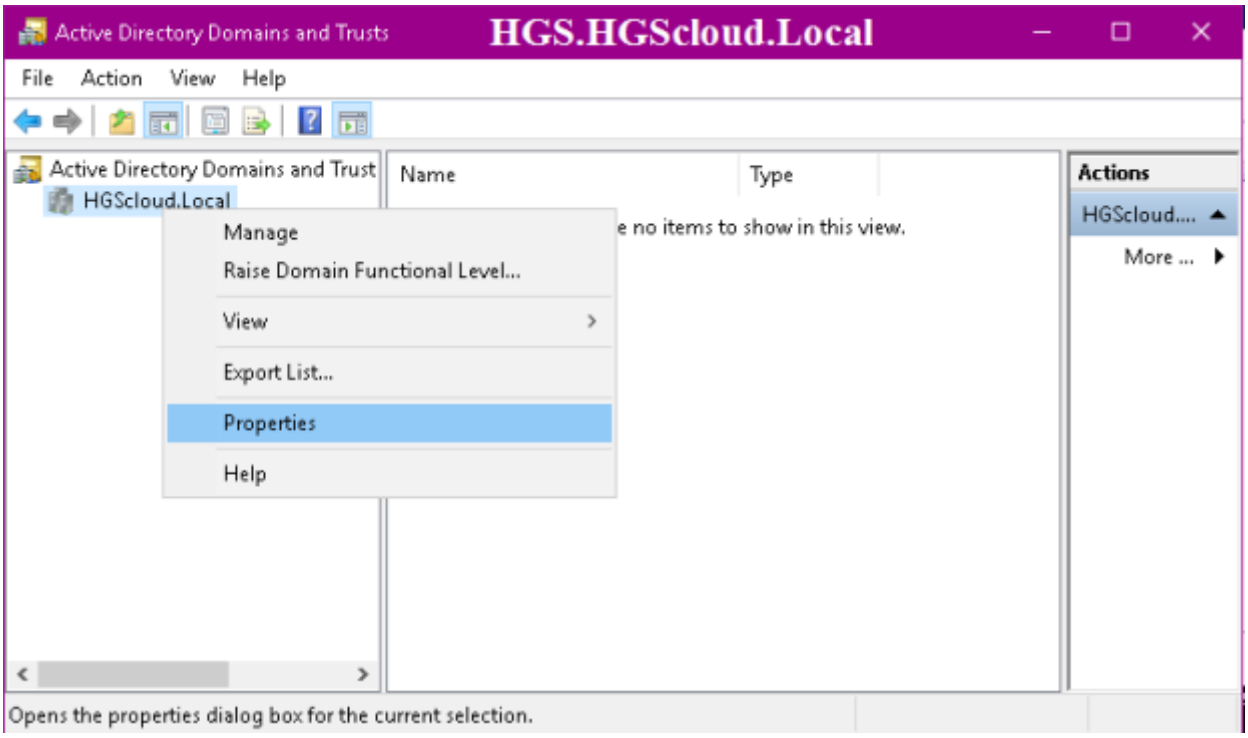

DNS Manager
File Action View Help
DNS
HGS
Forward Lookup Zones
_msdcs.HGScloud.Local
HGScloud.Local
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Reverse Lookup Zones
0.0.10.in-addr.arpa
Trust Points
Conditional Forwarders
Name
Type
Data
Timestamp
(same as parent folder)
Start of Authority (SOA)
[1], hgs.hgscloud.local., h...
static
(same as parent folder)
Name Server (NS)
hgs.hgscloud.local.
static

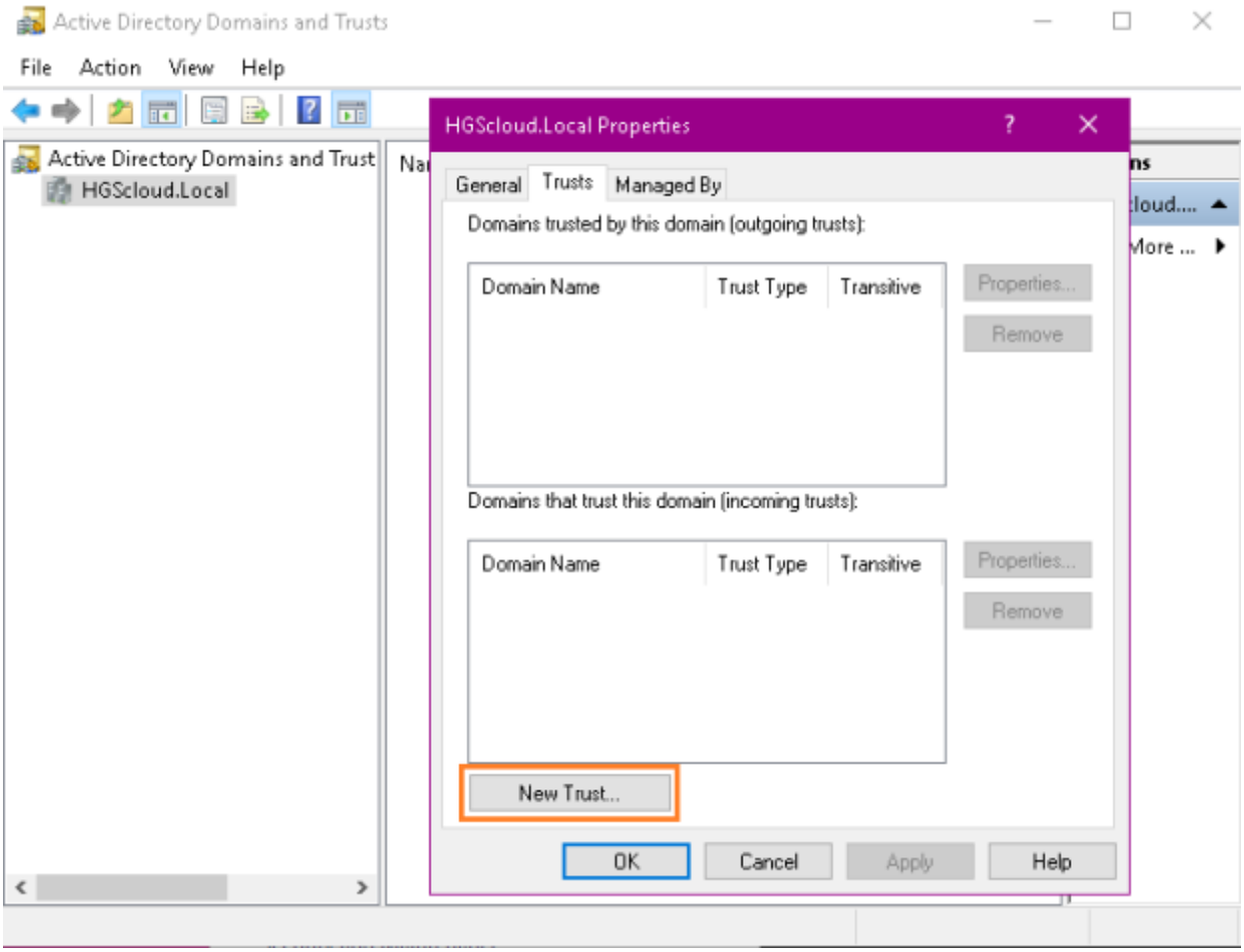

DNS Manager
File Action View Help
DNS
HGS
Forward Lookup Zones
_msdcs.HGScloud.Local
HGScloud.Local
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Reverse Lookup Zones
0.0.10.in-addr.arpa
Trust Points
Conditional Forwarders
Fabric.Local
IP Address
10.0.0.2
Fabric.Local Properties
General
Type: Conditional Forwarder
Replication: Not an Active Directory-integrated zone
Conditional forwarders are DNS servers that this server can use to resolve DNS queries for records in a specific domain. The domain is the name of the conditional forwarder.
Master Servers:
IP Address
Server FQDN
10.0.0.2
DC
Edit
OK
Cancel
Apply
Help

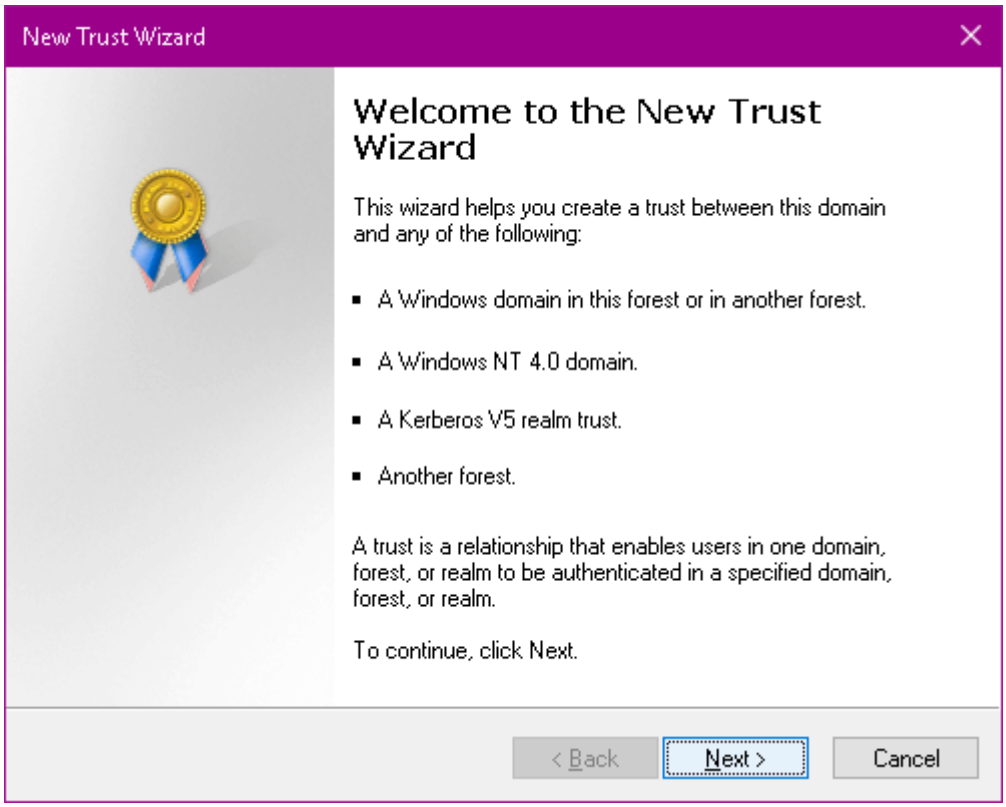


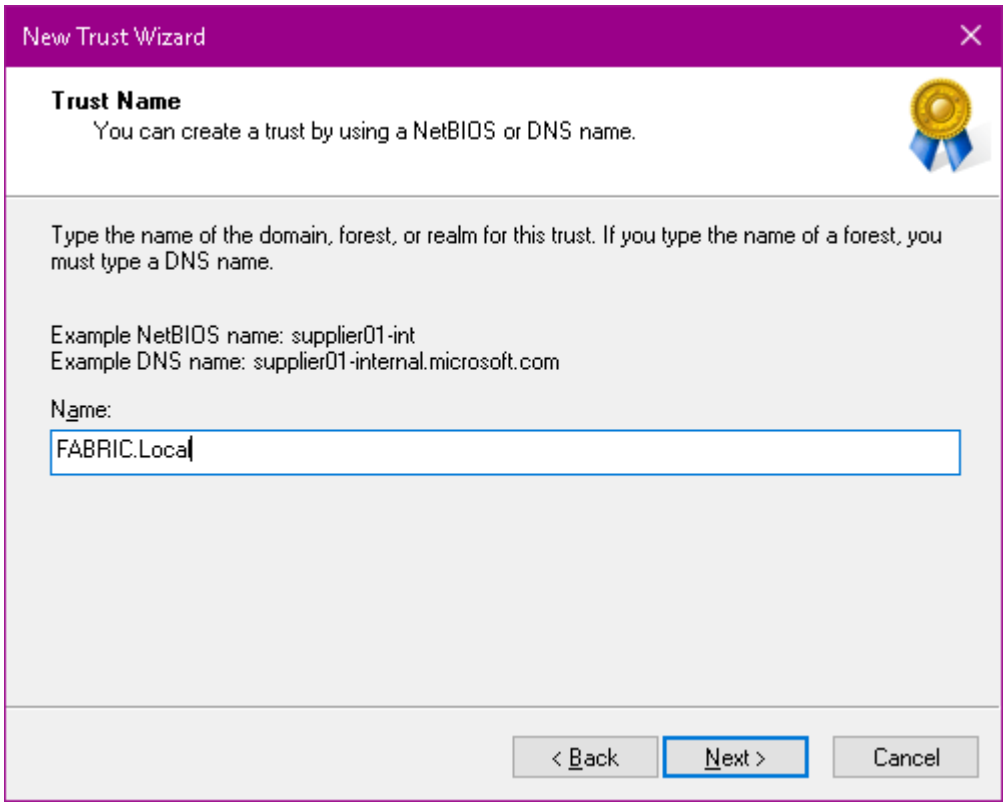
2) The one-way forest trust between the *hgs* and fabric domains must be configured (HGS domain trusts FABRIC domain).

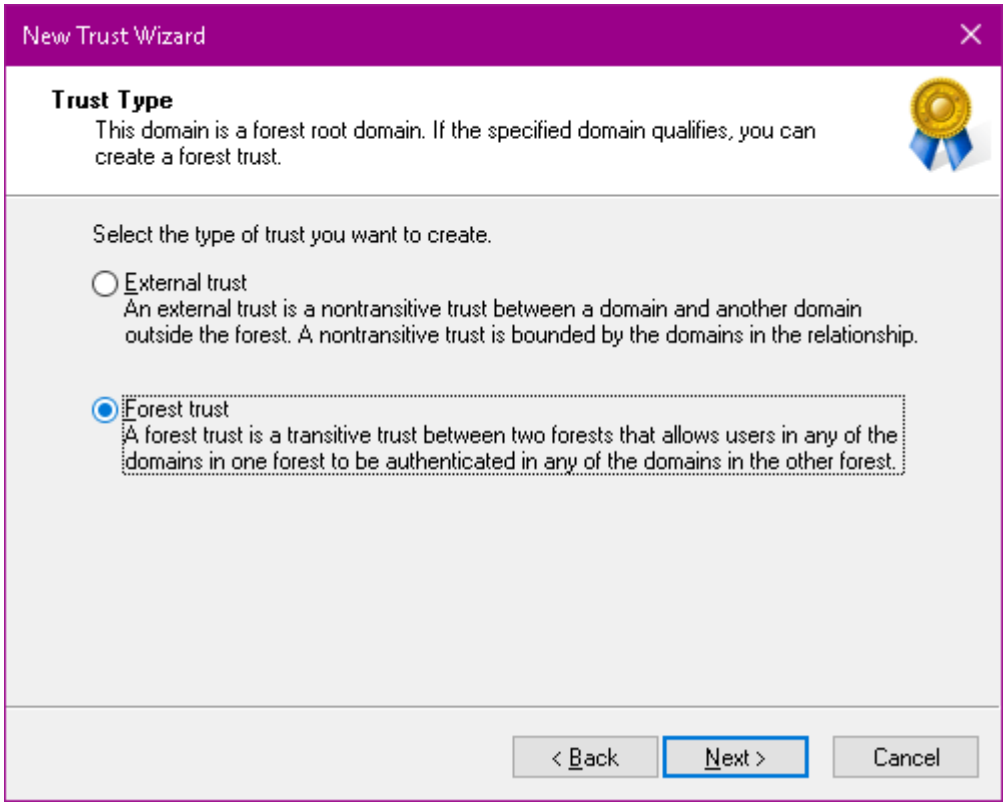
On HGS server:

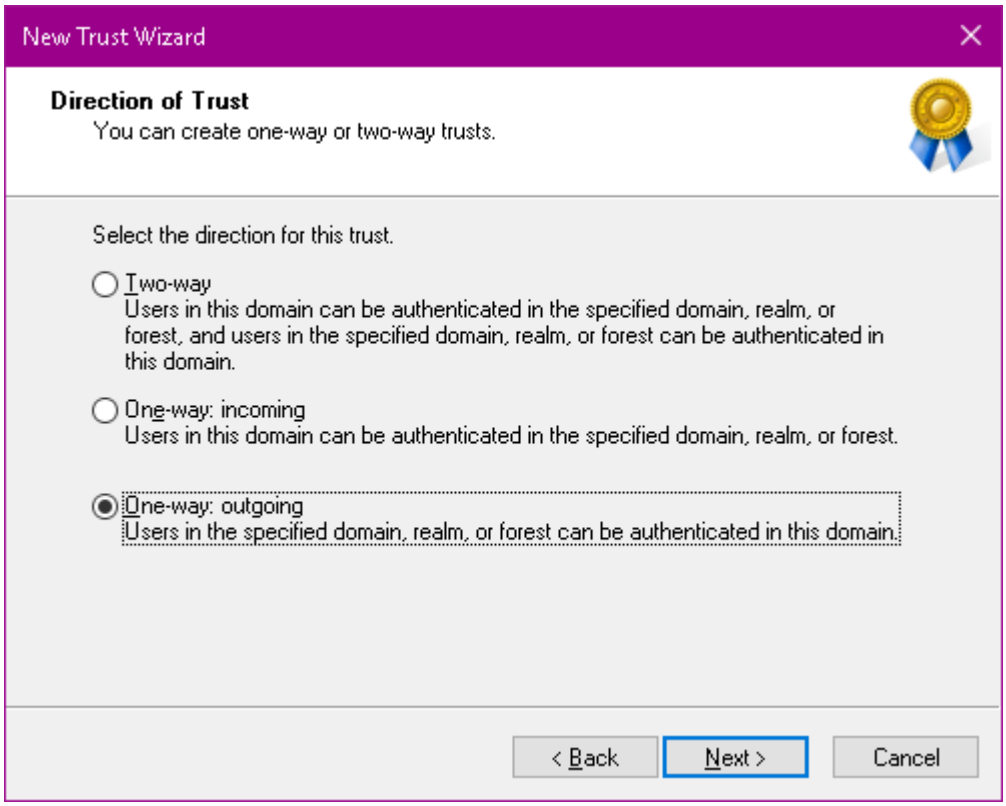


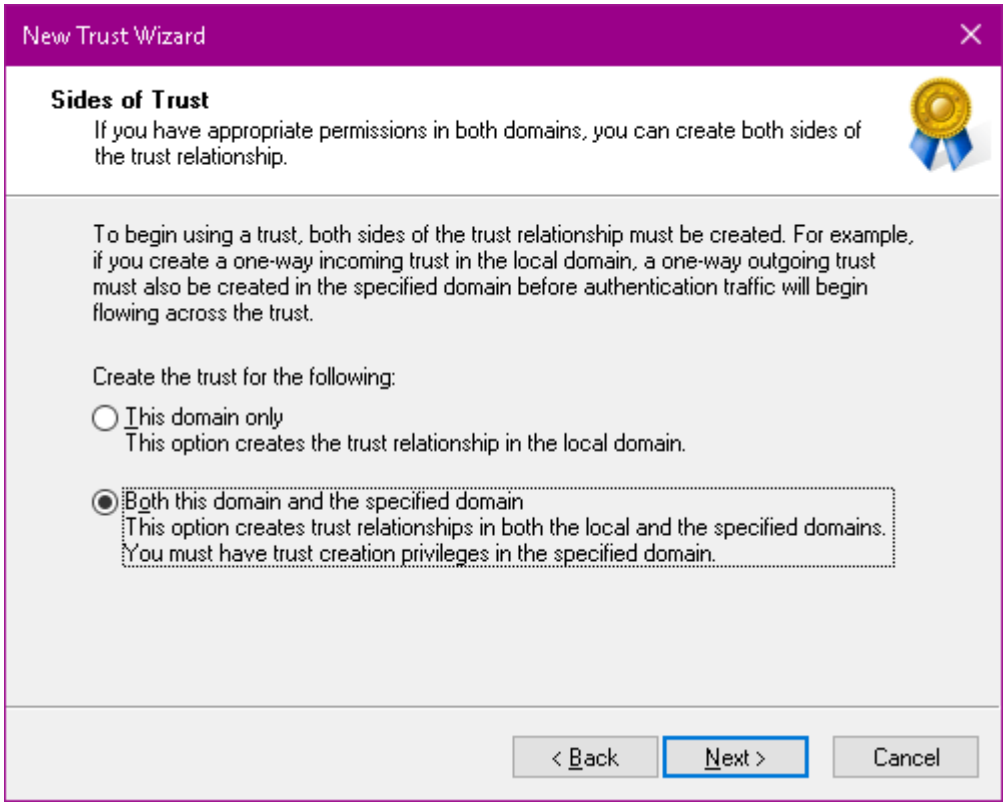

Active Directory Domains and Trusts
File Action View Help
Active Directory Domains and Trust
HGScloud.Local
HGScloud.Local Properties
General Trusts Managed By
Domains trusted by this domain (outgoing trusts):
Domain Name Trust Type Transitive
Properties...
Remove
Domains that trust this domain (incoming trusts):
Domain Name Trust Type Transitive
Properties...
Remove
New Trust...
OK Cancel Apply Help

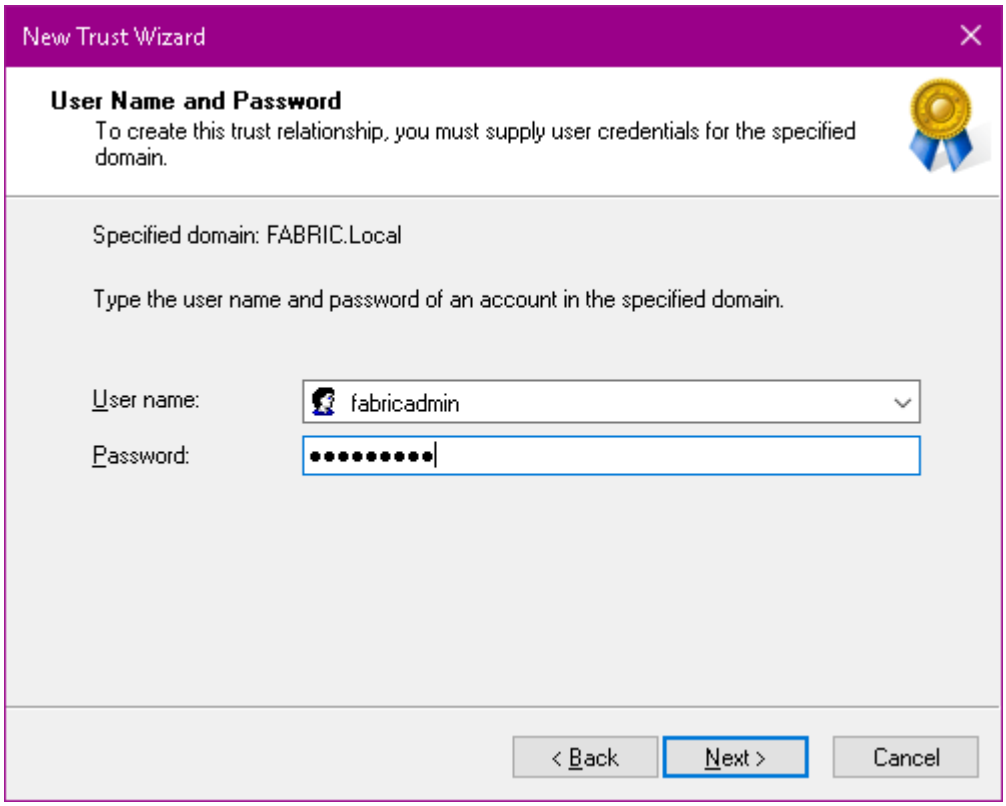

New Trust Wizard
Welcome to the New Trust Wizard
This wizard helps you create a trust between this domain and any of the following:
A Windows domain in this forest or in another forest.
A Windows NT 4.0 domain.
A Kerberos V5 realm trust.
Another forest.
A trust is a relationship that enables users in one domain, forest, or realm to be authenticated in a specified domain, forest, or realm.
To continue, click Next.
< Back
Next >
Cancel

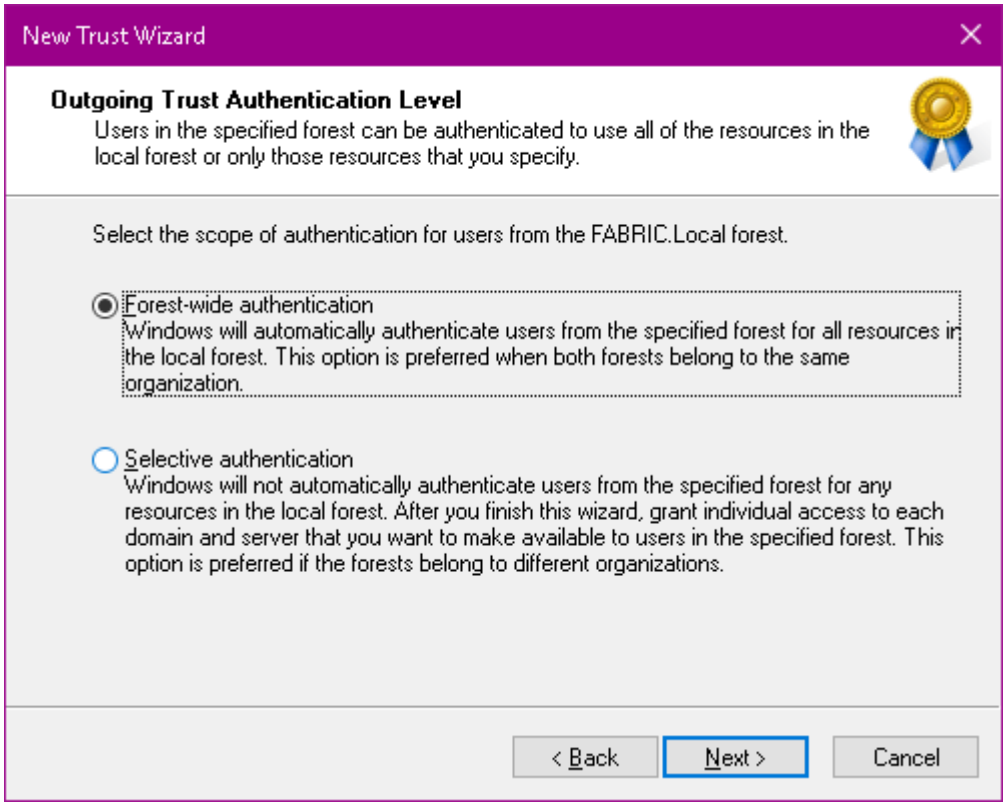

New Trust Wizard
Trust Name
You can create a trust by using a NetBIOS or DNS name.
Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.
Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com
Name:
FABRIC.Local
< Back
Next >
Cancel

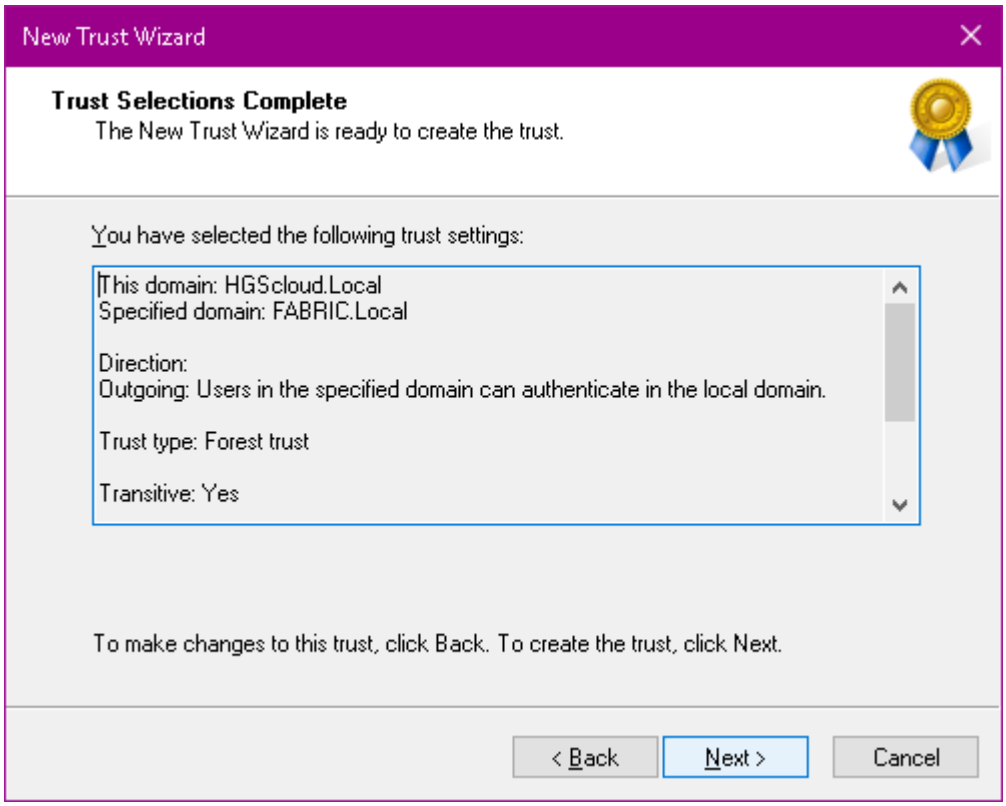

New Trust Wizard
Trust Type
This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.
Select the type of trust you want to create.
External trust
An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive 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.
< Back
Next >
Cancel

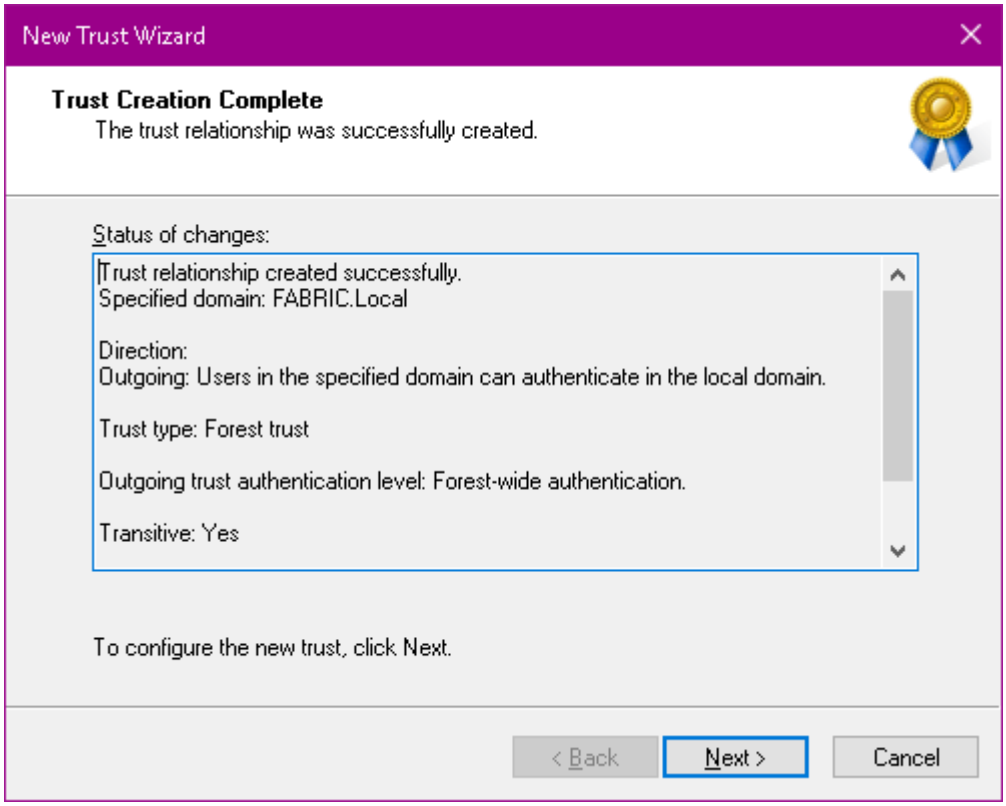

New Trust Wizard
Direction of Trust
You can create one-way or two-way trusts.
Select the direction for this trust.
Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.
One-way: 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.
< Back
Next >
Cancel

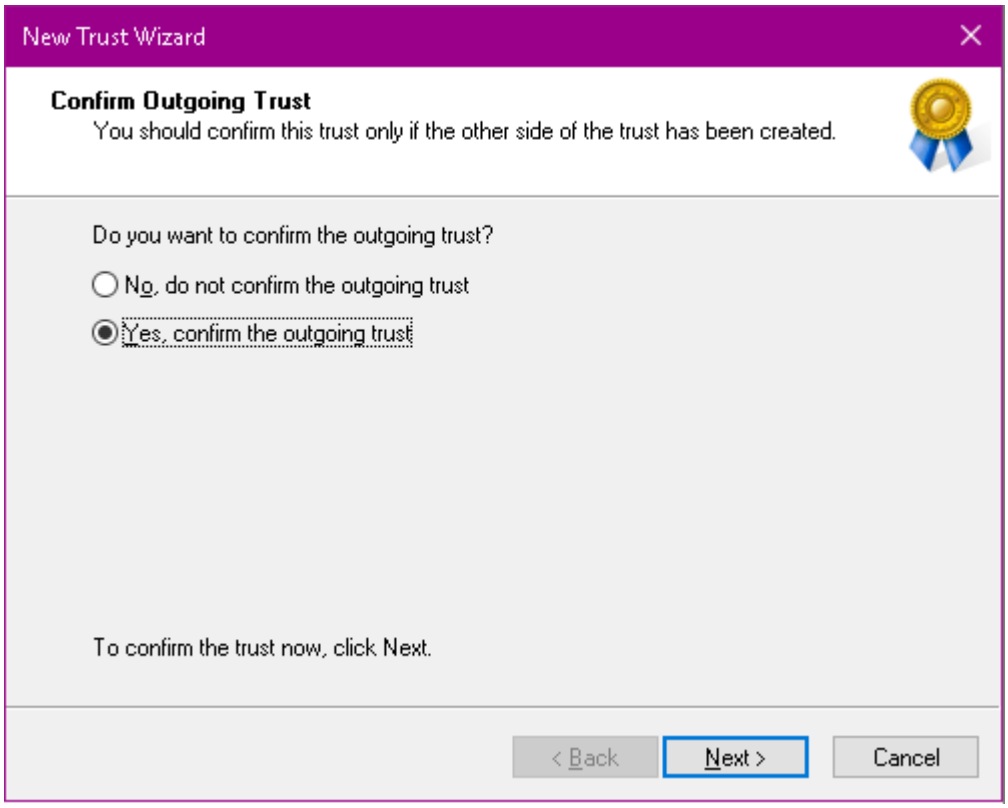

New Trust Wizard
Sides of Trust
If you have appropriate permissions in both domains, you can create both sides of the trust relationship.
To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing 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.
< Back
Next >
Cancel

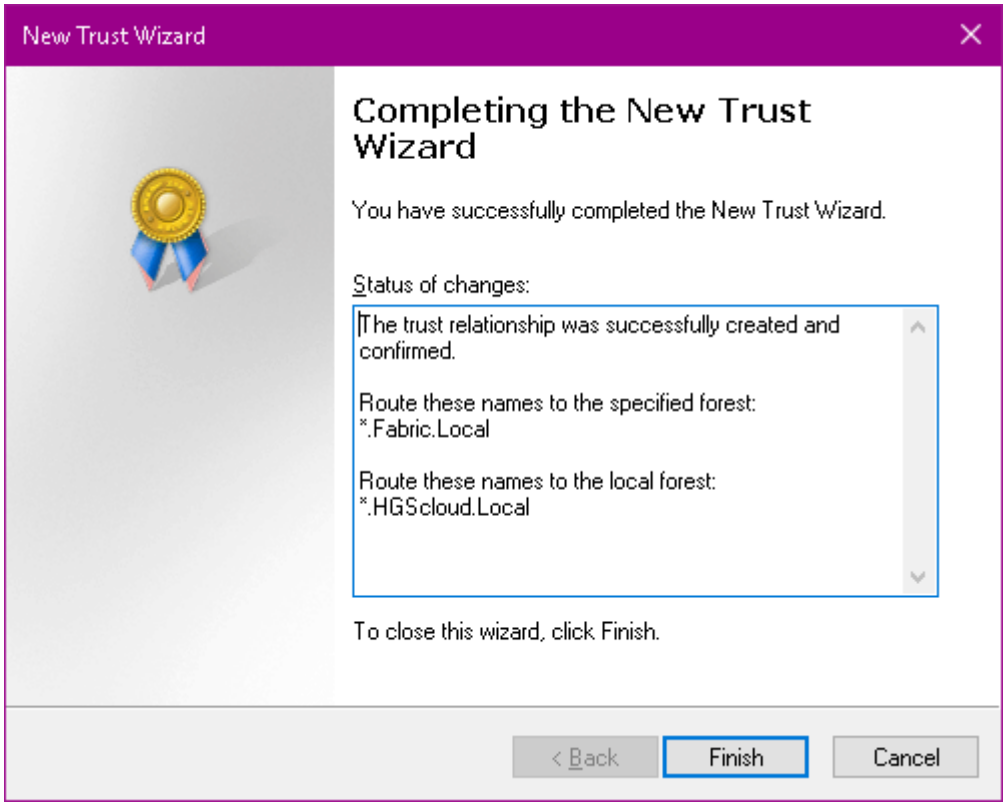

New Trust Wizard
User Name and Password
To create this trust relationship, you must supply user credentials for the specified domain.
Specified domain: FABRIC.Local
Type the user name and password of an account in the specified domain.
User name:
fabricadmin
Password:
< Back
Next >
Cancel

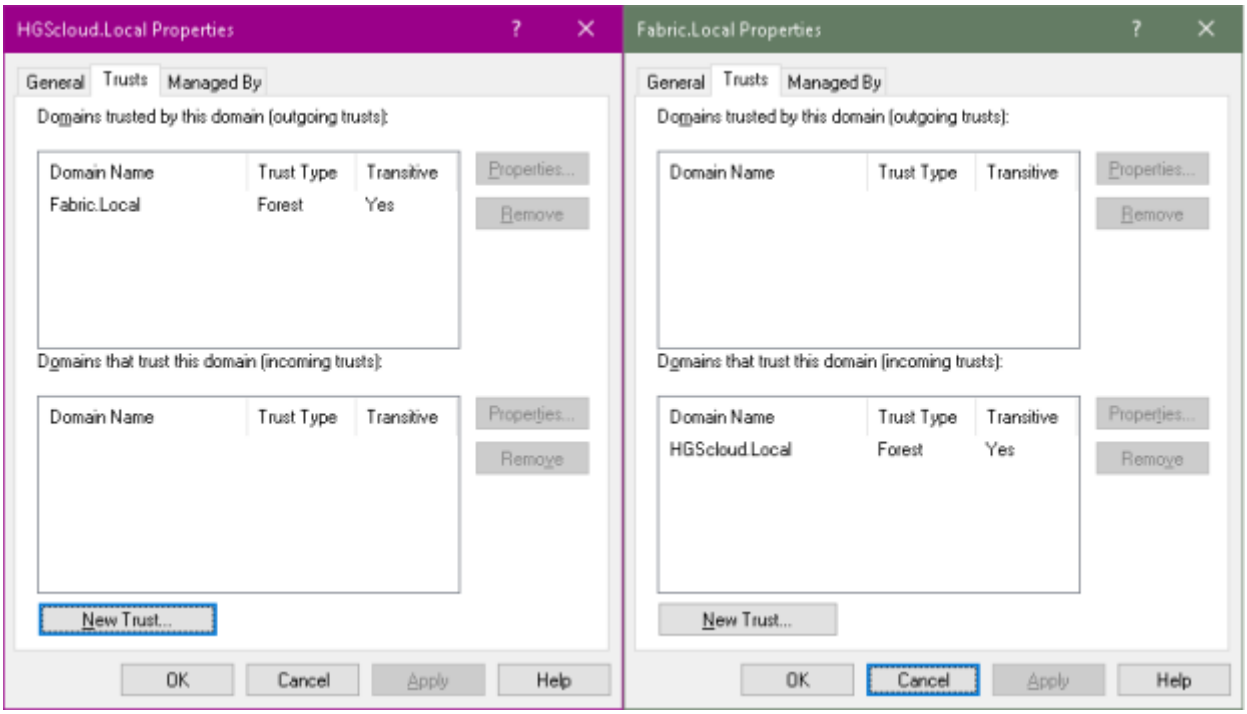

New Trust Wizard
Outgoing Trust Authentication Level
Users in the specified forest can be authenticated to use all of the resources in the local forest or only those resources that you specify.
Select the scope of authentication for users from the FABRIC.Local forest.
Forest-wide authentication
Windows 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.
< Back
Next >
Cancel


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: HGScloud.Local
Specified domain: FABRIC.Local
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.
< Back
Next >
Cancel

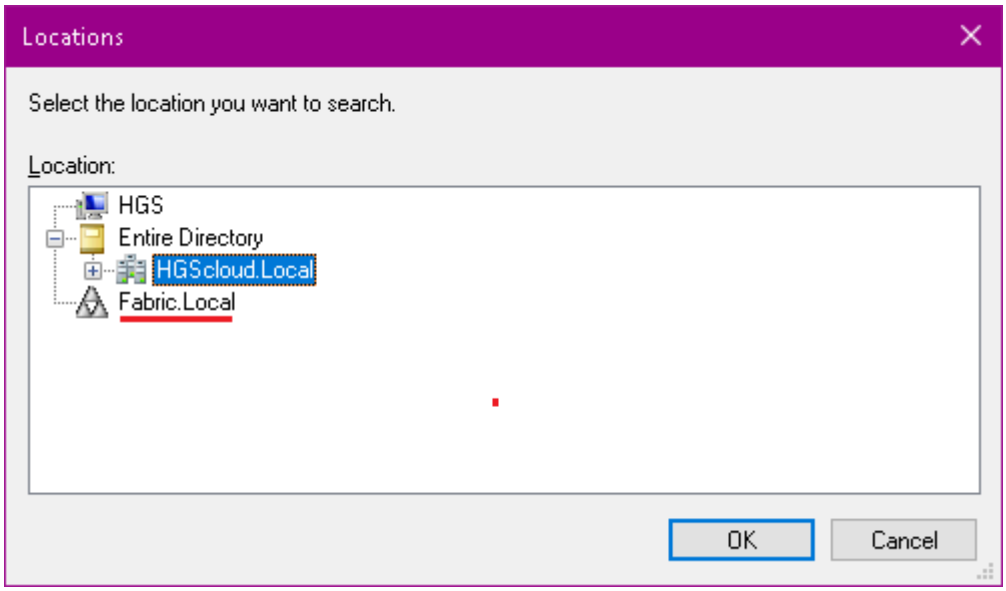

New Trust Wizard
Trust Creation Complete
The trust relationship was successfully created.
Status of changes:
Trust relationship created successfully.
Specified domain: FABRIC.Local
Direction:
Outgoing: Users in the specified domain can authenticate in the local domain.
Trust type: Forest trust
Outgoing trust authentication level: Forest-wide authentication.
Transitive: Yes
To configure the new trust, click Next.
< Back
Next >
Cancel


New Trust Wizard
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.
< Back
Next >
Cancel


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:
*.Fabric.Local
Route these names to the local forest:
*.HGScloud.Local
To close this wizard, click Finish.
< Back
Finish
Cancel

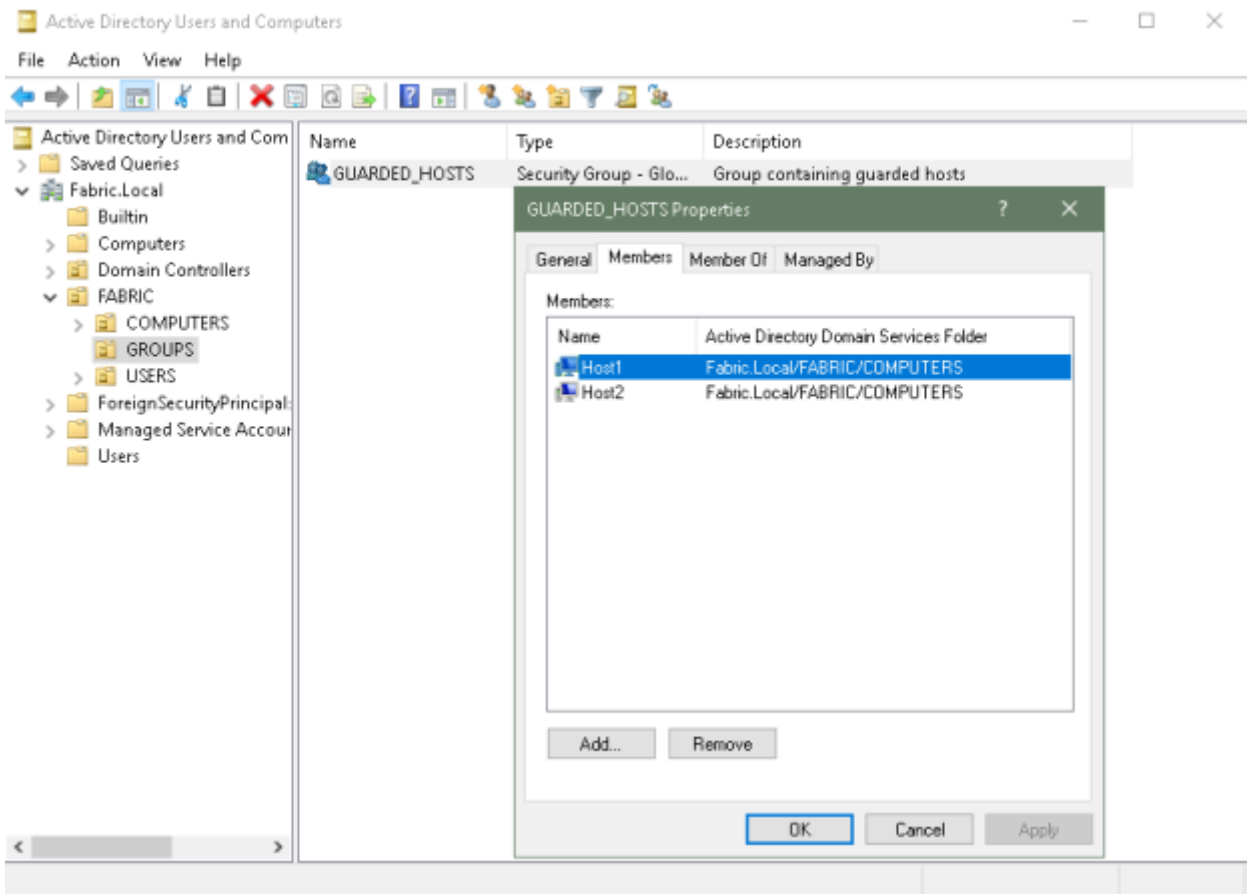


As a result, in the HGSLocal.Local domain we can select users from Fabricam.Local domain:



3) As I'm going to use AD attestetion mode I must create a computer group which will contain computer accounts of the Hyper-V hosts: only these hosts will be allowed to run shielded VMs:

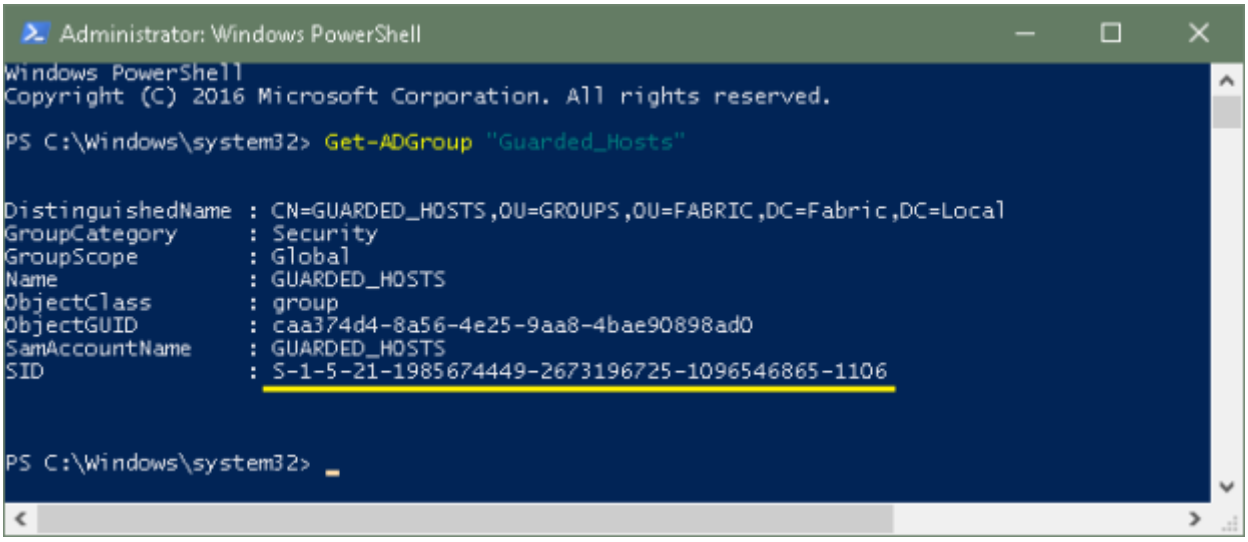
On *dc.fabric.local*



4) This group must be registered on the HGS server (meaning HGS will allow shielded VMs to be run only on the hosts from the GUARDED_HOSTS group.

On *dc.fabric.local*

Get-ADGroup “Guarded_Hosts”



On *hgs.hgscloud.local*

Add-HgsAttestationHostGroup -Name “Guarded_Hosts” -Identifier “S-1-5-21-1985674449-2673196725-1096546865-1106”

Run Get-HgsAttestationHostGroup to make sure the attestestion host group has been configured successfully.

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Add-HgsAttestationHostGroup -Name "Guarded_Hosts" -Identifier "S-1-5-21-1985674449-2673196725-10
96546865-1106"
S-1-5-21-1985674449-2673196725-1096546865-1106:Guarded_Hosts
PS C:\Windows\system32> Get-HgsAttestationHostGroup

Name          Identifier
----          ----------
Guarded_Hosts S-1-5-21-1985674449-2673196725-1096546865-1106


PS C:\Windows\system32> _
```

Now that all the preliminary configuration steps have been taken it's time to configure the guided fabric.

First off all, let's install Hyper-V and HGS Client on Host1 *(*and later on Host2*)*:

Install-WindowsFeature Hyper-V, HostGuardian -IncludeManagementTools -Restart

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Install-WindowsFeature Hyper-V, HostGuardian -IncludeManagementTools -Restart_
```

Then let's configure the host's Key Protection and Attestation URLs by issuing the following command:

Set-HgsClientConfiguration -AttestationServerUrl 'http://hgs.hgscloud.local/Attestation’ -KeyProtectionServerUrl 'http://hgs.hgscloud.local/KeyProtection’

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Set-HgsClientConfiguration -AttestationServerUrl 'http://hgs.hgscloud.local/Attestation' -KeyPro
tectionServerUrl 'http://hgs.hgscloud.local/KeyProtection'


IsHostGuarded            : True
Mode                     : HostGuardianService
KeyProtectionServerUrl   : http://hgs.hgscloud.local/KeyProtection
AttestationServerUrl     : http://hgs.hgscloud.local/Attestation
AttestationOperationMode : ActiveDirectory
AttestationStatus        : Passed
AttestationSubstatus     : NoInformation


PS C:\Windows\system32> _
```

By the way, should there be any problem with HGS client configuration you can run the following cmdlet (for example, when I first tried to run Set-HgsClientConfiguration I forgot to run Add-HgsAttestationHostGroup before it and the resulting explanation was very useful in troubleshooting):

Get-HgsTrace -RunDiagnostics -Detailed

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-HgsTrace -RunDiagnostics -Detailed
Overall Result: Fail
    Host1: Fail
        Test Attestation: Fail
            Check Attestation Status: Fail
            >>> Host is not authorized to use HGS.  Ensure the host is a member of an authorized host group registered
            >>> on the server with the Add-HgsAttestationHostGroup command and that a fresh Kerberos ticket has been
            >>> granted with the new membership.  (Have you restarted this host since updating its group memberships?)
        HGS Client Configuration: Pass
            Code Integrity Policy Installed: NotApplicable
            Code Integrity Policy Active: NotApplicable
            Attestation Service Responds to Requests: Pass
            Key Protection Service Responds to Requests: Pass
            Valid VSM IDK Detected at Boot: NotApplicable
        Hardware: Fail
            Secure Boot: DependencyFailed
                UefiHardwareProfileCollector: Exception
                >>> Could not read the UEFI variable "SecureBoot".  This usually indicates a lack of administrator
                >>> privileges or a host that utilizes a legacy BIOS.  If you have sufficient privileges and are on a
                >>> UEFI-enabled host, verify you have the latest version of the manufacturer's firmware and drivers.
                >>> You may need to run this locally if the cmdlet was called remotely.
            Full Boot: NotApplicable
            TPM Presence: NotApplicable
            TPM Version: NotApplicable
            UEFI Setup Mode: DependencyFailed
                UefiHardwareProfileCollector: Exception
                >>> Could not read the UEFI variable "SecureBoot".  This usually indicates a lack of administrator
                >>> privileges or a host that utilizes a legacy BIOS.  If you have sufficient privileges and are on a
                >>> UEFI-enabled host, verify you have the latest version of the manufacturer's firmware and drivers.
                >>> You may need to run this locally if the cmdlet was called remotely.
        HTTPS: Pass
            Attestation Server Certificate Verification: NotApplicable
            Key Protection Server Certificate Verification: NotApplicable
        Network: Fail
            HGS Servers Reachable: NotRun
            >>> No IP's could be found to test.  Check DNS and service URL configuration.
            DNS Servers Reachable: Fail
            >>> DNS server at 10.0.0.2 could not be contacted within the time allotted by the DNS client; this server
            >>> cannot be used to resolve names.
            >>> No DNS servers were reachable.  Host will be unable to resolve any names including the HGS service URL.
            >>> Resolve any networking and/or configuration problems with this host's DNS servers to repair name
            >>> resolution.  Host must be able to communicate with DNS servers on port 53 within 8 seconds in order to
            >>> resolve names.
            Resolves Service Hostname: Fail
            >>> No DNS servers were reachable.  Host will be unable to resolve any names including the HGS service URL.
            Service Hostname Resolves the Same on All DNS Servers: NotRun
            >>> No IP's could be found to test.  Check DNS and service URL configuration.
        Best Practices: Pass
            Local Mode: Pass
            Resolves Service Hostname to Multiple Addresses: NotApplicable
            >>> No DNS servers were reachable.  Host will be unable to resolve any names including the HGS service URL.

Traces have been stored at "C:\Users\fabricadmin\AppData\Local\Temp\HgsDiagnostics-20180606-170130".

PS C:\Windows\system32>
```

To test the attestation we can run this command:

Get-HgsClientConfiguration

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-HgsClientConfiguration


IsHostGuarded             : True
Mode                      : HostGuardianService
KeyProtectionServerUrl    : http://hgs.hgscloud.local/KeyProtection
AttestationServerUrl      : http://hgs.hgscloud.local/Attestation
AttestationOperationMode  : ActiveDirectory
AttestationStatus         : Passed
AttestationSubstatus      : NoInformation


PS C:\Windows\system32>
```

In part3 we will shield the DC virtual machine and see on which hosts it will be allowed to run.