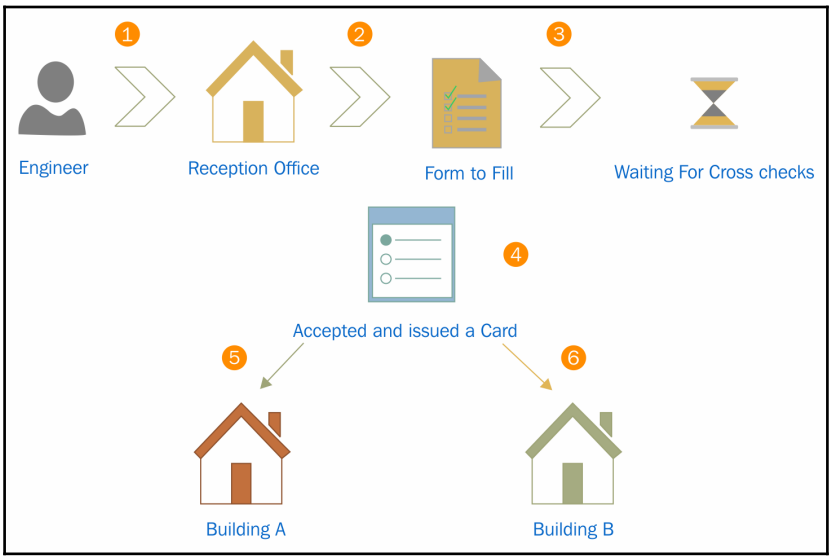
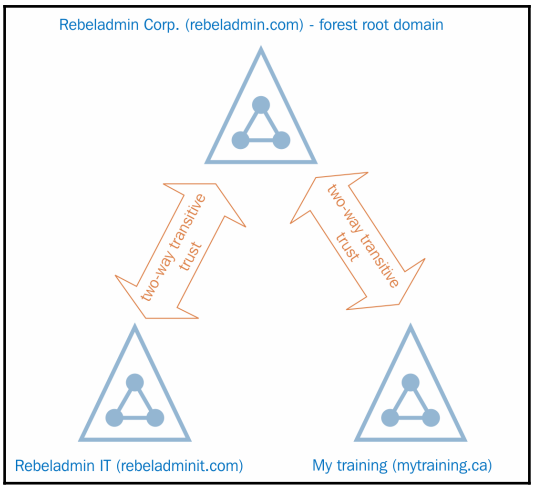
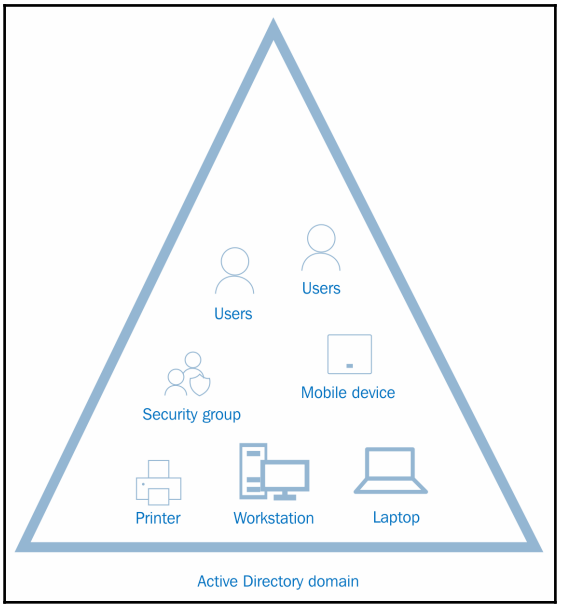
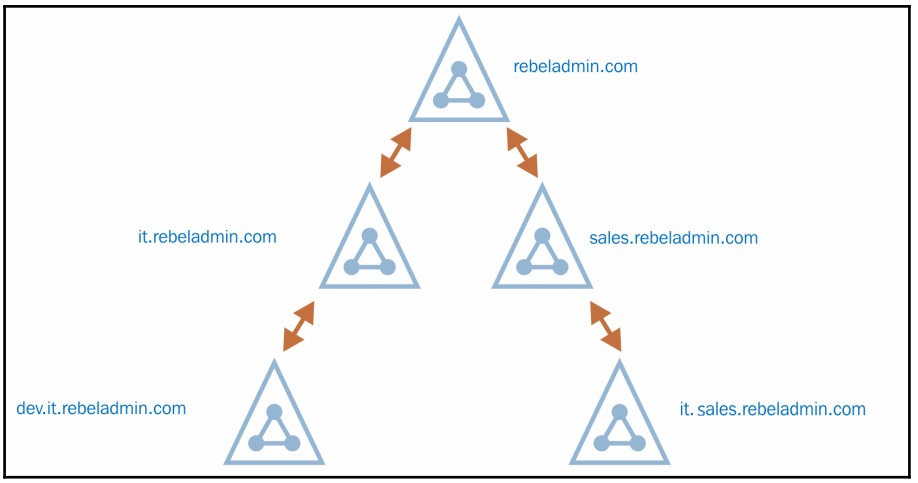
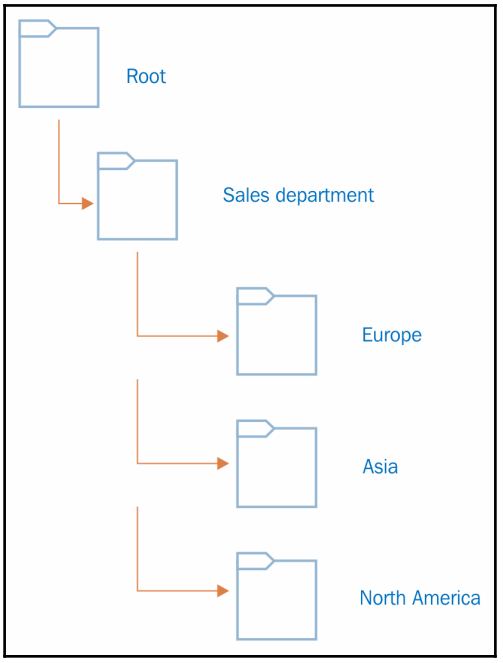
Chapter 1: Active Directory Fundamentals

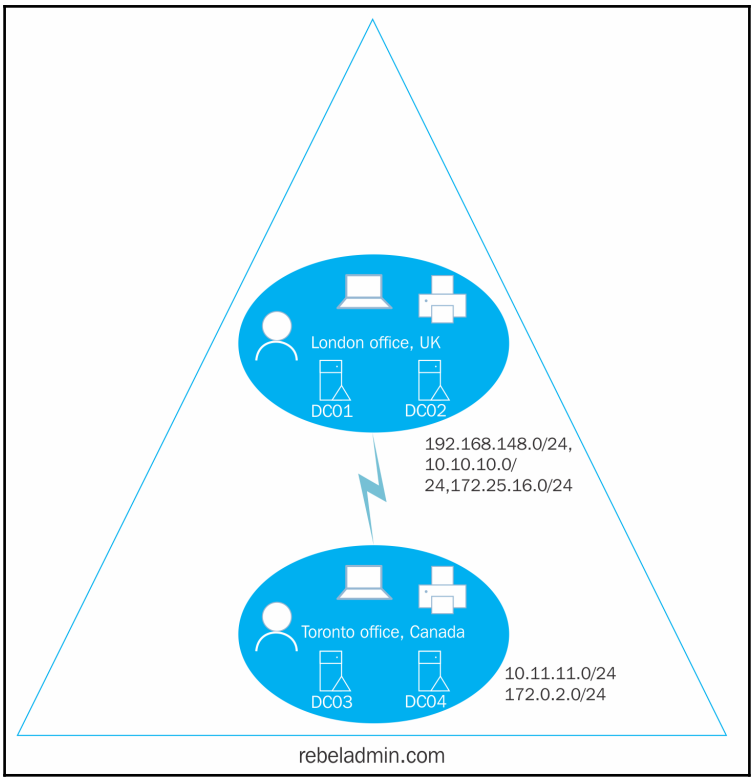


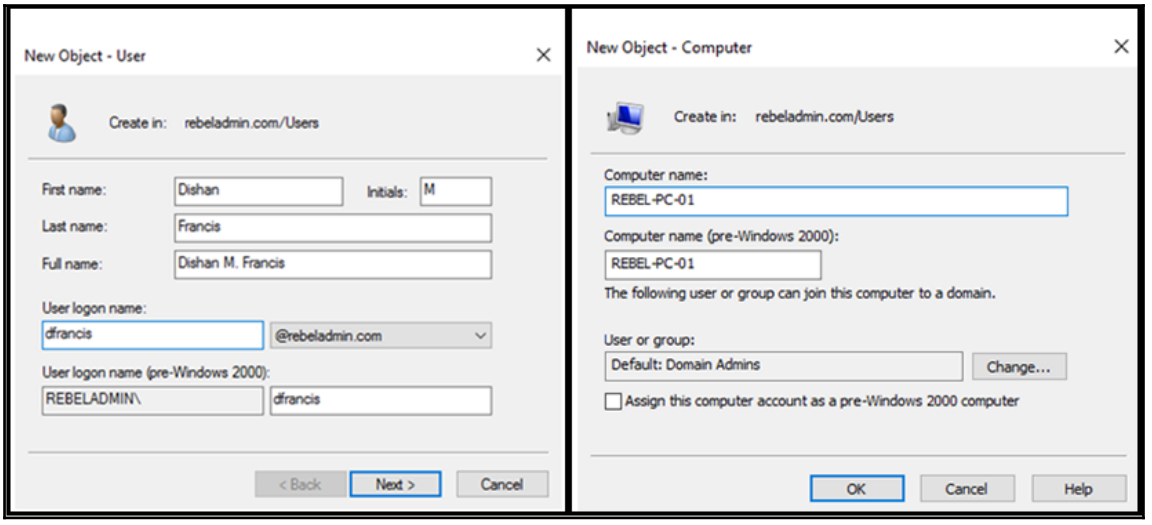

Rebeladmin Corp. (rebeladmin.com) - forest root domain
two-way transitive trust
two-way transitive trust
Rebeladmin IT (rebeladminit.com)
My training (mytraining.ca)

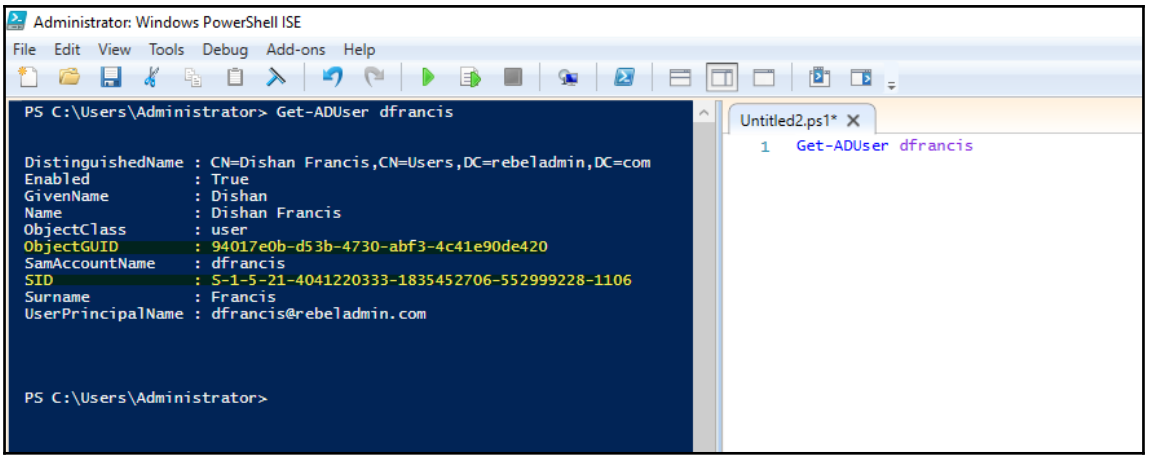

Users
Users
Mobile device
Security group
Printer
Workstation
Laptop
Active Directory domain

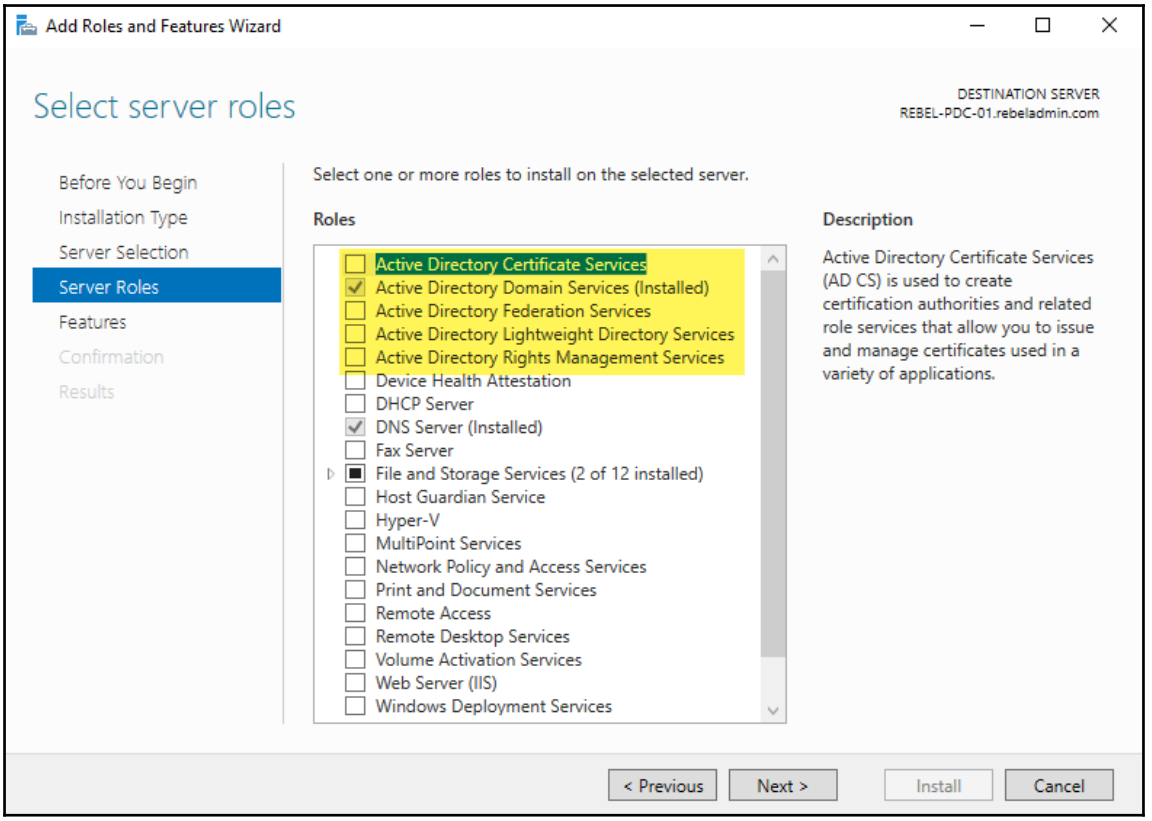

rebeladmin.com
it.rebeladmin.com
sales.rebeladmin.com
dev.it.rebeladmin.com
it. sales.rebeladmin.com


Root
Sales department
Europe
Asia
North America

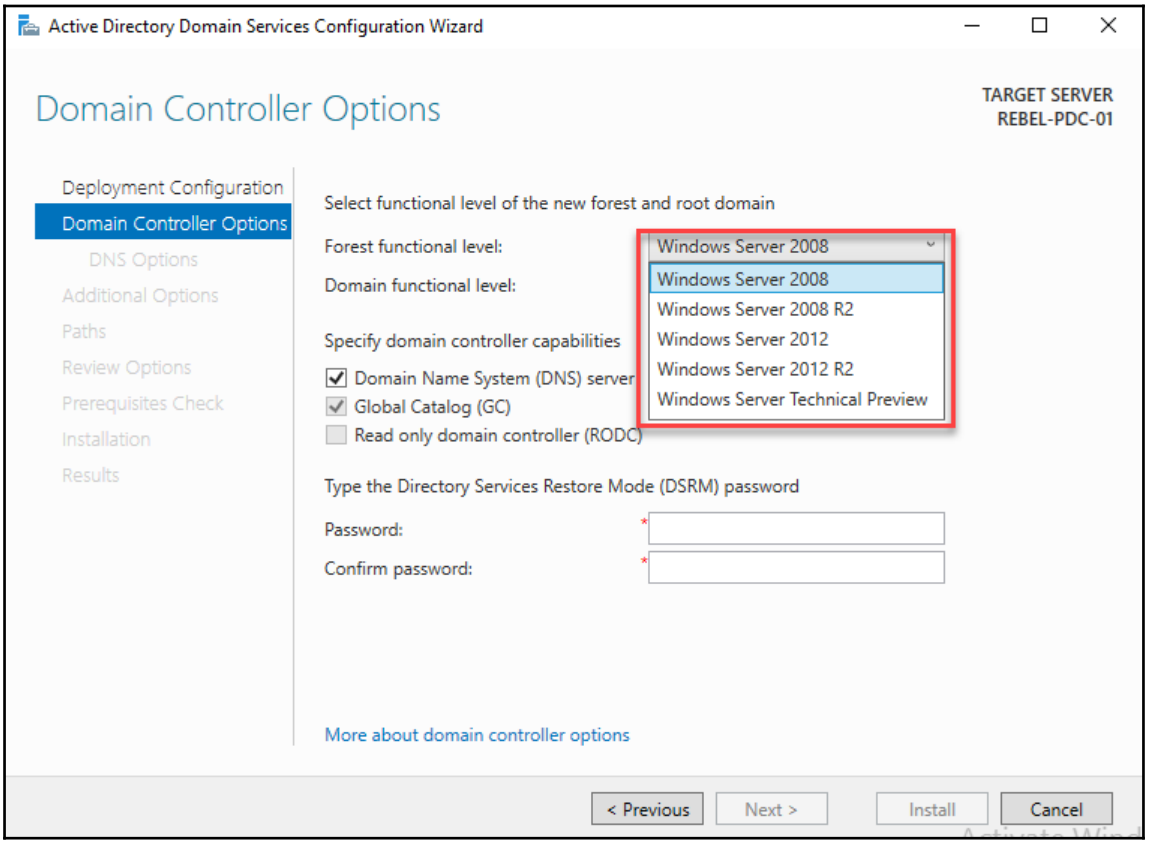

London office, UK
DC01
DC02
192.168.148.0/24,
10.10.10.0/
24,172.25.16.0/24
Toronto office, Canada
DC03
DC04
10.11.11.0/24
172.0.2.0/24
rebeladmin.com

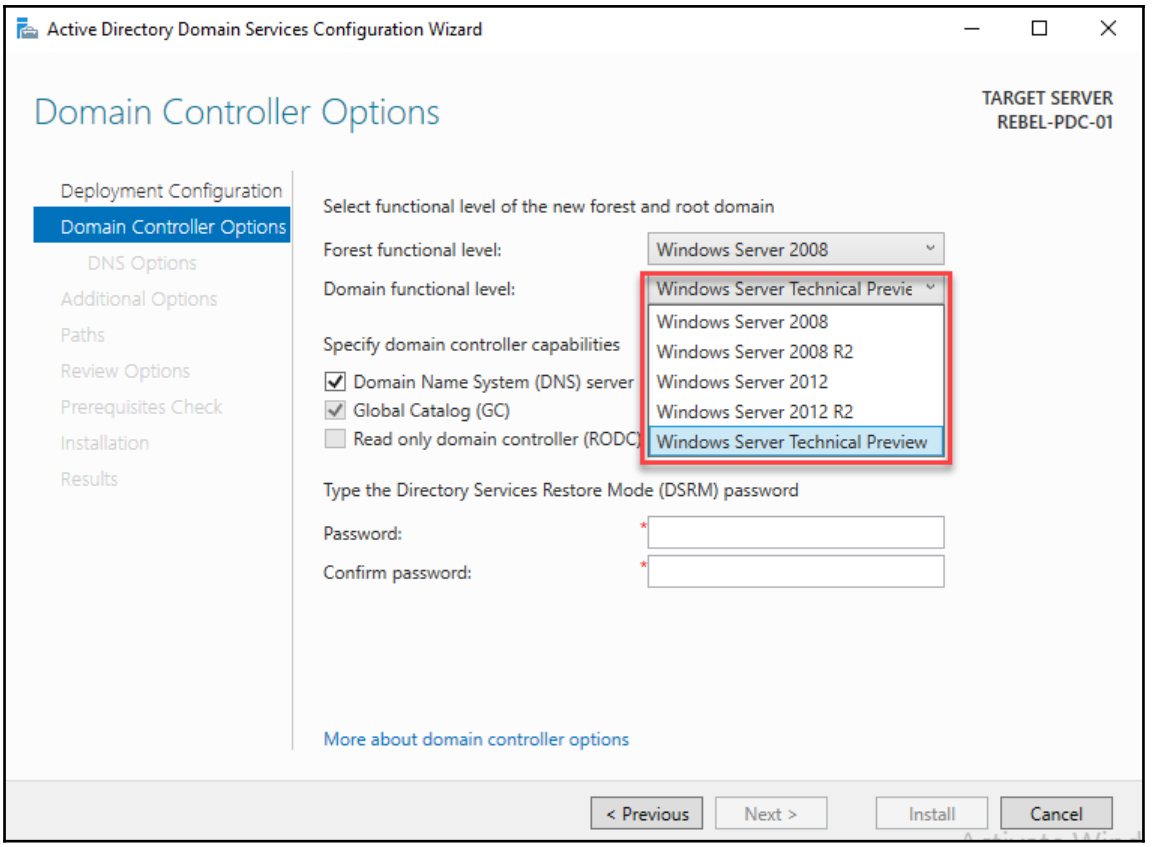

New Object - User
Create in: rebeladmin.com/Users
First name:
Dishan
Initials:
M
Last name:
Francis
Full name:
Dishan M. Francis
User logon name:
dfrancis
@rebeladmin.com
User logon name (pre-Windows 2000):
REBELADMIN\
dfrancis
< Back
Next >
Cancel
New Object - Computer
Create in: rebeladmin.com/Users
Computer name:
REBEL-PC-01
Computer name (pre-Windows 2000):
REBEL-PC-01
The following user or group can join this computer to a domain.
User or group:
Default: Domain Admins
Change...
Assign this computer account as a pre-Windows 2000 computer
OK
Cancel
Help

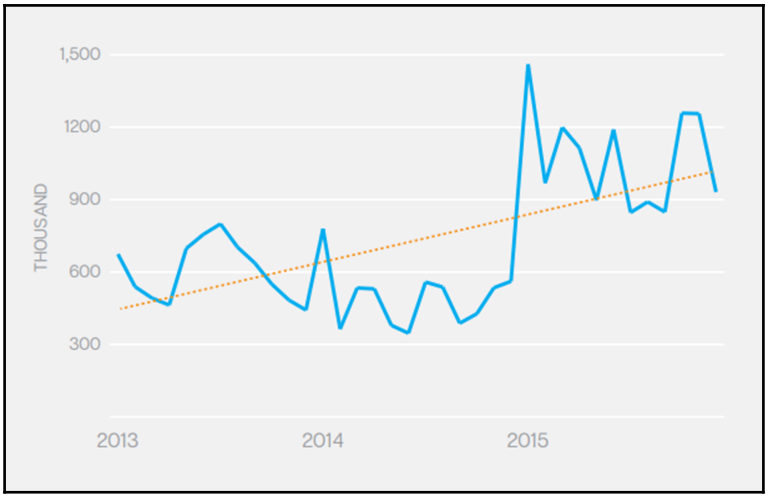

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\Users\Administrator> Get-ADUser dfrancis
DistinguishedName : CN=Dishan Francis,CN=Users,DC=rebeladmin,DC=com
Enabled : True
GivenName : Dishan
Name : Dishan Francis
ObjectClass : user
ObjectGUID : 94017e0b-d53b-4730-abf3-4c41e90de420
SamAccountName : dfrancis
SID : S-1-5-21-4041220333-1835452706-552999228-1106
Surname : Francis
UserPrincipalName : dfrancis@rebeladmin.com
PS C:\Users\Administrator>
Untitled2.ps1*
1 Get-ADUser dfrancis


Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
REBEL-PDC-01.rebeladmin.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (2 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
< Previous
Next >
Install
Cancel

Chapter 2: Active Directory Domain Services 2016



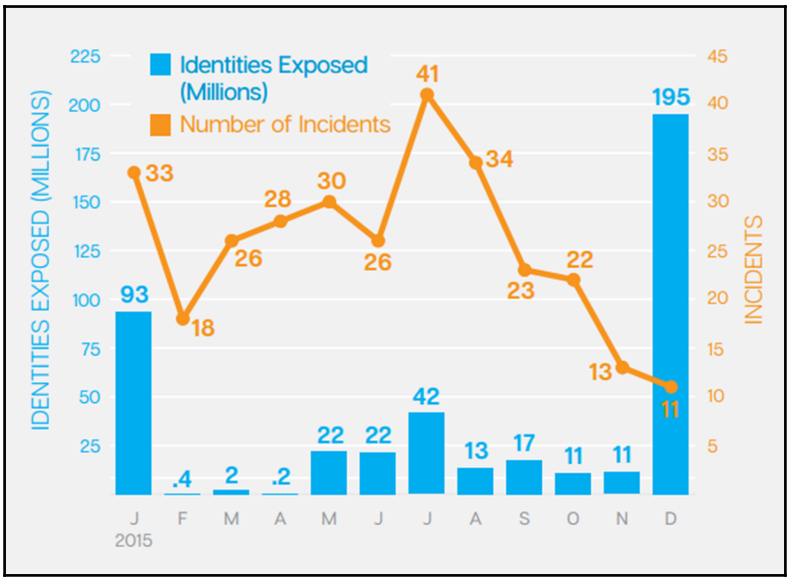

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
REBEL-PDC-01
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2008
Domain functional level:
Windows Server Technical Previe
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server Technical Preview
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel

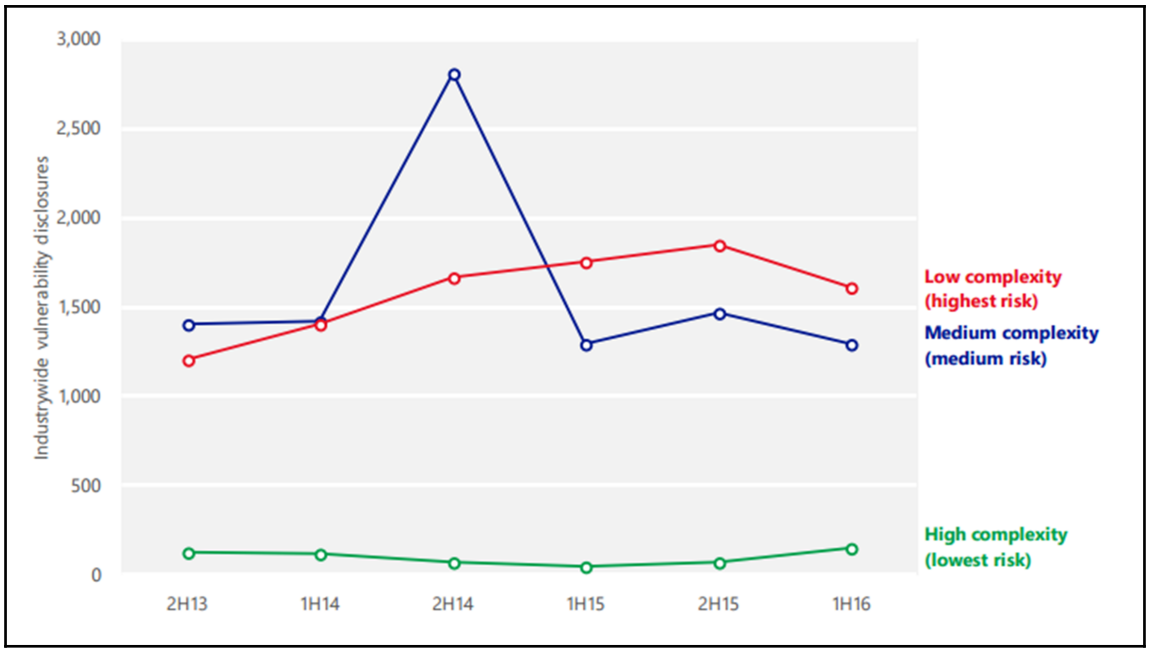

1,500
1200
900
600
300
THOUSAND
2013
2014
2015

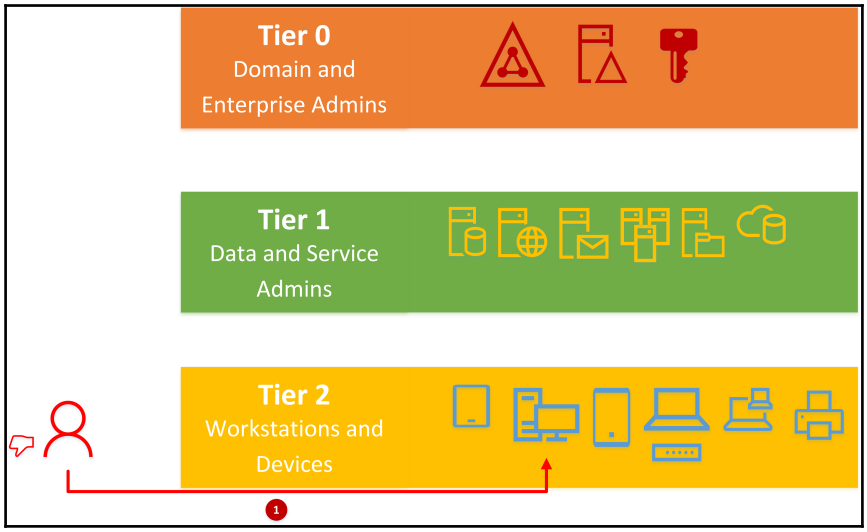
Top 10 Types of Information Exposed

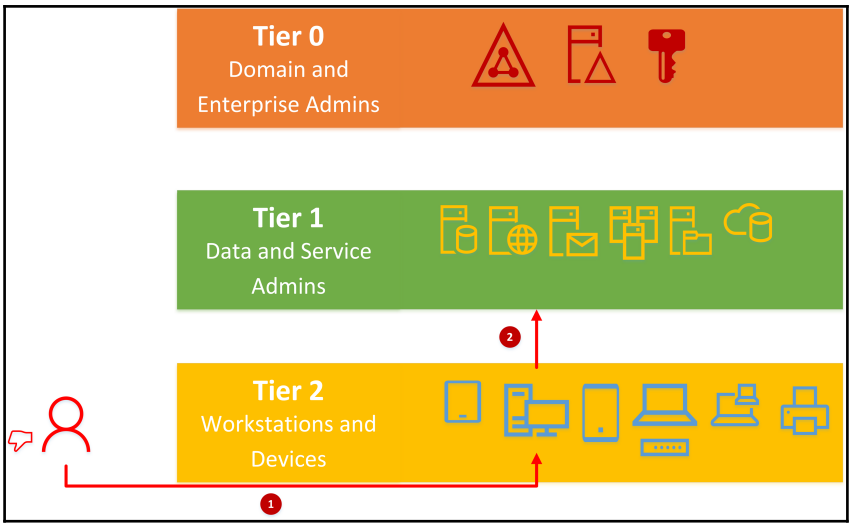
Financial information includes stolen credit card details and other financial credentials.

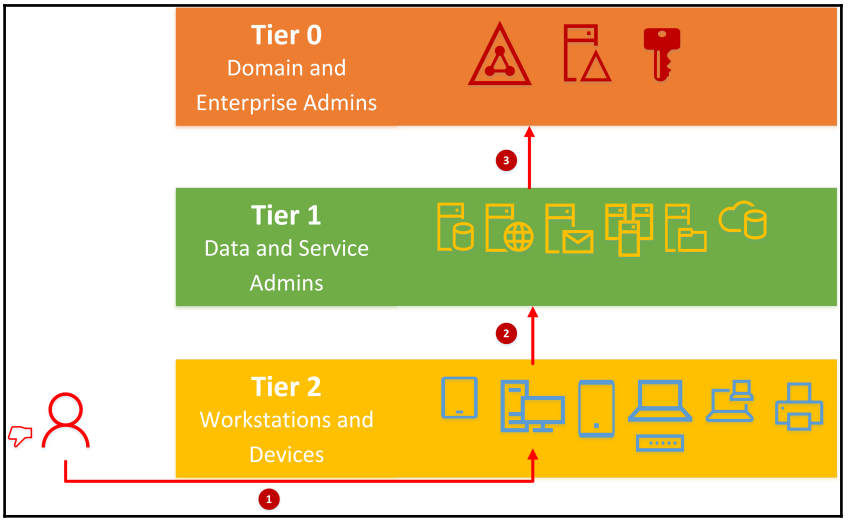
	2015 Type	2015 %	2014 Type	2014 %
1	Real Names	78%	Real Names	69%
2	Home Addresses	44%	Gov. ID Numbers (e.g., SSN)	45%
3	Birth Dates	41%	Home Addresses	43%
4	Gov. ID Numbers (e.g., SSN)	38%	Financial Information	36%
5	Medical Records	36%	Birth Dates	35%
6	Financial Information	33%	Medical Records	34%
7	Email Addresses	21%	Phone Numbers	21%
8	Phone Numbers	19%	Email Addresses	20%
9	Insurance	13%	User Names & Passwords	13%
10	User Names & Passwords	11%	Insurance	11%

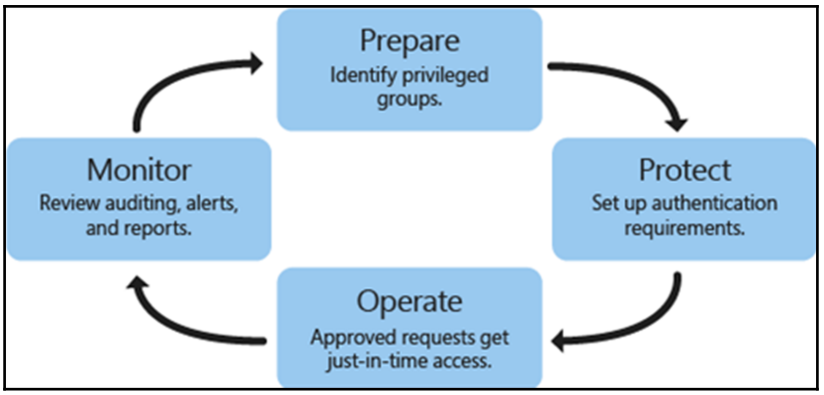


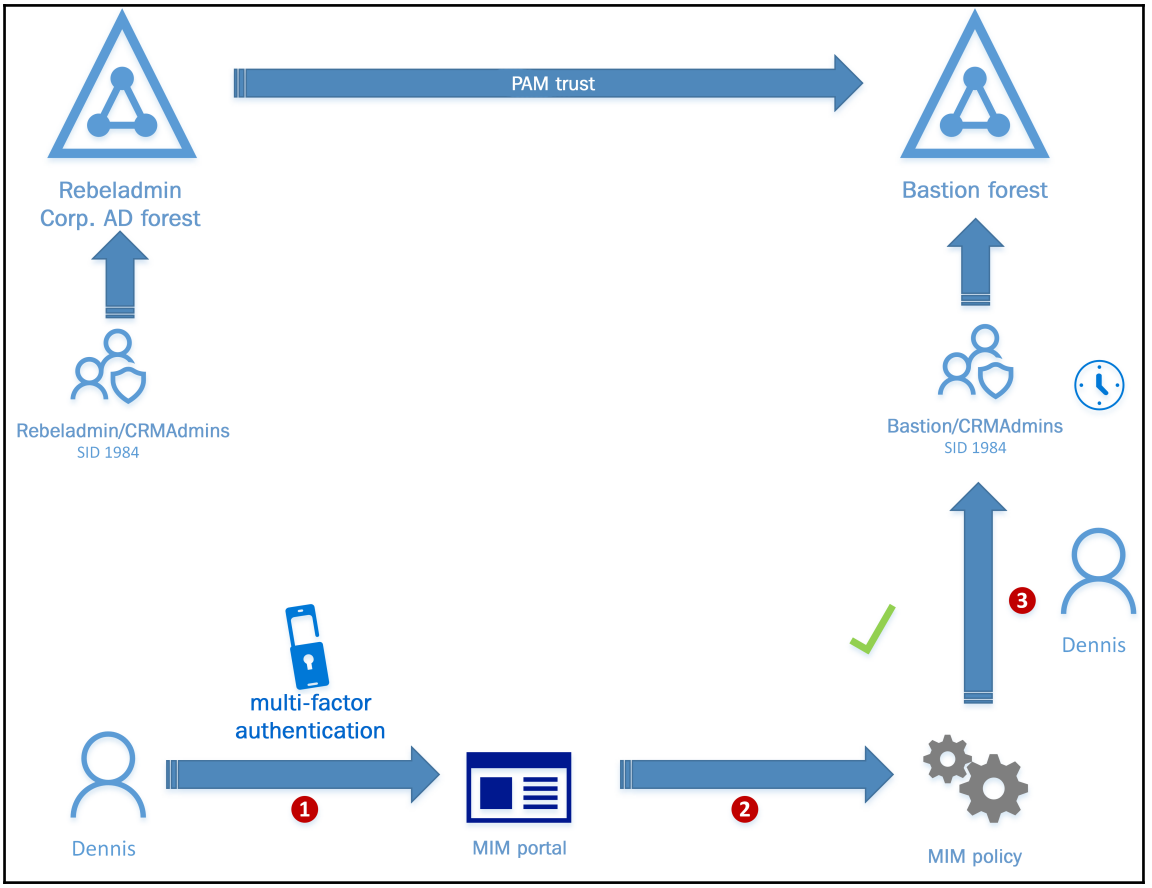

3,000
2,500
2,000
1,500
1,000
500
0
Industrywide vulnerability disclosures
2H13
1H14
2H14
1H15
2H15
1H16
Low complexity (highest risk)
Medium complexity (medium risk)
High complexity (lowest risk)

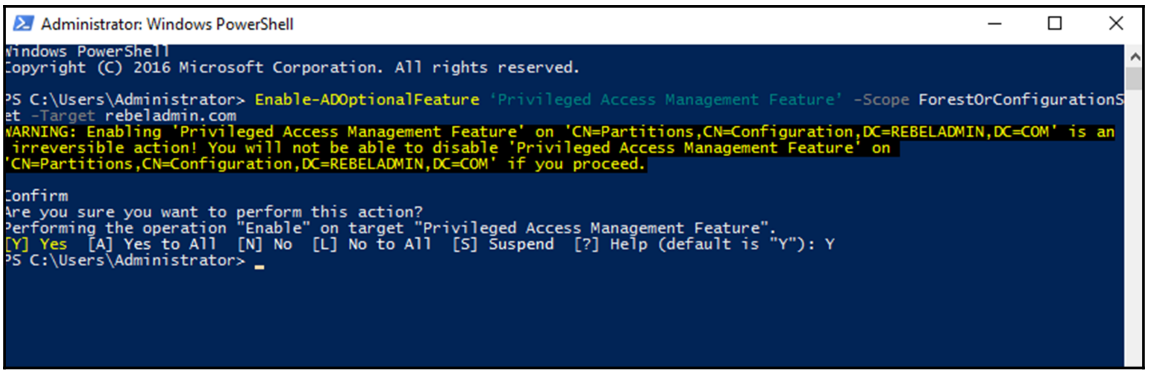

Tier 0
Domain and Enterprise Admins
Tier 1
Data and Service Admins
Tier 2
Workstations and Devices
1

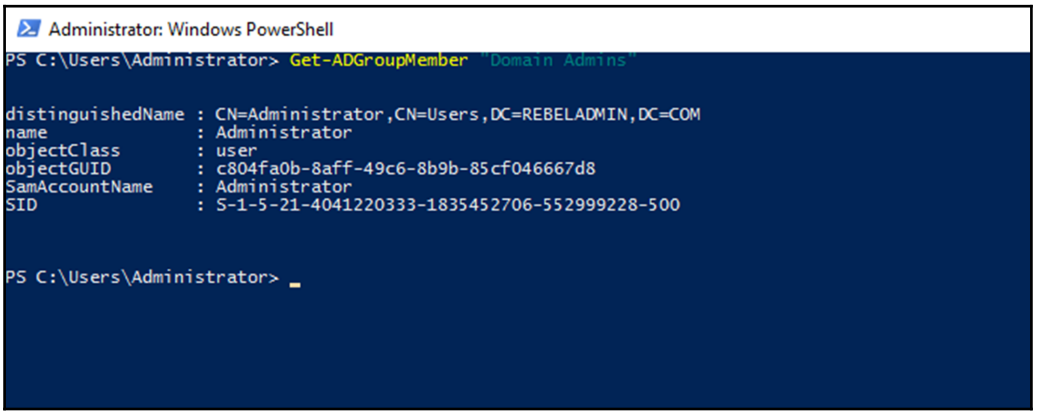

Tier 0
Domain and
Enterprise Admins
Tier 1
Data and Service
Admins
Tier 2
Workstations and
Devices
2
1

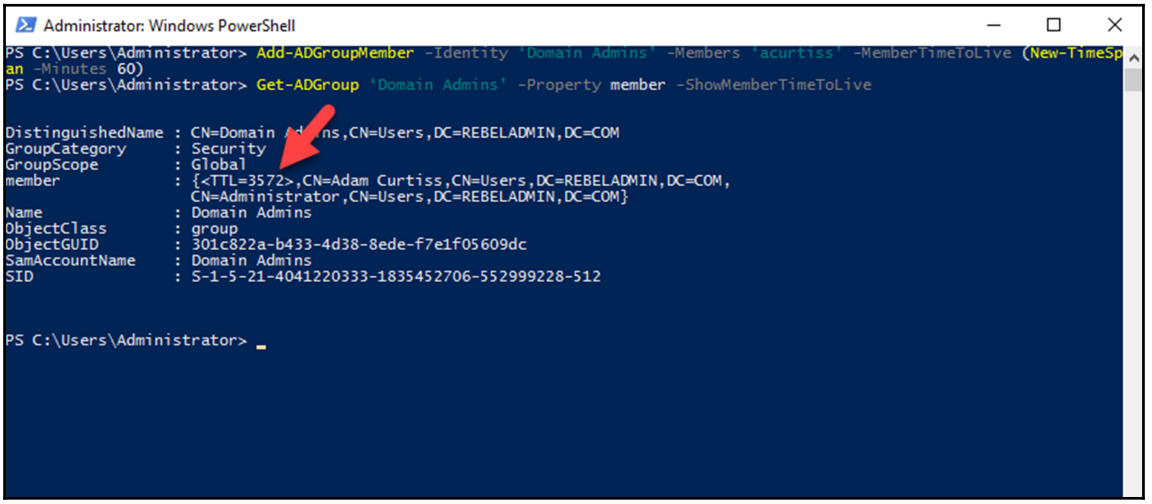

Tier 0
Domain and
Enterprise Admins
Tier 1
Data and Service
Admins
Tier 2
Workstations and
Devices
3
2
1

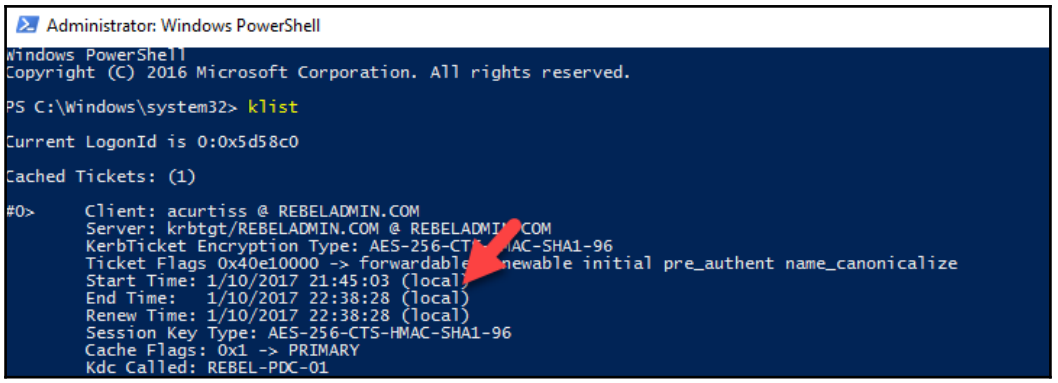

Prepare
Identify privileged groups.
Protect
Set up authentication requirements.
Operate
Approved requests get just-in-time access.
Monitor
Review auditing, alerts, and reports.


PAM trust
Rebeladmin
Corp. AD forest
Bastion forest
Rebeladmin/CRMAdmins
SID 1984
Bastion/CRMAdmins
SID 1984
multi-factor
authentication
Dennis
Dennis
MIM portal
MIM policy
1
2
3

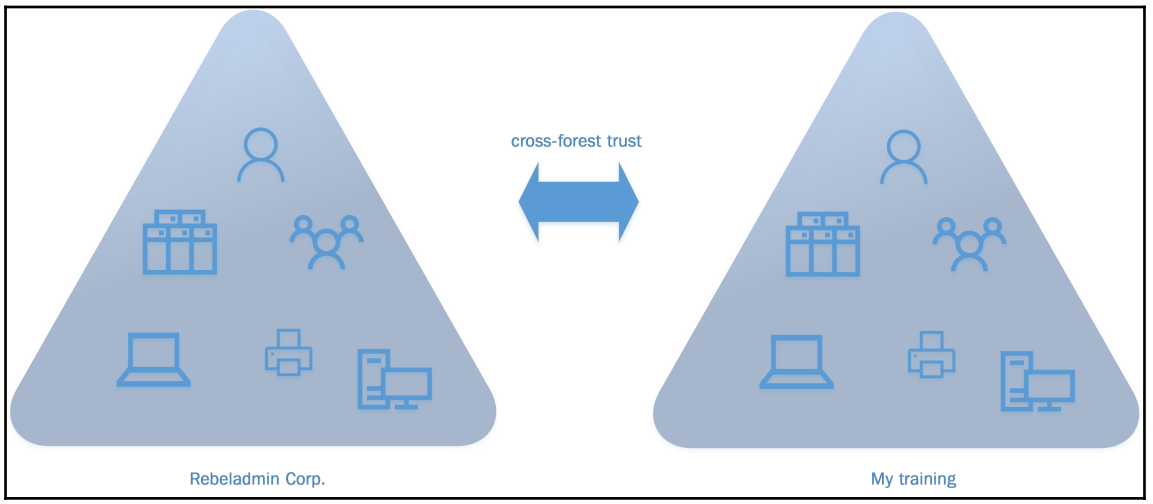

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> Enable-ADOptionalFeature 'Privileged Access Management Feature' -Scope ForestOrConfigurationSet -Target rebeladmin.com
WARNING: Enabling 'Privileged Access Management Feature' on 'CN=Partitions,CN=Configuration,DC=REBELADMIN,DC=COM' is an irreversible action! You will not be able to disable 'Privileged Access Management Feature' on 'CN=Partitions,CN=Configuration,DC=REBELADMIN,DC=COM' if you proceed.
Confirm
Are you sure you want to perform this action?
Performing the operation "Enable" on target "Privileged Access Management Feature".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
PS C:\Users\Administrator>

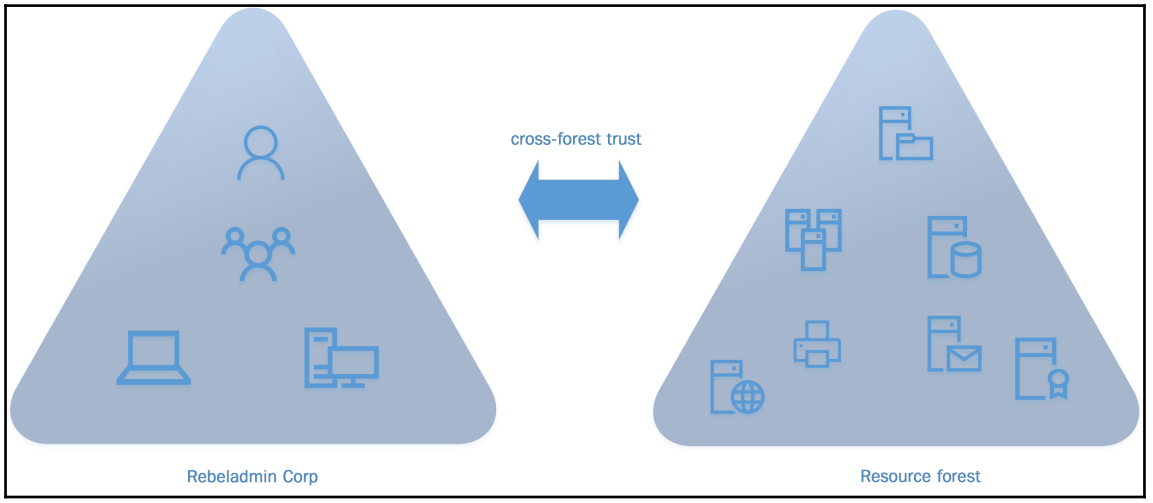

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADGroupMember "Domain Admins"
distinguishedName : CN=Administrator,CN=Users,DC=REBELADMIN,DC=COM
name : Administrator
objectClass : user
objectGUID : c804fa0b-8aff-49c6-8b9b-85cf046667d8
SamAccountName : Administrator
SID : S-1-5-21-4041220333-1835452706-552999228-500
PS C:\Users\Administrator>

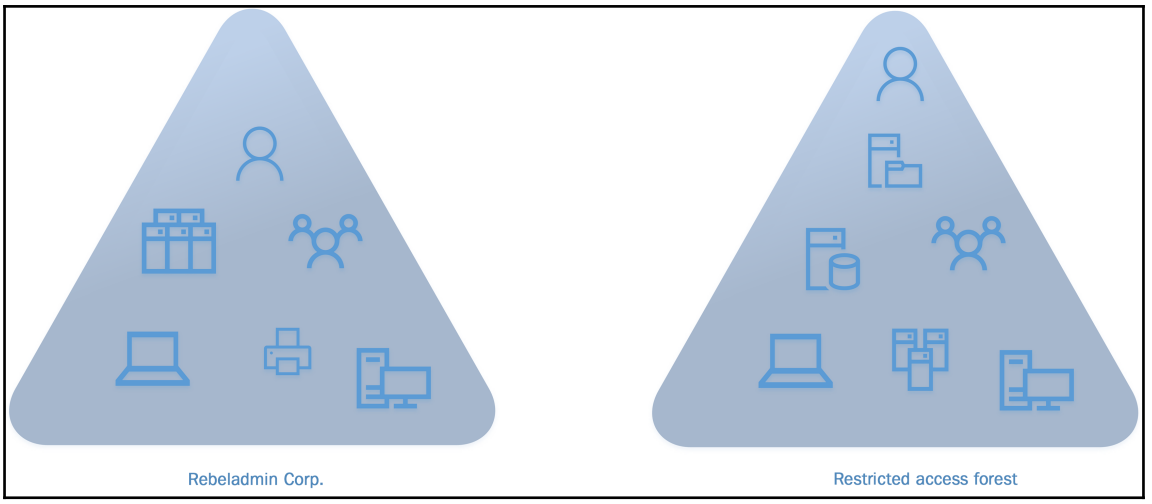

Administrator: Windows PowerShell
PS C:\Users\Administrator> Add-ADGroupMember -Identity 'Domain Admins' -Members 'acurtiss' -MemberTimeToLive (New-TimeSpan -Minutes 60)
PS C:\Users\Administrator> Get-ADGroup 'Domain Admins' -Property member -ShowMemberTimeToLive
DistinguishedName : CN=Domain Admins,CN=Users,DC=REBELADMIN,DC=COM
GroupCategory : Security
GroupScope : Global
member : {<TTL=3572>,CN=Adam Curtiss,CN=Users,DC=REBELADMIN,DC=COM,
CN=Administrator,CN=Users,DC=REBELADMIN,DC=COM}
Name : Domain Admins
ObjectClass : group
ObjectGUID : 301c822a-b433-4d38-8ede-f7e1f05609dc
SamAccountName : Domain Admins
SID : S-1-5-21-4041220333-1835452706-552999228-512
PS C:\Users\Administrator>

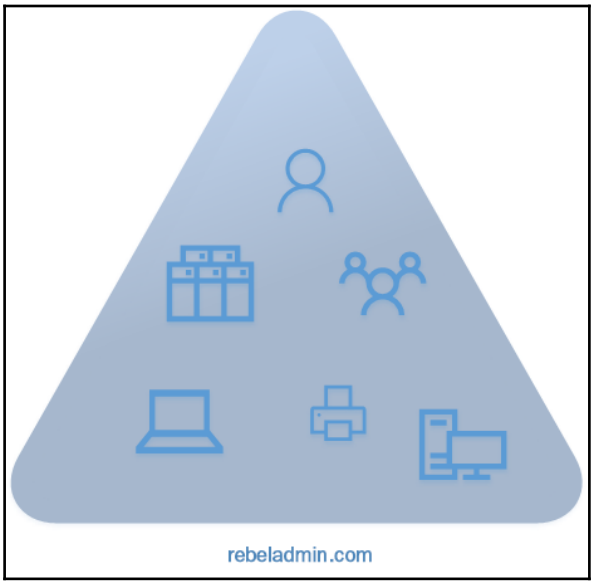

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> klist
Current LogonId is 0:0x5d58c0
Cached Tickets: (1)
#0> Client: acurtiss @ REBELADMIN.COM
Server: krbtgt/REBELADMIN.COM @ REBELADMIN.COM
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 1/10/2017 21:45:03 (local)
End Time: 1/10/2017 22:38:28 (local)
Renew Time: 1/10/2017 22:38:28 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called: REBEL-PDC-01

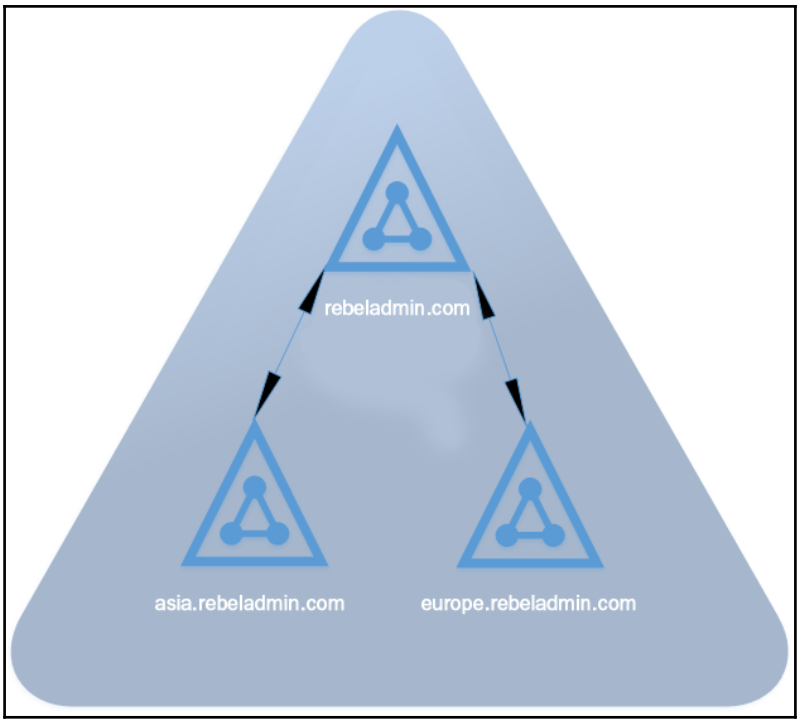
Chapter 3: Designing Active Directory Infrastructure





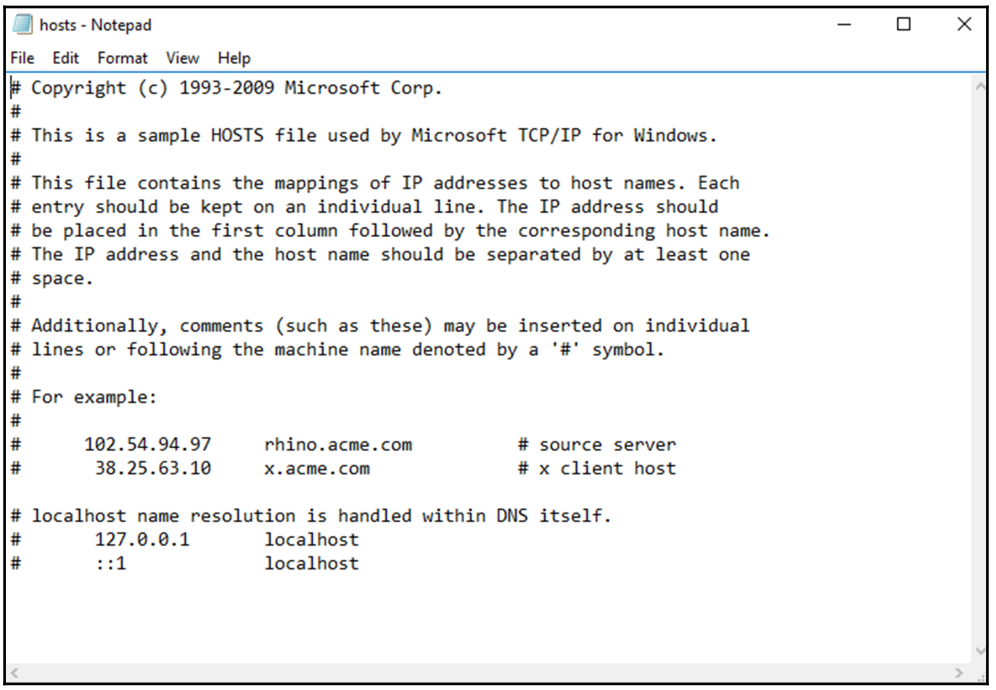

Rebeladmin Corp.
Restricted access forest

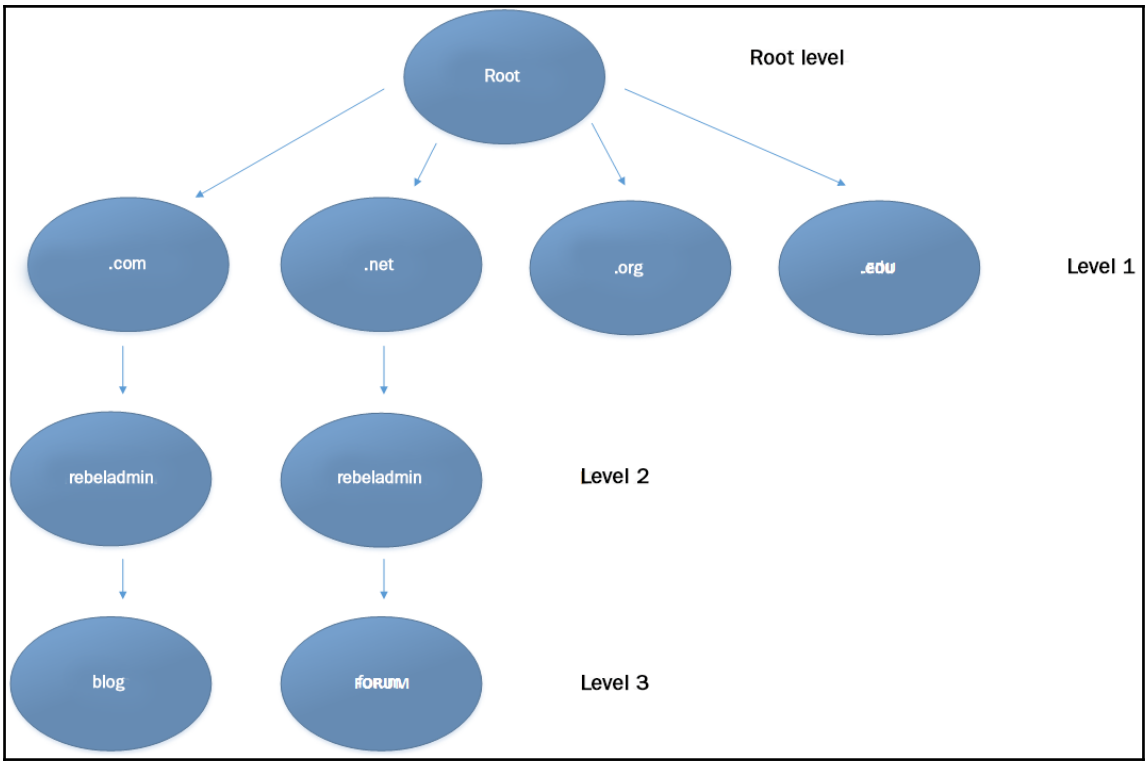

rebeladmin.com



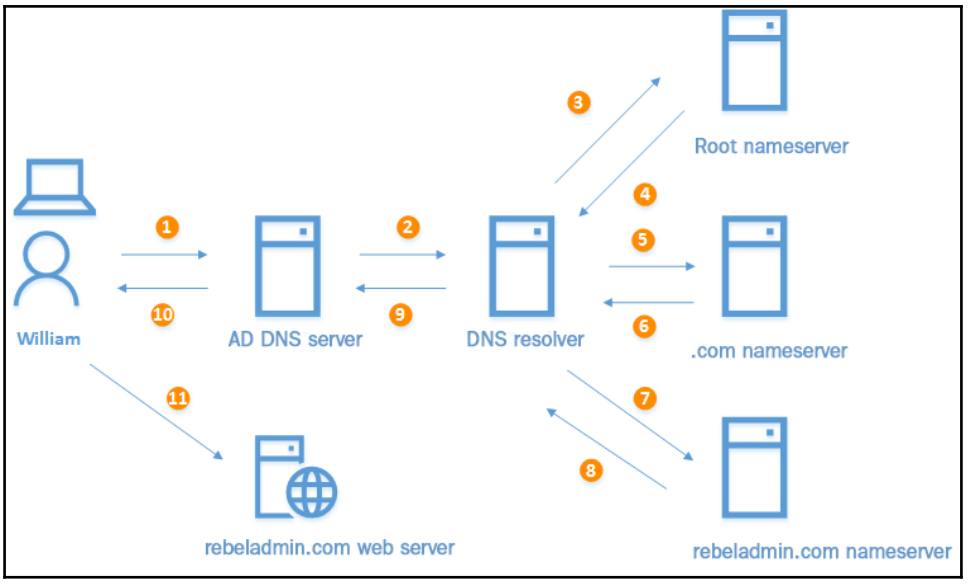

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ADDomain | fl Name,DomainMode


Name       : REBELADMIN
DomainMode : Windows2016Domain


PS C:\Users\Administrator> Get-ADForest | fl Name,ForestMode


Name       : REBELADMIN.COM
ForestMode : Windows2016Forest


PS C:\Users\Administrator> _
```

Chapter 4: Active Directory Domain Name System




Root
Root level
.com
.net
.org
.edu
Level 1
rebeladmin
rebeladmin
Level 2
blog
FORUM
Level 3

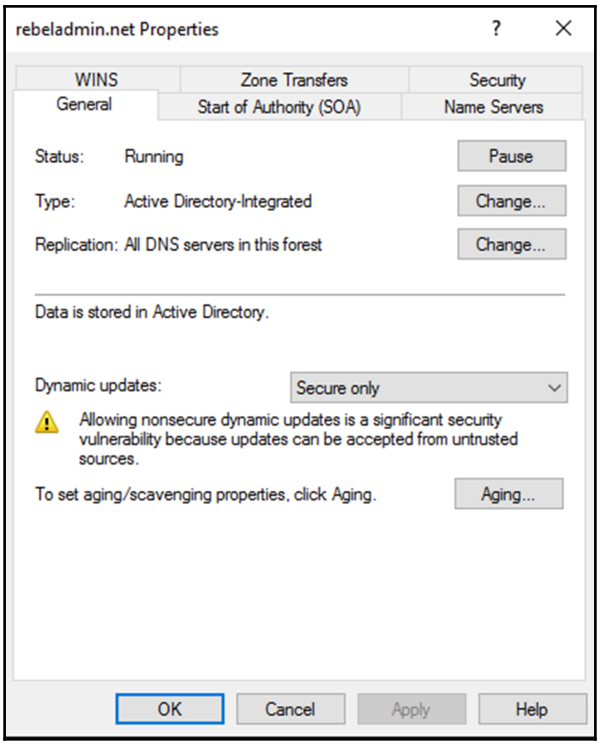

blog.rebeladmin.com

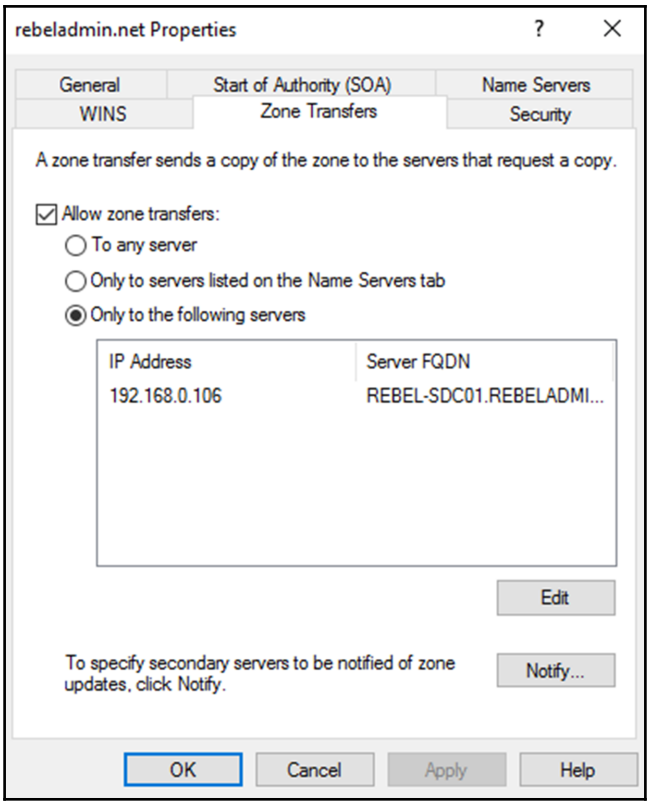


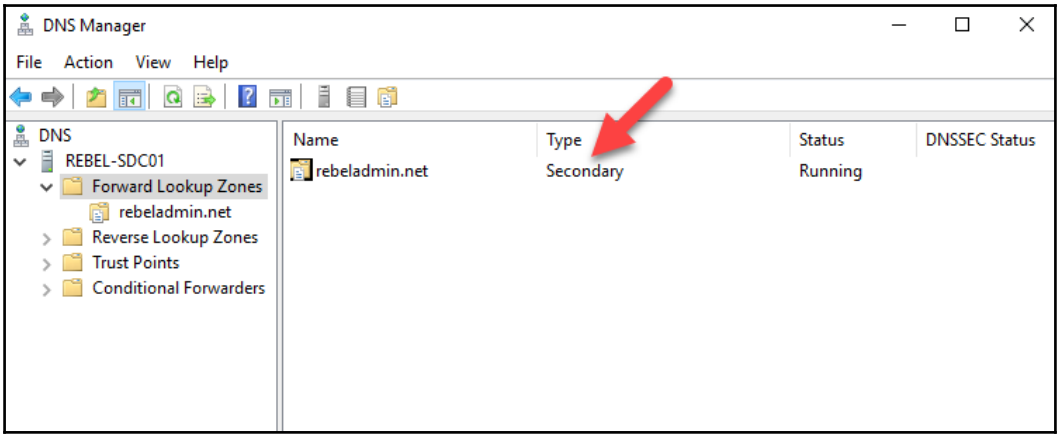

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-DnsServerForwarder


UseRootHint         : True
Timeout(s)          : 3
EnableReordering    : True
IPAddress           : 8.8.8.8
ReorderedIPAddress : 8.8.8.8


PS C:\Users\Administrator>
```

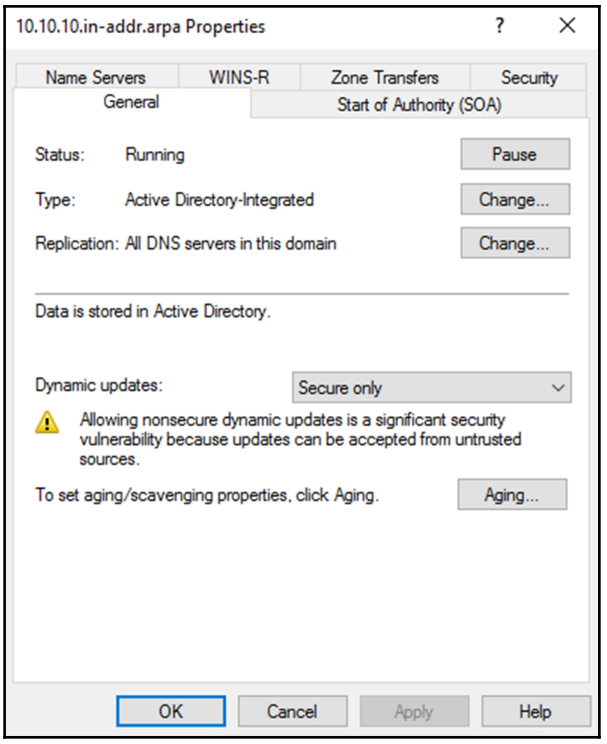
```
PS C:\Users\Administrator> Get-DnsServerRootHint

NameServer          IPAddress
----------          ---------
m.root-servers.net. 2001:dc3::35
l.root-servers.net. 2001:500:9f::42
k.root-servers.net. 2001:7fd::1
j.root-servers.net. 2001:503:c27::2:30
i.root-servers.net. 2001:7fe::53
h.root-servers.net. 2001:500:1::53
g.root-servers.net. 2001:500:12::d0d
f.root-servers.net. 2001:500:2f::f
e.root-servers.net. 2001:500:a8::e
d.root-servers.net. 2001:500:2d::d
c.root-servers.net. 2001:500:2::c
b.root-servers.net. 2001:500:84::b
a.root-servers.net. 2001:503:ba3e::2:30


PS C:\Users\Administrator>
```

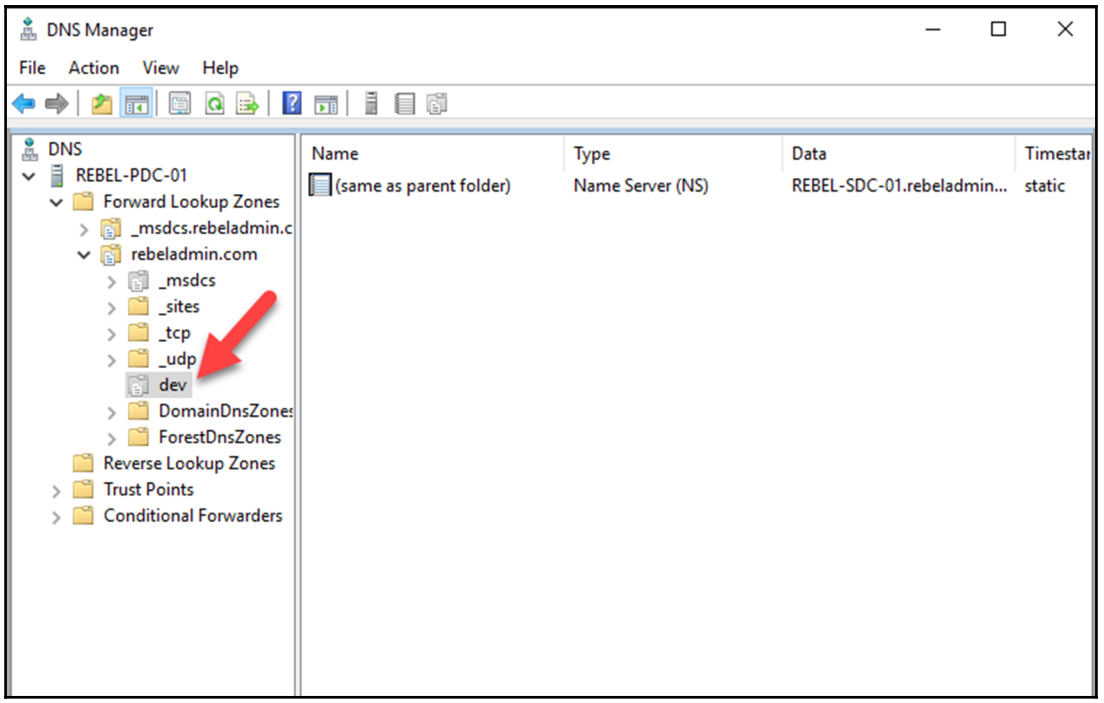
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Add-DnsServerPrimaryZone -Name "rebeladmin.net" -ReplicationScope "Forest" -PassThru

ZoneName                        ZoneType        IsAutoCreated   IsDsIntegrated  IsReverseLookupZone  IsSigned
--------                        --------        -------------   --------------  -------------------  --------
rebeladmin.net                  Primary         False           True            False                False

PS C:\Users\Administrator>
```

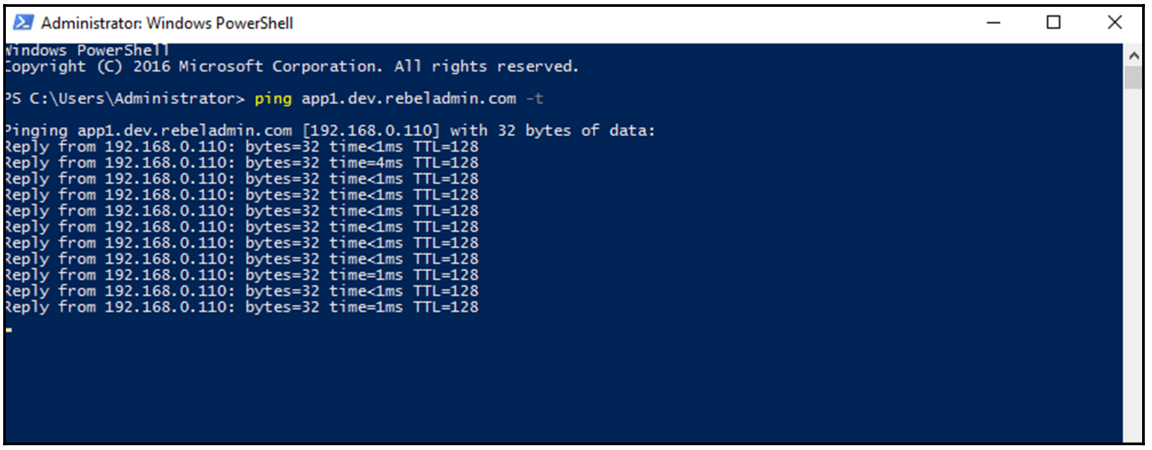

rebeladmin.net Properties
WINS
Zone Transfers
Security
General
Start of Authority (SOA)
Name Servers
Status: Running
Pause
Type: Active Directory-Integrated
Change...
Replication: All DNS servers in this forest
Change...
Data is stored in Active Directory.
Dynamic updates:
Secure only
Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.
To set aging/scavenging properties, click Aging.
Aging...
OK
Cancel
Apply
Help


rebeladmin.net Properties
General
Start of Authority (SOA)
Name Servers
WINS
Zone Transfers
Security
A zone transfer sends a copy of the zone to the servers that request a copy.
Allow zone transfers:
To any server
Only to servers listed on the Name Servers tab
Only to the following servers
IP Address
Server FQDN
192.168.0.106
REBEL-SDC01.REBELADMI...
Edit
To specify secondary servers to be notified of zone updates, click Notify.
Notify...
OK
Cancel
Apply
Help

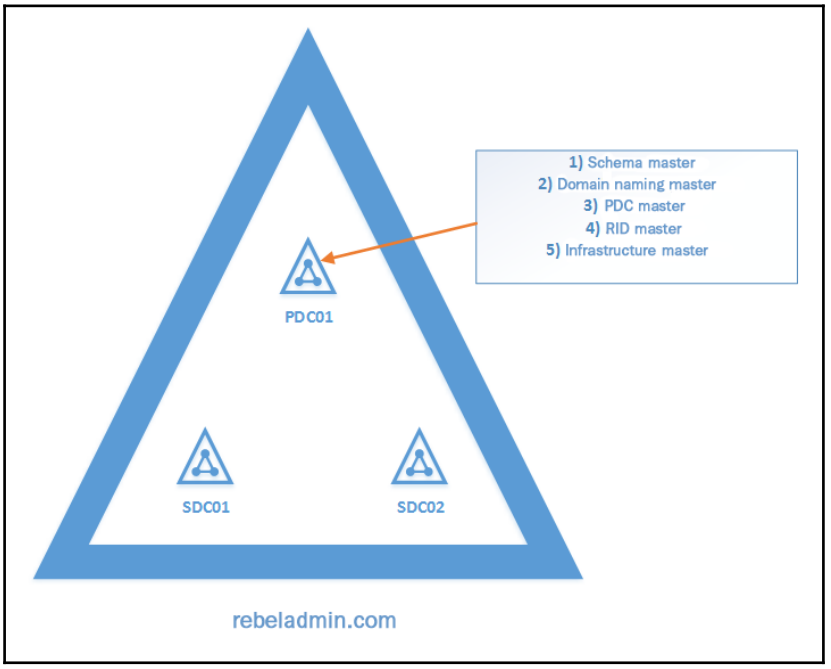

DNS Manager
File
Action
View
Help
DNS
REBEL-SDC01
Forward Lookup Zones
rebeladmin.net
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name
Type
Status
DNSSEC Status
rebeladmin.net
Secondary
Running

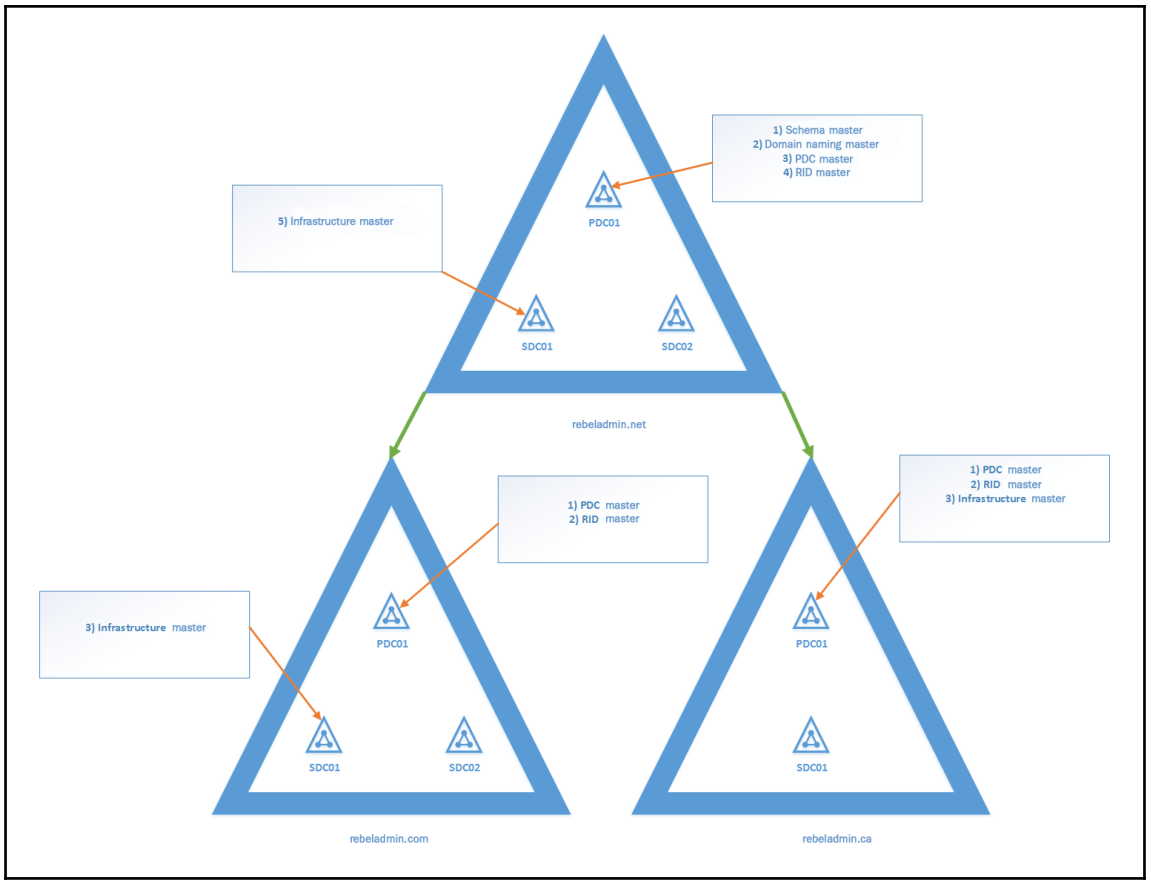

10.10.10.in-addr.arpa Properties
Name Servers
WINS-R
Zone Transfers
Security
General
Start of Authority (SOA)
Status: Running
Pause
Type: Active Directory-Integrated
Change...
Replication: All DNS servers in this domain
Change...
Data is stored in Active Directory.
Dynamic updates:
Secure only
Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.
To set aging/scavenging properties, click Aging.
Aging...
OK
Cancel
Apply
Help

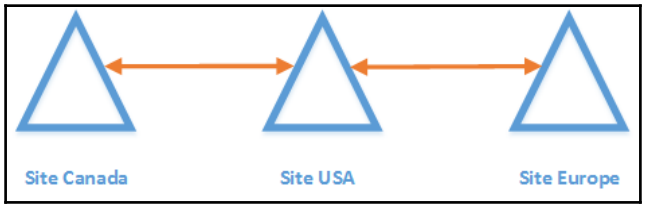

DNS Manager
File Action View Help
DNS
REBEL-PDC-01
Forward Lookup Zones
_msdcs.rebeladmin.c
rebeladmin.com
_msdcs
_sites
_tcp
_udp
dev
DomainDnsZones
ForestDnsZones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name
Type
Data
Timestar
(same as parent folder)
Name Server (NS)
REBEL-SDC-01.rebeladmin...
static

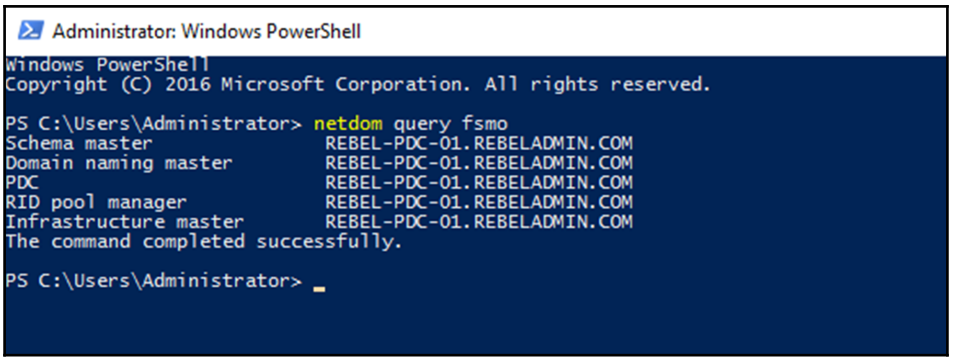

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> ping app1.dev.rebeladmin.com -t
Pinging app1.dev.rebeladmin.com [192.168.0.110] with 32 bytes of data:
Reply from 192.168.0.110: bytes=32 time<1ms TTL=128
Reply from 192.168.0.110: bytes=32 time=4ms TTL=128
Reply from 192.168.0.110: bytes=32 time<1ms TTL=128
Reply from 192.168.0.110: bytes=32 time<1ms TTL=128
Reply from 192.168.0.110: bytes=32 time<1ms TTL=128
Reply from 192.168.0.110: bytes=32 time<1ms TTL=128
Reply from 192.168.0.110: bytes=32 time<1ms TTL=128
Reply from 192.168.0.110: bytes=32 time<1ms TTL=128
Reply from 192.168.0.110: bytes=32 time=1ms TTL=128
Reply from 192.168.0.110: bytes=32 time<1ms TTL=128
Reply from 192.168.0.110: bytes=32 time=1ms TTL=128

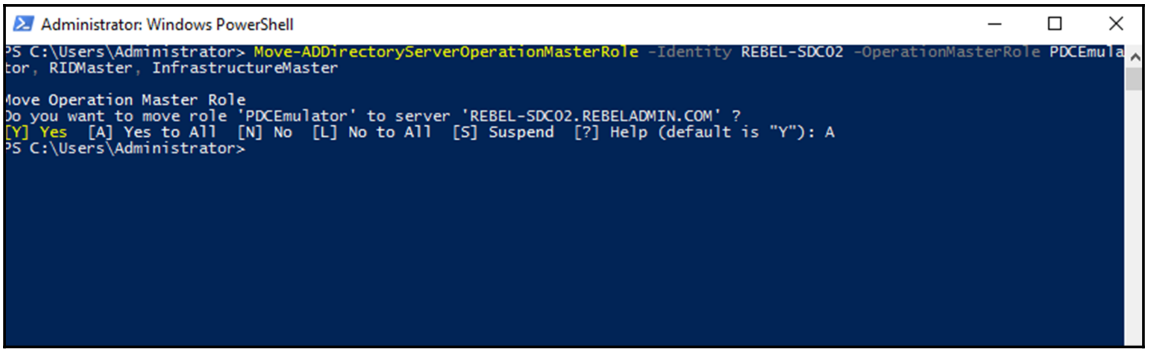
Chapter 5: Placing Operations Master Roles

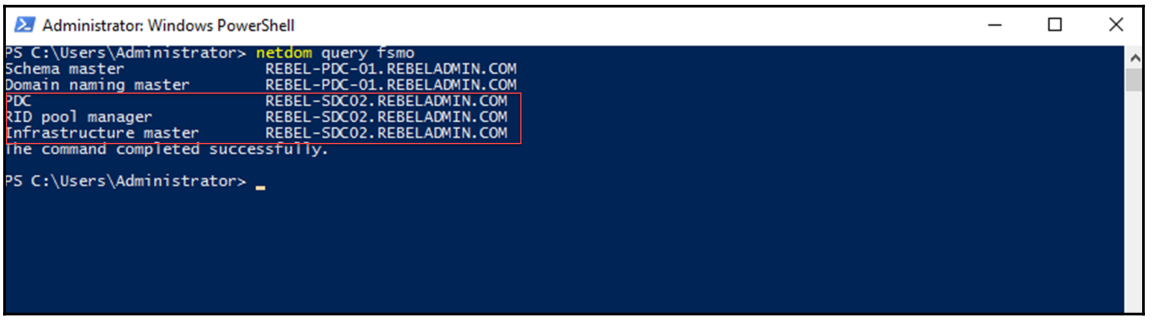


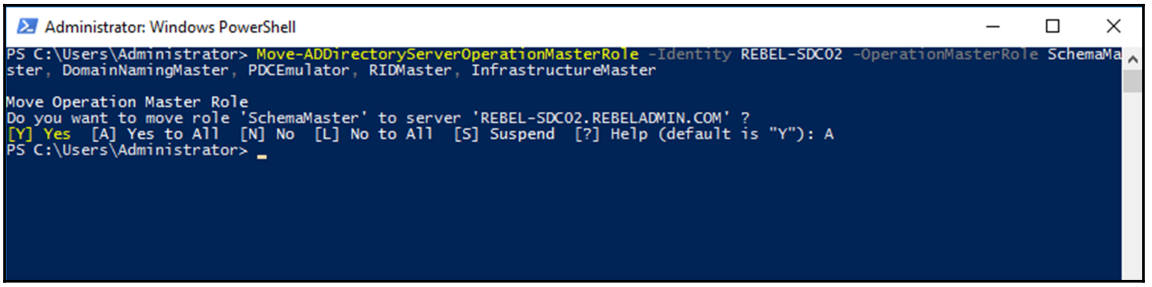

1) Schema master
2) Domain naming master
3) PDC master
4) RID master
5) Infrastructure master
PDC01
SDC01
SDC02
rebeladmin.net
1) PDC master
2) RID master
3) Infrastructure master
PDC01
SDC01
SDC02
rebeladmin.com
1) PDC master
2) RID master
3) Infrastructure master
PDC01
SDC01
rebeladmin.ca

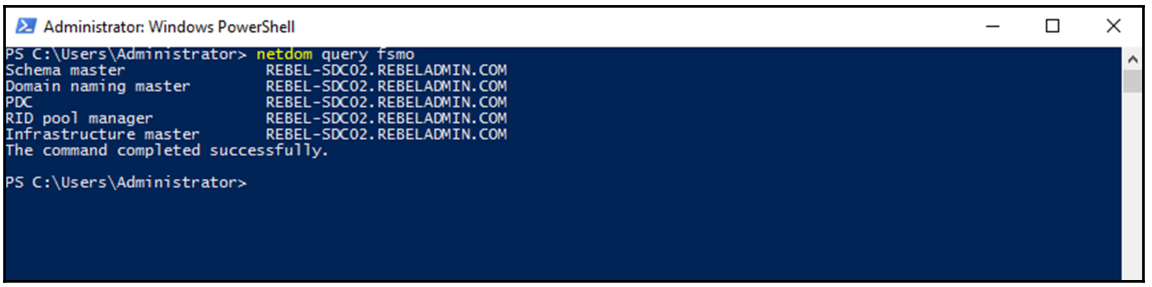

Site Canada
Site USA
Site Europe

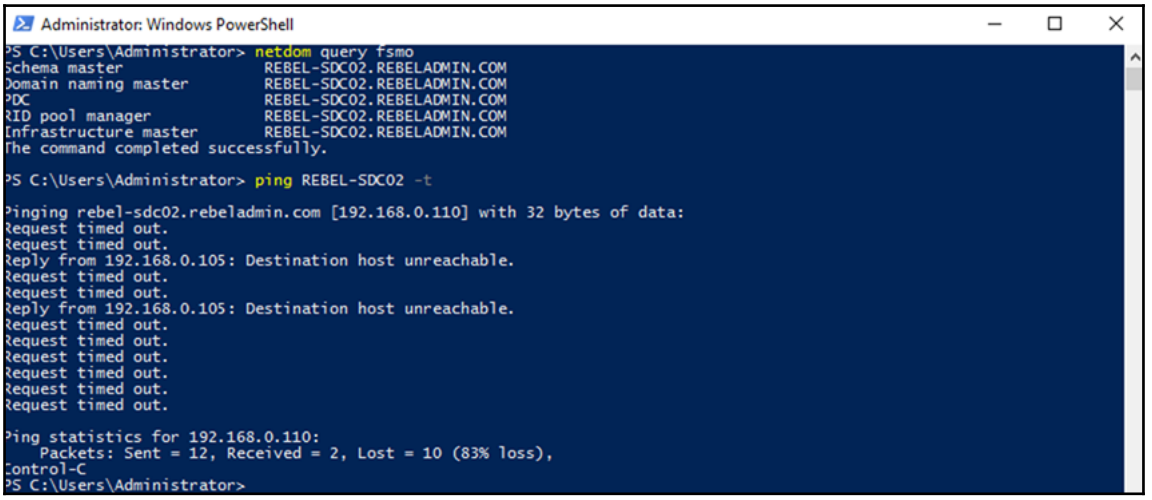

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> netdom query fsmo
Schema master REBEL-PDC-01.REBELADMIN.COM
Domain naming master REBEL-PDC-01.REBELADMIN.COM
PDC REBEL-PDC-01.REBELADMIN.COM
RID pool manager REBEL-PDC-01.REBELADMIN.COM
Infrastructure master REBEL-PDC-01.REBELADMIN.COM
The command completed successfully.
PS C:\Users\Administrator>

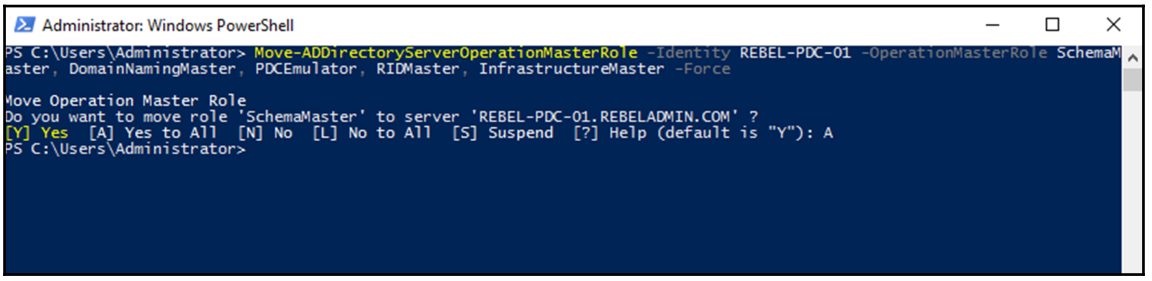

Administrator: Windows PowerShell
PS C:\Users\Administrator> Move-ADDirectoryServerOperationMasterRole -Identity REBEL-SDC02 -OperationMasterRole PDCEmulator, RIDMaster, InfrastructureMaster
Move Operation Master Role
Do you want to move role 'PDCEmulator' to server 'REBEL-SDC02.REBELADMIN.COM' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A
PS C:\Users\Administrator>

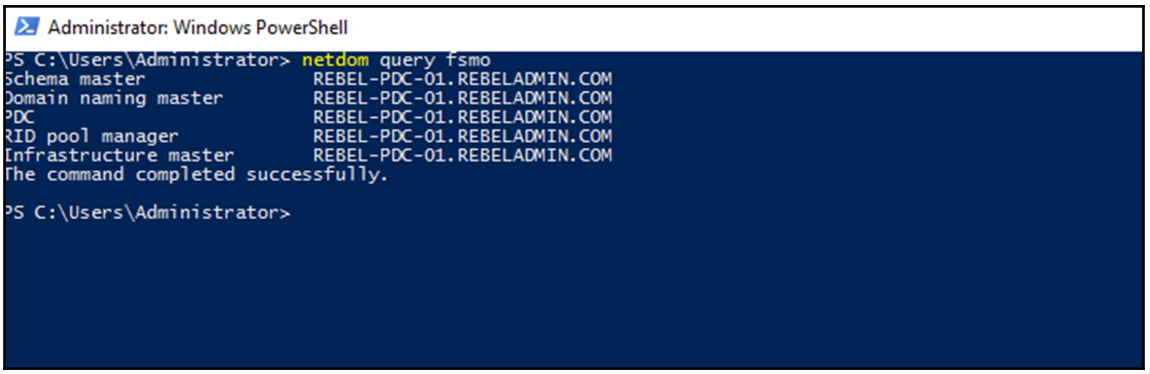

Administrator: Windows PowerShell
PS C:\Users\Administrator> netdom query fsmo
Schema master REBEL-PDC-01.REBELADMIN.COM
Domain naming master REBEL-PDC-01.REBELADMIN.COM
PDC REBEL-SDC02.REBELADMIN.COM
RID pool manager REBEL-SDC02.REBELADMIN.COM
Infrastructure master REBEL-SDC02.REBELADMIN.COM
The command completed successfully.
PS C:\Users\Administrator>


Administrator: Windows PowerShell
PS C:\Users\Administrator> Move-ADDirectoryServerOperationMasterRole -Identity REBEL-SDC02 -OperationMasterRole SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster, InfrastructureMaster
Move Operation Master Role
Do you want to move role 'SchemaMaster' to server 'REBEL-SDC02.REBELADMIN.COM' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A
PS C:\Users\Administrator>

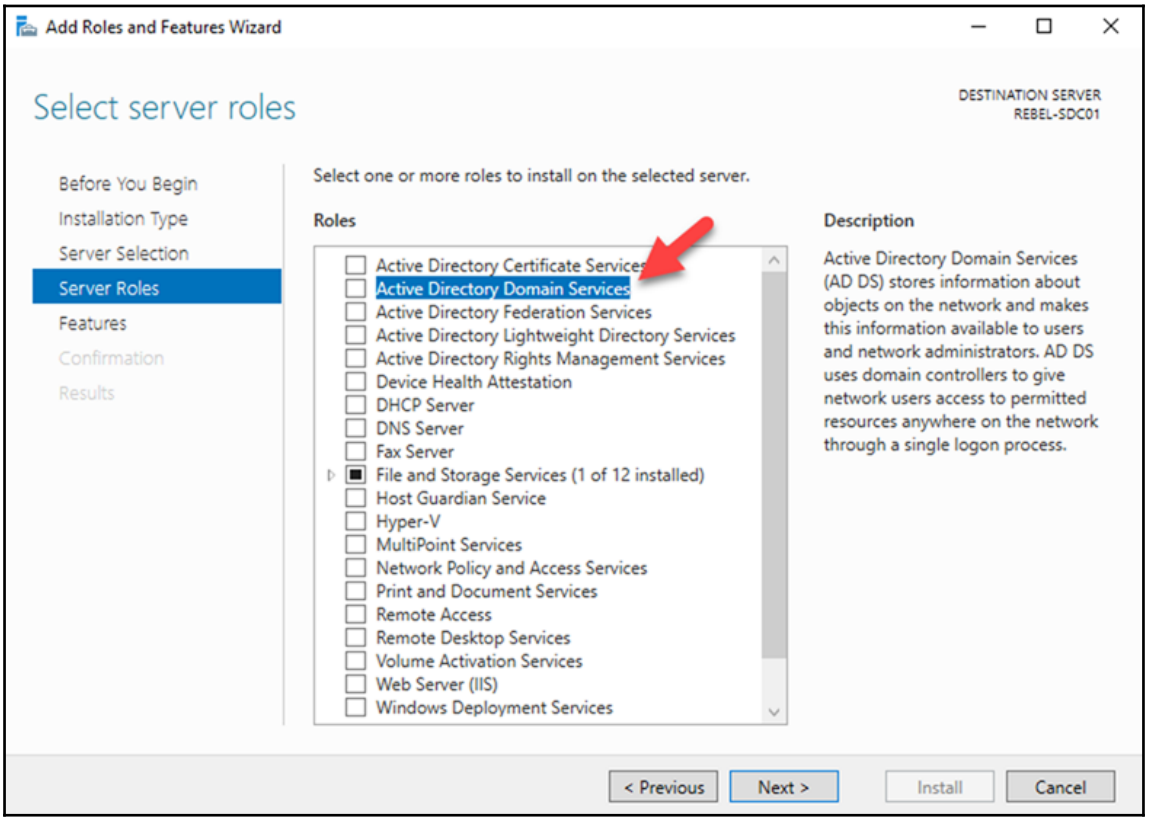

Administrator: Windows PowerShell
PS C:\Users\Administrator> netdom query fsmo
Schema master REBEL-SDC02.REBELADMIN.COM
Domain naming master REBEL-SDC02.REBELADMIN.COM
PDC REBEL-SDC02.REBELADMIN.COM
RID pool manager REBEL-SDC02.REBELADMIN.COM
Infrastructure master REBEL-SDC02.REBELADMIN.COM
The command completed successfully.
PS C:\Users\Administrator>

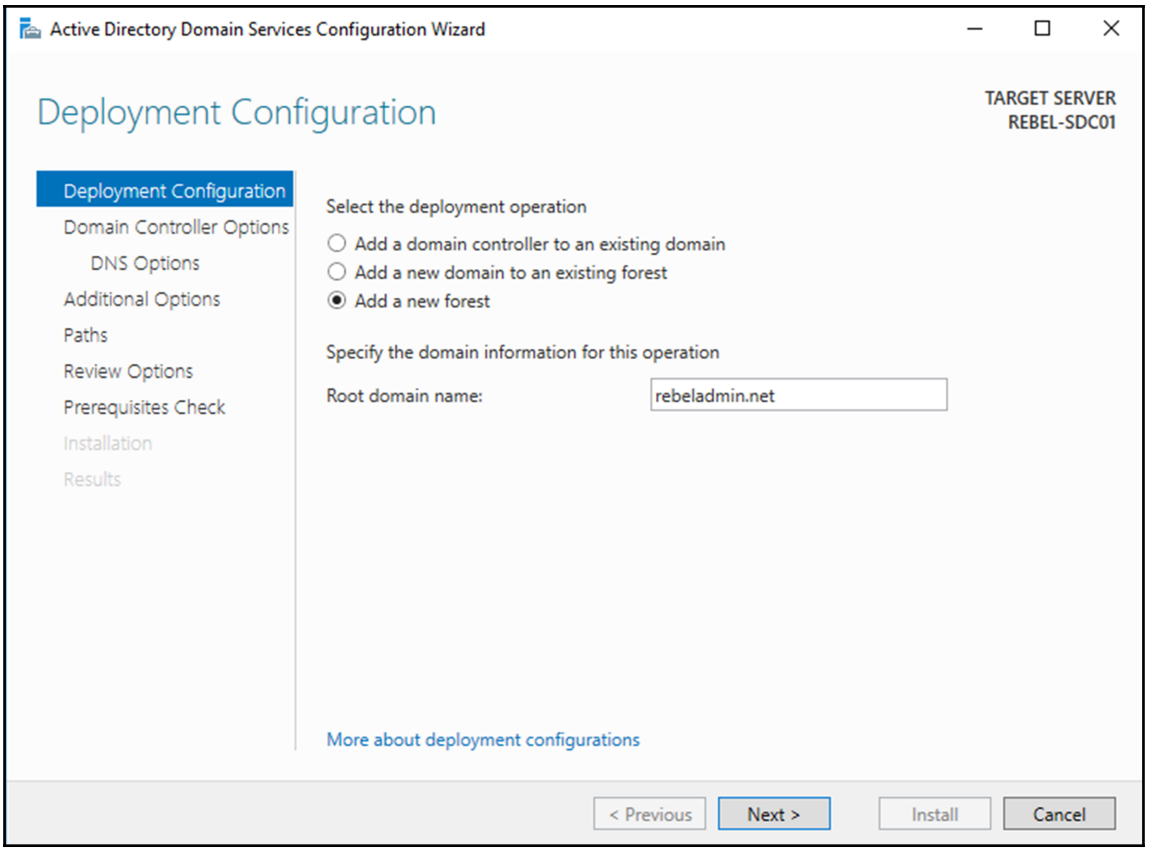

Administrator: Windows PowerShell
PS C:\Users\Administrator> netdom query fsmo
Schema master REBEL-SDC02.REBELADMIN.COM
Domain naming master REBEL-SDC02.REBELADMIN.COM
PDC REBEL-SDC02.REBELADMIN.COM
RID pool manager REBEL-SDC02.REBELADMIN.COM
Infrastructure master REBEL-SDC02.REBELADMIN.COM
The command completed successfully.
PS C:\Users\Administrator> ping REBEL-SDC02 -t
Pinging rebel-sdc02.rebeladmin.com [192.168.0.110] with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.0.105: Destination host unreachable.
Request timed out.
Request timed out.
Reply from 192.168.0.105: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.0.110:
Packets: Sent = 12, Received = 2, Lost = 10 (83% loss),
Control-C
PS C:\Users\Administrator>

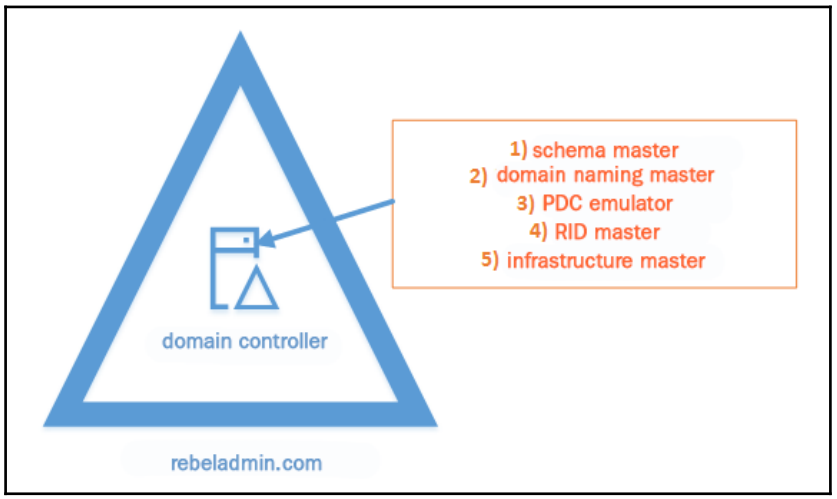

Administrator: Windows PowerShell
PS C:\Users\Administrator> Move-ADDirectoryServerOperationMasterRole -Identity REBEL-PDC-01 -OperationMasterRole SchemaM
aster, DomainNamingMaster, PDCEmulator, RIDMaster, InfrastructureMaster -Force
Move Operation Master Role
Do you want to move role 'SchemaMaster' to server 'REBEL-PDC-01.REBELADMIN.COM' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A
PS C:\Users\Administrator>

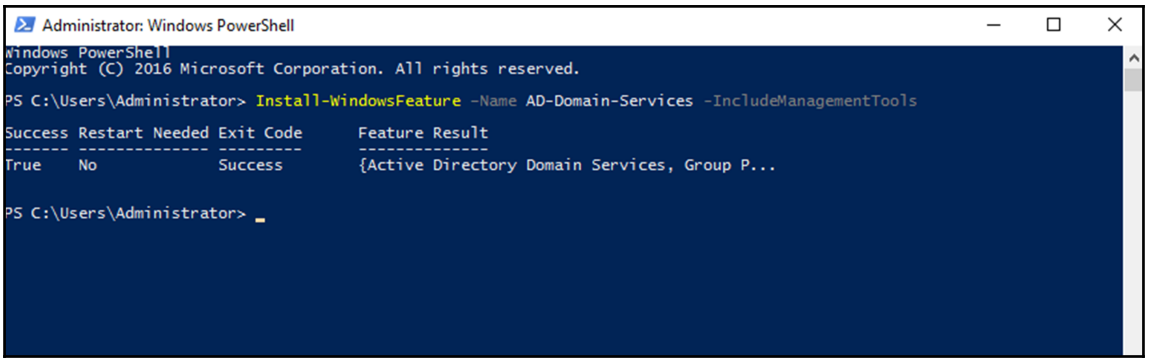

Administrator: Windows PowerShell
PS C:\Users\Administrator> netdom query fsmo
Schema master REBEL-PDC-01.REBELADMIN.COM
Domain naming master REBEL-PDC-01.REBELADMIN.COM
PDC REBEL-PDC-01.REBELADMIN.COM
RID pool manager REBEL-PDC-01.REBELADMIN.COM
Infrastructure master REBEL-PDC-01.REBELADMIN.COM
The command completed successfully.
PS C:\Users\Administrator>

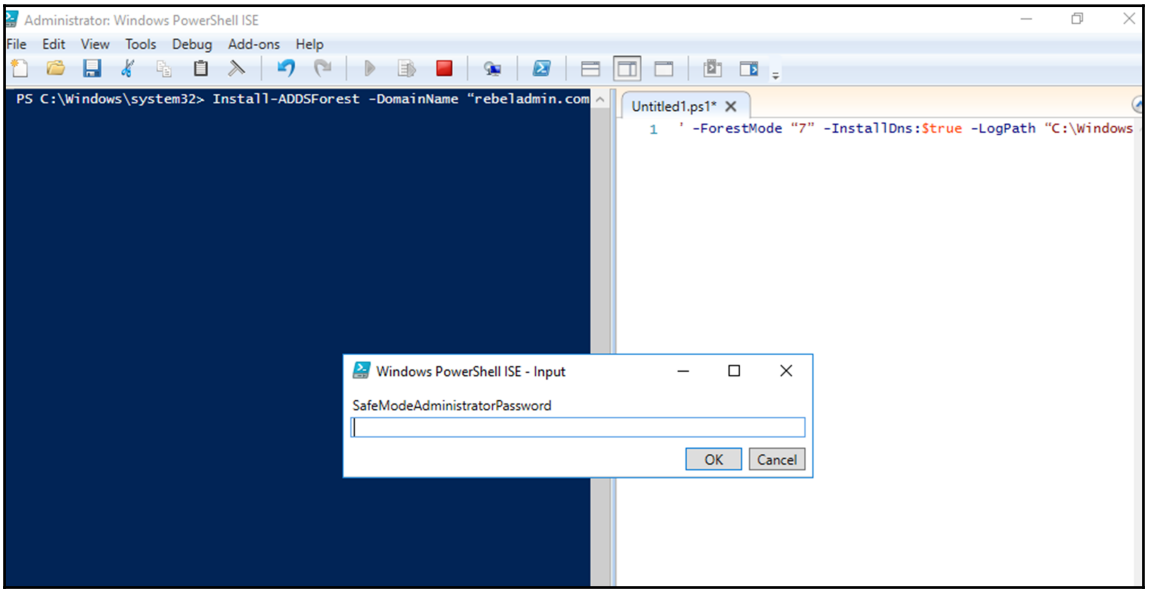
Chapter 6: Migrating to Active Directory 2016

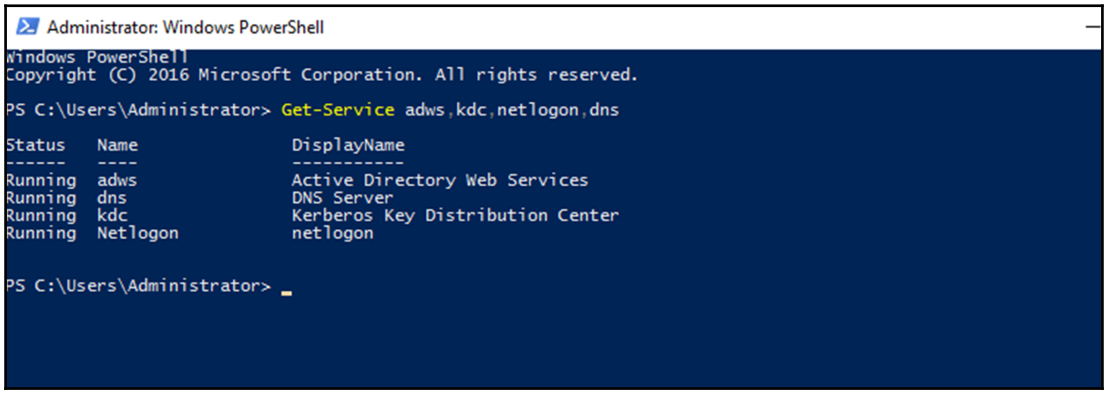


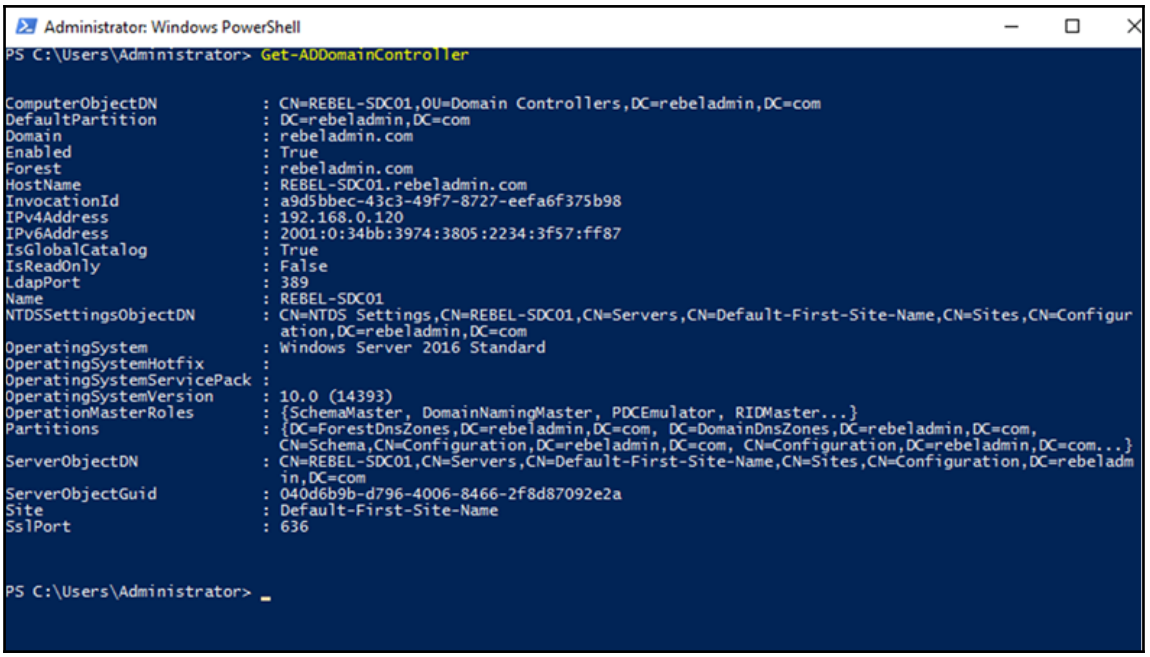

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
REBEL-SDC01
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
rebeladmin.net
More about deployment configurations
< Previous
Next >
Install
Cancel

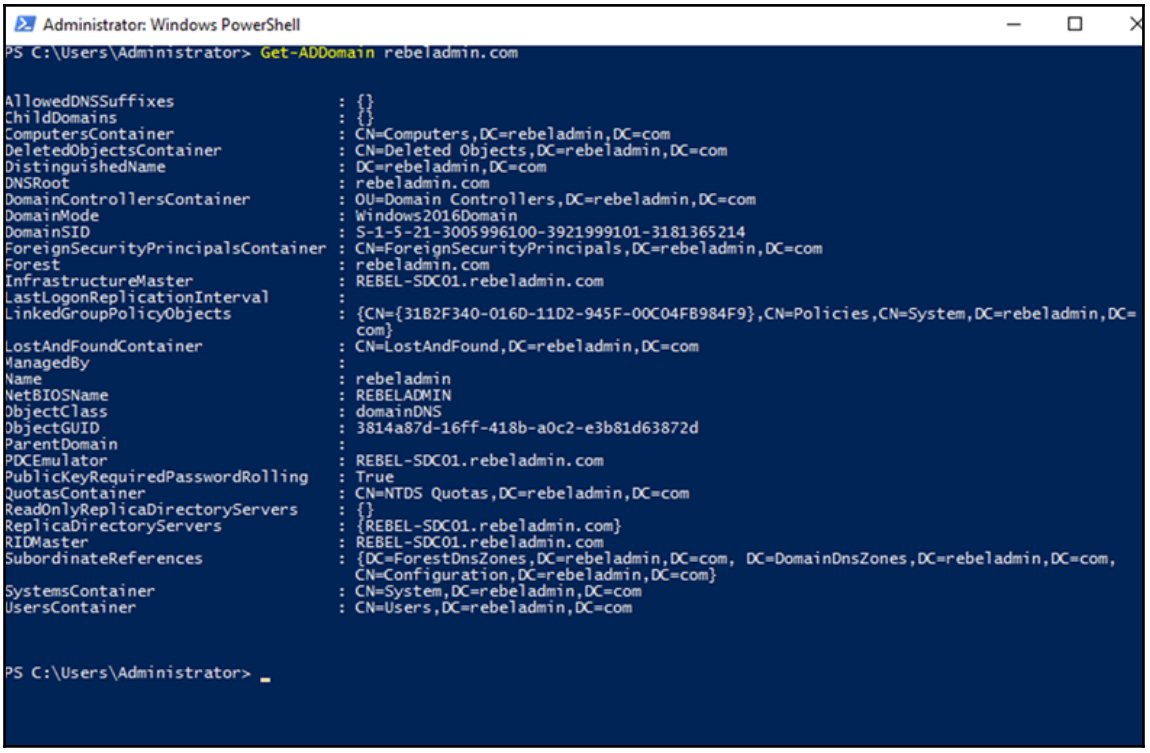

1) schema master
2) domain naming master
3) PDC emulator
4) RID master
5) infrastructure master
domain controller
rebeladmin.com

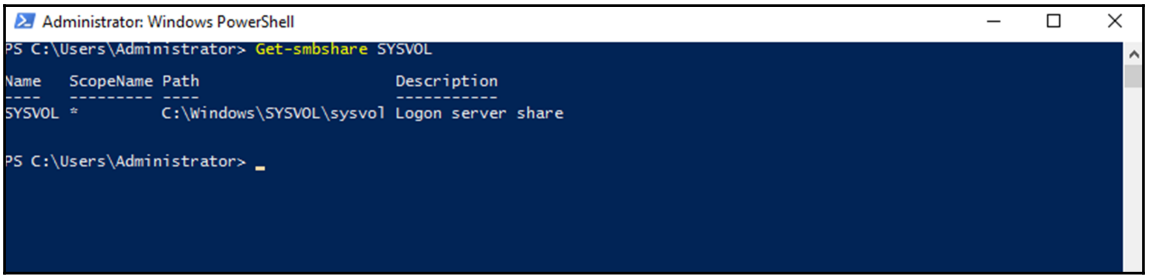

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
Success Restart Needed Exit Code Feature Result
True No Success {Active Directory Domain Services, Group P...
PS C:\Users\Administrator>

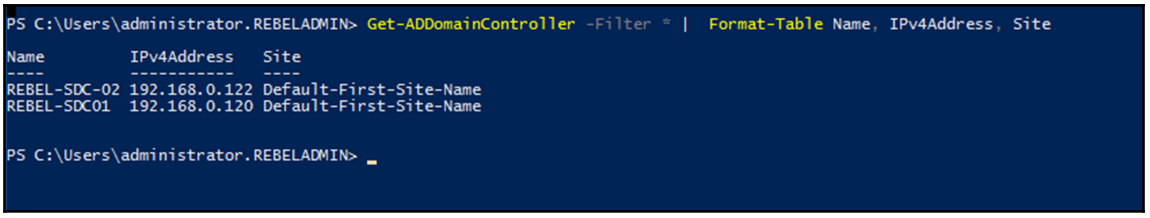

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\Windows\system32> Install-ADDSForest -DomainName "rebeladmin.com
Untitled1.ps1*
1 ' -ForestMode "7" -InstallDns:$true -LogPath "C:\Windows
Windows PowerShell ISE - Input
SafeModeAdministratorPassword
OK
Cancel


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> Get-Service adws,kdc,netlogon,dns
Status Name DisplayName
Running adws Active Directory Web Services
Running dns DNS Server
Running kdc Kerberos Key Distribution Center
Running Netlogon netlogon
PS C:\Users\Administrator>


Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADDomainController
ComputerObjectDN : CN=REBEL-SDC01,OU=Domain Controllers,DC=rebeladmin,DC=com
DefaultPartition : DC=rebeladmin,DC=com
Domain : rebeladmin.com
Enabled : True
Forest : rebeladmin.com
HostName : REBEL-SDC01.rebeladmin.com
InvocationId : a9d5bbec-43c3-49f7-8727-eefa6f375b98
IPv4Address : 192.168.0.120
IPv6Address : 2001:0:34bb:3974:3805:2234:3f57:ff87
IsGlobalCatalog : True
IsReadOnly : False
LdapPort : 389
Name : REBEL-SDC01
NTDSSettingsObjectDN : CN=NTDS Settings,CN=REBEL-SDC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
OperatingSystem : Windows Server 2016 Standard
OperatingSystemHotfix :
OperatingSystemServicePack :
OperatingSystemVersion : 10.0 (14393)
OperationMasterRoles : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}
Partitions : {DC=ForestDnsZones,DC=rebeladmin,DC=com, DC=DomainDnsZones,DC=rebeladmin,DC=com, CN=Schema,CN=Configuration,DC=rebeladmin,DC=com, CN=Configuration,DC=rebeladmin,DC=com...}
ServerObjectDN : CN=REBEL-SDC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
ServerObjectGuid : 040d6b9b-d796-4006-8466-2f8d87092e2a
Site : Default-First-Site-Name
SslPort : 636
PS C:\Users\Administrator>

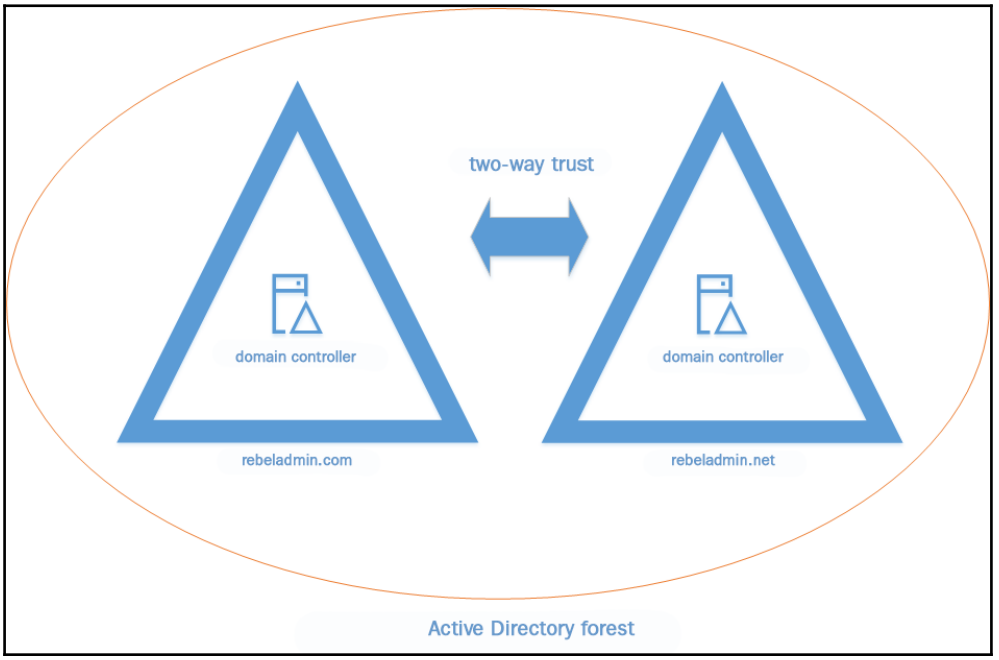

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADDomain rebeladmin.com
AllowedDNSSuffixes : {}
ChildDomains : {}
ComputersContainer : CN=Computers,DC=rebeladmin,DC=com
DeletedObjectsContainer : CN=Deleted Objects,DC=rebeladmin,DC=com
DistinguishedName : DC=rebeladmin,DC=com
DNSRoot : rebeladmin.com
DomainControllersContainer : OU=Domain Controllers,DC=rebeladmin,DC=com
DomainMode : Windows2016Domain
DomainSID : S-1-5-21-3005996100-3921999101-3181365214
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=rebeladmin,DC=com
Forest : rebeladmin.com
InfrastructureMaster : REBEL-SDC01.rebeladmin.com
LastLogonReplicationInterval :
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=rebeladmin,DC=com}
LostAndFoundContainer : CN=LostAndFound,DC=rebeladmin,DC=com
ManagedBy :
Name : rebeladmin
NetBIOSName : REBELADMIN
ObjectClass : domainDNS
ObjectGUID : 3814a87d-16ff-418b-a0c2-e3b81d63872d
ParentDomain :
PDCEmulator : REBEL-SDC01.rebeladmin.com
PublicKeyRequiredPasswordRolling : True
QuotasContainer : CN=NTDS Quotas,DC=rebeladmin,DC=com
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers : {REBEL-SDC01.rebeladmin.com}
RIDMaster : REBEL-SDC01.rebeladmin.com
SubordinateReferences : {DC=ForestDnsZones,DC=rebeladmin,DC=com, DC=DomainDnsZones,DC=rebeladmin,DC=com, CN=Configuration,DC=rebeladmin,DC=com}
SystemsContainer : CN=System,DC=rebeladmin,DC=com
UsersContainer : CN=Users,DC=rebeladmin,DC=com
PS C:\Users\Administrator>

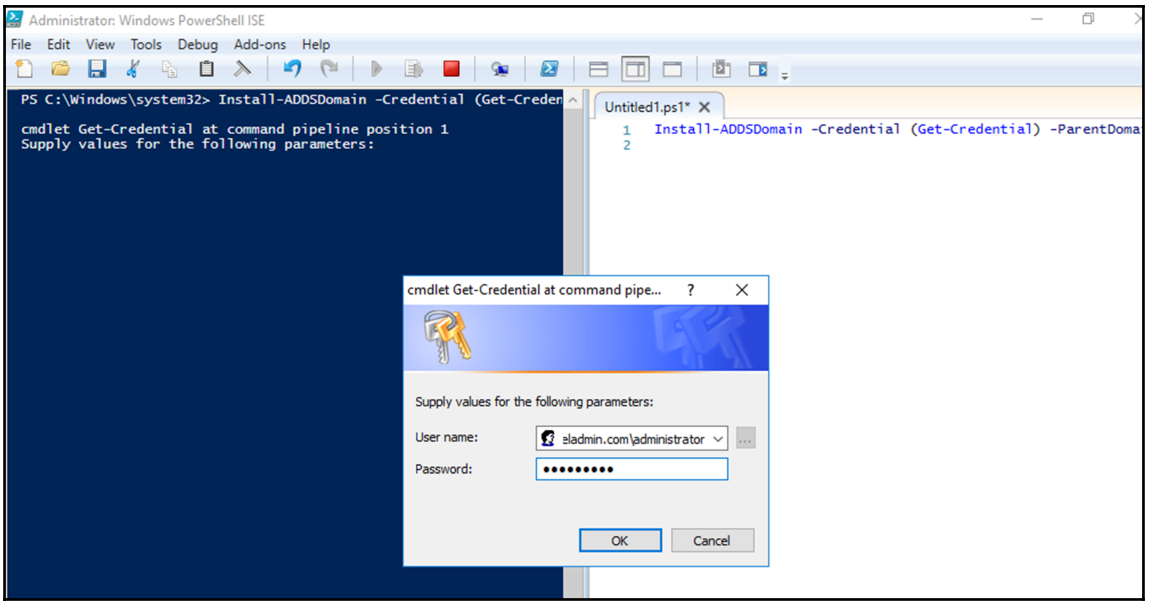

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-smbshare SYSVOL
Name ScopeName Path Description
SYSVOL * C:\Windows\SYSVOL\sysvol Logon server share
PS C:\Users\Administrator>

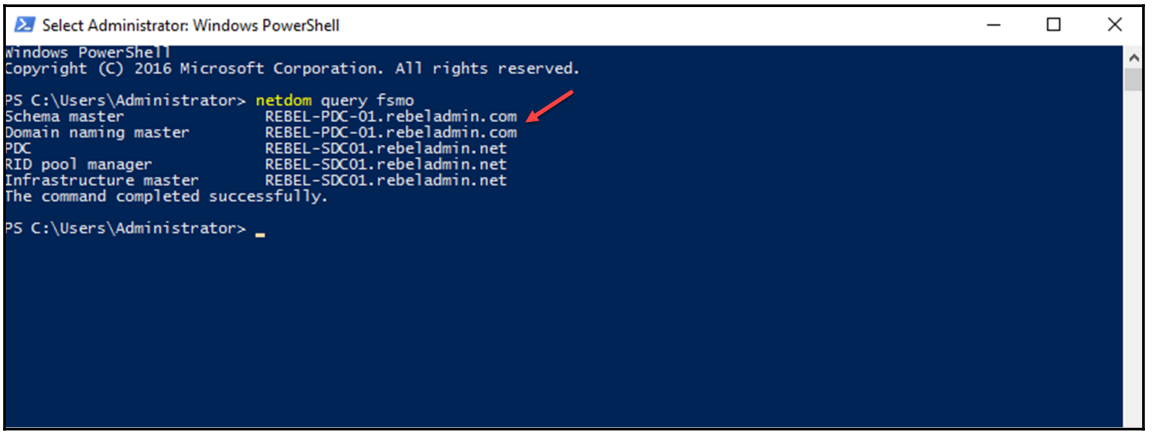

PS C:\Users\administrator.REBELADMIN> Get-ADDomainController -Filter * | Format-Table Name, IPv4Address, Site
Name IPv4Address Site
REBEL-SDC-02 192.168.0.122 Default-First-Site-Name
REBEL-SDC01 192.168.0.120 Default-First-Site-Name
PS C:\Users\administrator.REBELADMIN>

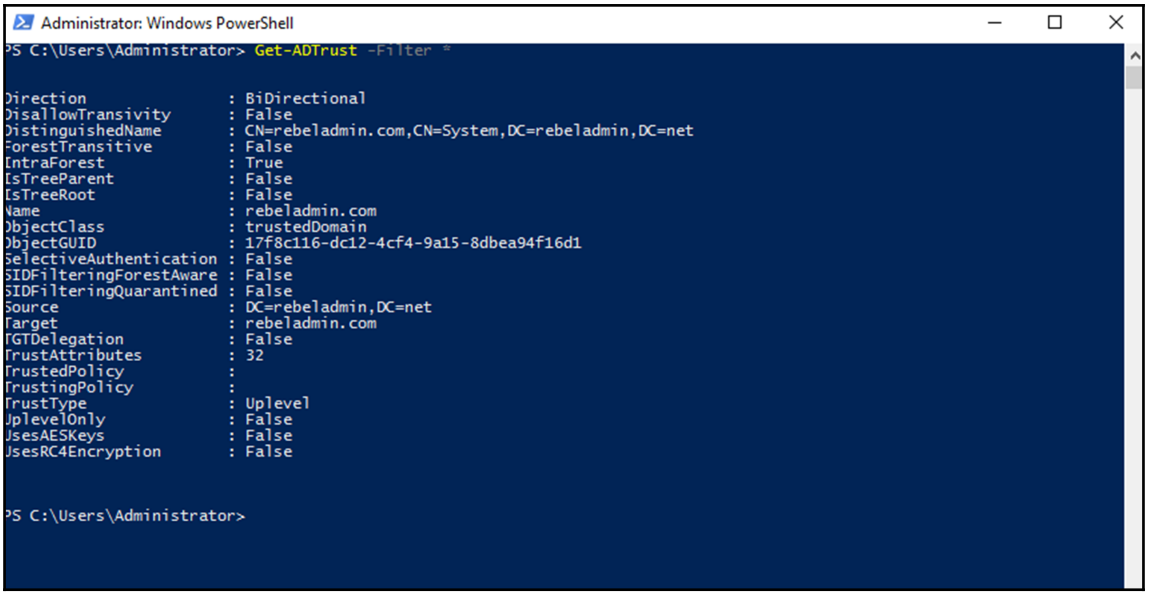
```
Administrator: Windows PowerShell
PS C:\Users\administrator.REBELADMIN> Get-ADDomainController -Discover -Service "GlobalCatalog"

Domain      : rebeladmin.com
Forest      : rebeladmin.com
HostName    : {REBEL-SDC01.rebeladmin.com}
IPv4Address : 192.168.0.120
IPv6Address :
Name        : REBEL-SDC01
Site        : Default-First-Site-Name


PS C:\Users\administrator.REBELADMIN>
```

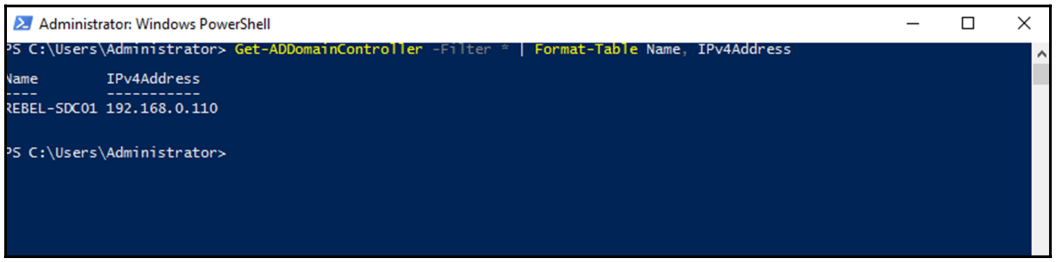
```
PS C:\Users\administrator.REBELADMIN> netdom query fsmo
Schema master               REBEL-SDC01.rebeladmin.com
Domain naming master        REBEL-SDC01.rebeladmin.com
PDC                         REBEL-SDC01.rebeladmin.com
RID pool manager            REBEL-SDC01.rebeladmin.com
Infrastructure master       REBEL-SDC-02.rebeladmin.com
The command completed successfully.

PS C:\Users\administrator.REBELADMIN>
```

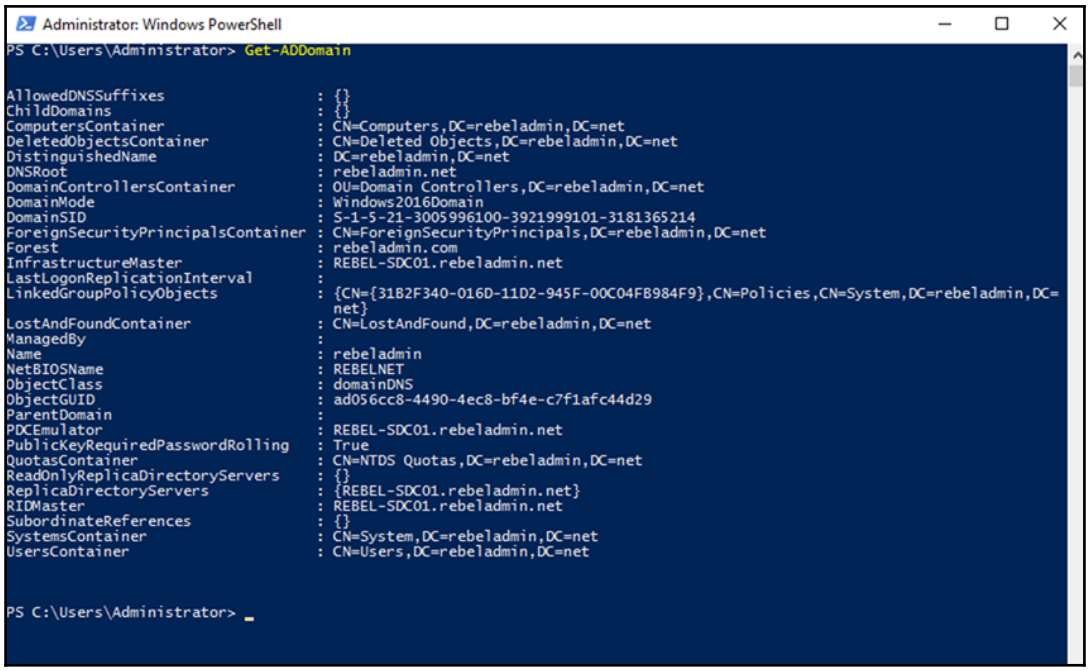


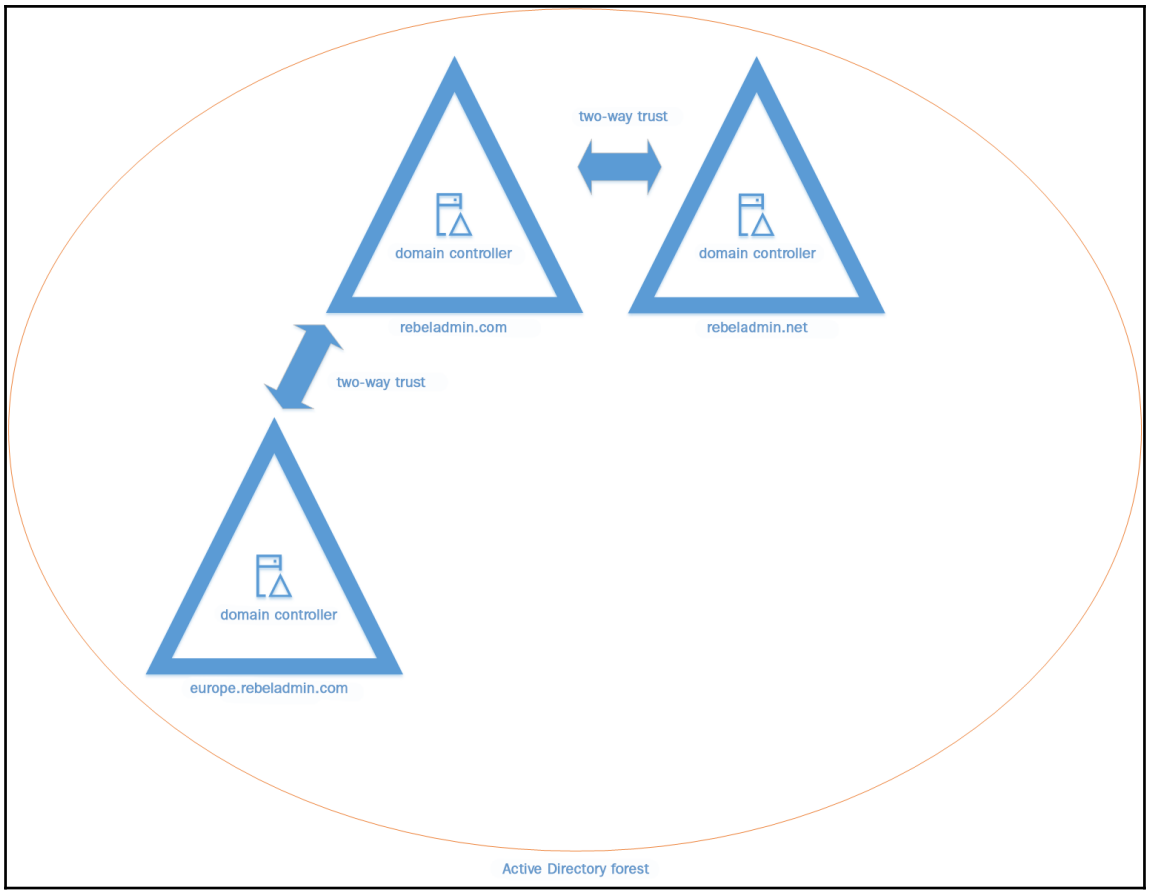

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\Windows\system32> Install-ADDSDomain -Credential (Get-Creden
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Untitled1.ps1*
1 Install-ADDSDomain -Credential (Get-Credential) -ParentDoma
2
cmdlet Get-Credential at command pipe...
Supply values for the following parameters:
User name:
sladmin.com\administrator
Password:
OK
Cancel

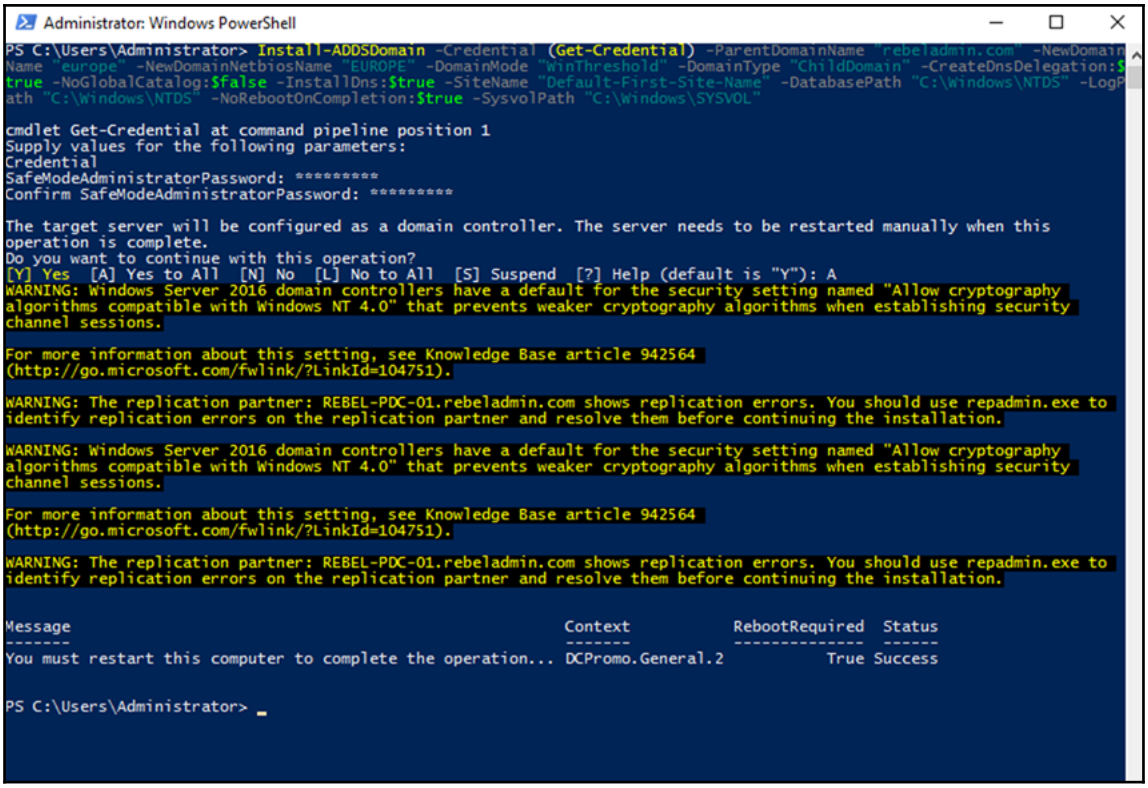

Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> netdom query fsmo
Schema master REBEL-PDC-01.rebeladmin.com
Domain naming master REBEL-PDC-01.rebeladmin.com
PDC REBEL-SDC01.rebeladmin.net
RID pool manager REBEL-SDC01.rebeladmin.net
Infrastructure master REBEL-SDC01.rebeladmin.net
The command completed successfully.
PS C:\Users\Administrator>

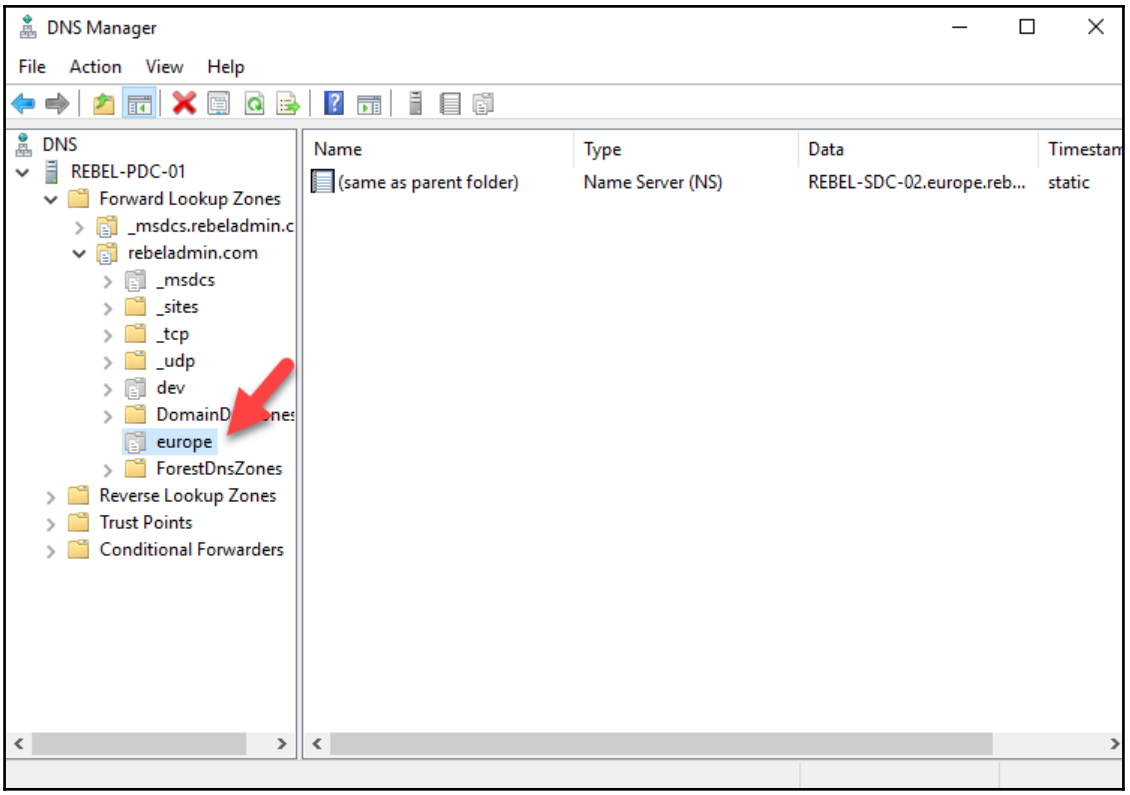

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADTrust -Filter *
Direction : BiDirectional
DisallowTransivity : False
DistinguishedName : CN=rebeladmin.com,CN=System,DC=rebeladmin,DC=net
ForestTransitive : False
IntraForest : True
IsTreeParent : False
IsTreeRoot : False
Name : rebeladmin.com
ObjectClass : trustedDomain
ObjectGUID : 17f8c116-dc12-4cf4-9a15-8dbea94f16d1
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
Source : DC=rebeladmin,DC=net
Target : rebeladmin.com
TGTDelegation : False
TrustAttributes : 32
TrustedPolicy :
TrustingPolicy :
TrustType : Uplevel
UplevelOnly : False
UsesAESKeys : False
UsesRC4Encryption : False
PS C:\Users\Administrator>

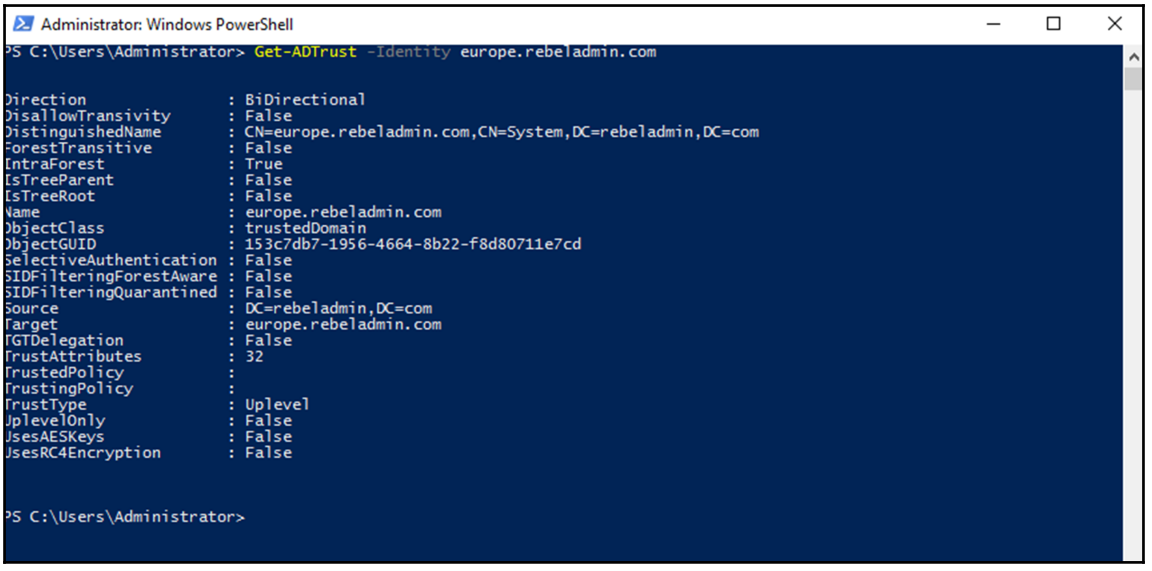

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADDomainController -Filter * | Format-Table Name, IPv4Address
Name IPv4Address
REBEL-SDC01 192.168.0.110
PS C:\Users\Administrator>

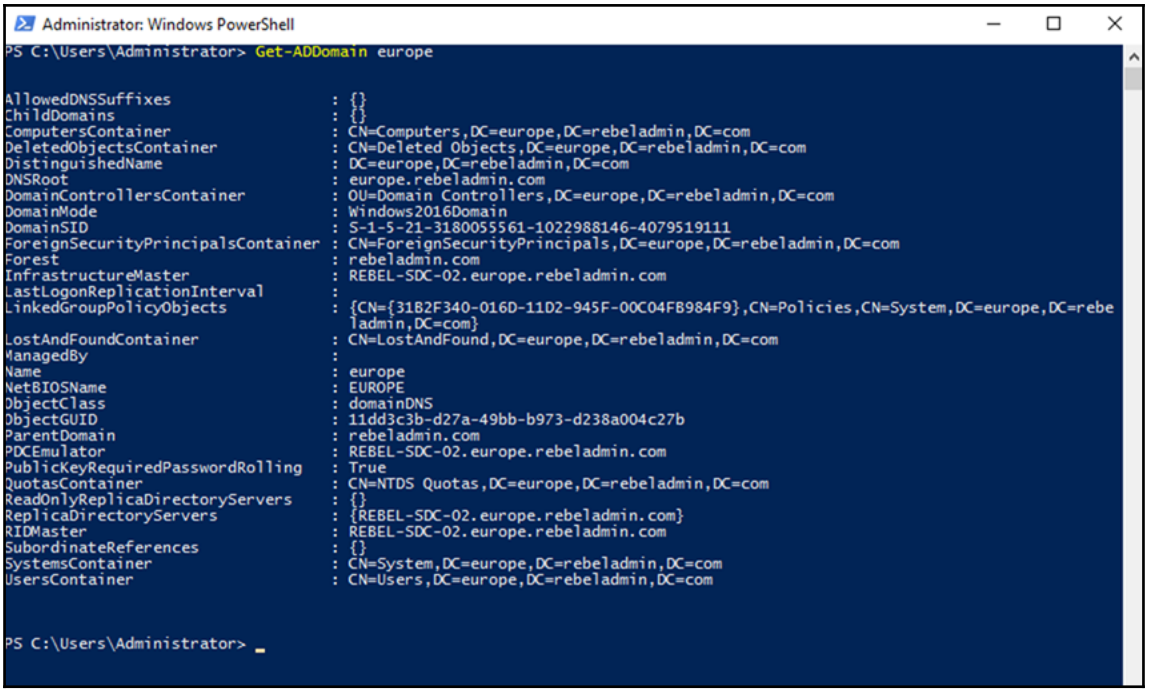

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADDomain
AllowedDNSSuffixes : {}
ChildDomains : {}
ComputersContainer : CN=Computers,DC=rebeladmin,DC=net
DeletedObjectsContainer : CN=Deleted Objects,DC=rebeladmin,DC=net
DistinguishedName : DC=rebeladmin,DC=net
DNSRoot : rebeladmin.net
DomainControllersContainer : OU=Domain Controllers,DC=rebeladmin,DC=net
DomainMode : Windows2016Domain
DomainSID : S-1-5-21-3005996100-3921999101-3181365214
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=rebeladmin,DC=net
Forest : rebeladmin.com
InfrastructureMaster : REBEL-SDC01.rebeladmin.net
LastLogonReplicationInterval :
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=rebeladmin,DC=net}
LostAndFoundContainer : CN=LostAndFound,DC=rebeladmin,DC=net
ManagedBy :
Name : rebeladmin
NetBIOSName : REBELNET
ObjectClass : domainDNS
ObjectGUID : ad056cc8-4490-4ec8-bf4e-c7f1afc44d29
ParentDomain :
PDCEmulator : REBEL-SDC01.rebeladmin.net
PublicKeyRequiredPasswordRolling : True
QuotasContainer : CN=NTDS Quotas,DC=rebeladmin,DC=net
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers : {REBEL-SDC01.rebeladmin.net}
RIDMaster : REBEL-SDC01.rebeladmin.net
SubordinateReferences : {}
SystemsContainer : CN=System,DC=rebeladmin,DC=net
UsersContainer : CN=Users,DC=rebeladmin,DC=net
PS C:\Users\Administrator>

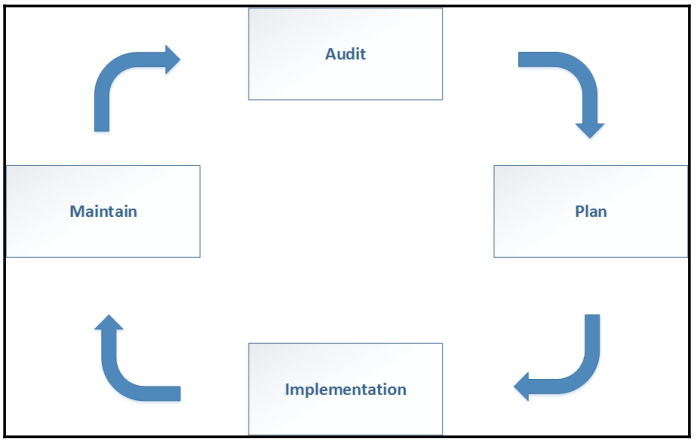

two-way trust
domain controller
rebeladmin.com
domain controller
rebeladmin.net
two-way trust
domain controller
europe.rebeladmin.com
Active Directory forest


Administrator: Windows PowerShell
PS C:\Users\Administrator> Install-ADDSDomain -Credential (Get-Credential) -ParentDomainName "rebeladmin.com" -NewDomainName "europe" -NewDomainNetbiosName "EUROPE" -DomainMode "WinThreshold" -DomainType "ChildDomain" -CreateDnsDelegation:$true -NoGlobalCatalog:$false -InstallDns:$true -SiteName "Default-First-Site-Name" -DatabasePath "C:\Windows\NTDS" -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:$true -SysvolPath "C:\Windows\SYSVOL"
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
SafeModeAdministratorPassword: ********
Confirm SafeModeAdministratorPassword: ********
The target server will be configured as a domain controller. The server needs to be restarted manually when this operation is complete.
Do you want to continue with this operation?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A
WARNING: Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
WARNING: The replication partner: REBEL-PDC-01.rebeladmin.com shows replication errors. You should use repadmin.exe to identify replication errors on the replication partner and resolve them before continuing the installation.
WARNING: Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
WARNING: The replication partner: REBEL-PDC-01.rebeladmin.com shows replication errors. You should use repadmin.exe to identify replication errors on the replication partner and resolve them before continuing the installation.
Message Context RebootRequired Status
You must restart this computer to complete the operation... DCPromo.General.2 True Success
PS C:\Users\Administrator>

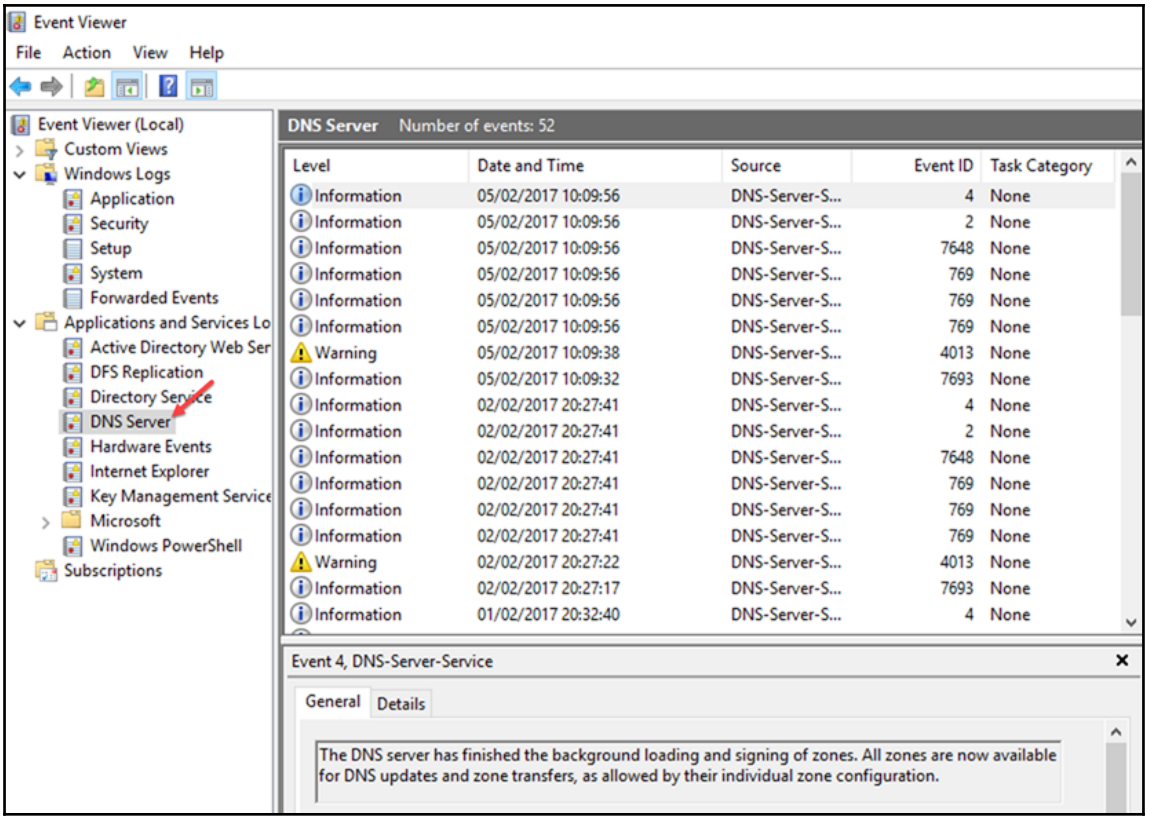

DNS Manager
File Action View Help
DNS
REBEL-PDC-01
Forward Lookup Zones
_msdcs.rebeladmin.c
rebeladmin.com
_msdcs
_sites
_tcp
_udp
dev
europe
ForestDnsZones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name
Type
Data
Timestam
(same as parent folder)
Name Server (NS)
REBEL-SDC-02.europe.reb...
static

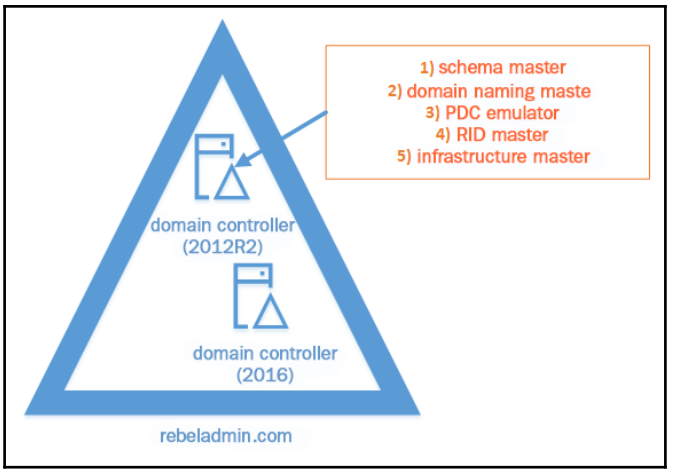

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADTrust -Identity europe.rebeladmin.com
Direction : BiDirectional
DisallowTransivity : False
DistinguishedName : CN=europe.rebeladmin.com,CN=System,DC=rebeladmin,DC=com
ForestTransitive : False
IntraForest : True
IsTreeParent : False
IsTreeRoot : False
Name : europe.rebeladmin.com
ObjectClass : trustedDomain
ObjectGUID : 153c7db7-1956-4664-8b22-f8d80711e7cd
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
Source : DC=rebeladmin,DC=com
Target : europe.rebeladmin.com
TGTDelegation : False
TrustAttributes : 32
TrustedPolicy :
TrustingPolicy :
TrustType : Uplevel
UplevelOnly : False
UsesAESKeys : False
UsesRC4Encryption : False
PS C:\Users\Administrator>

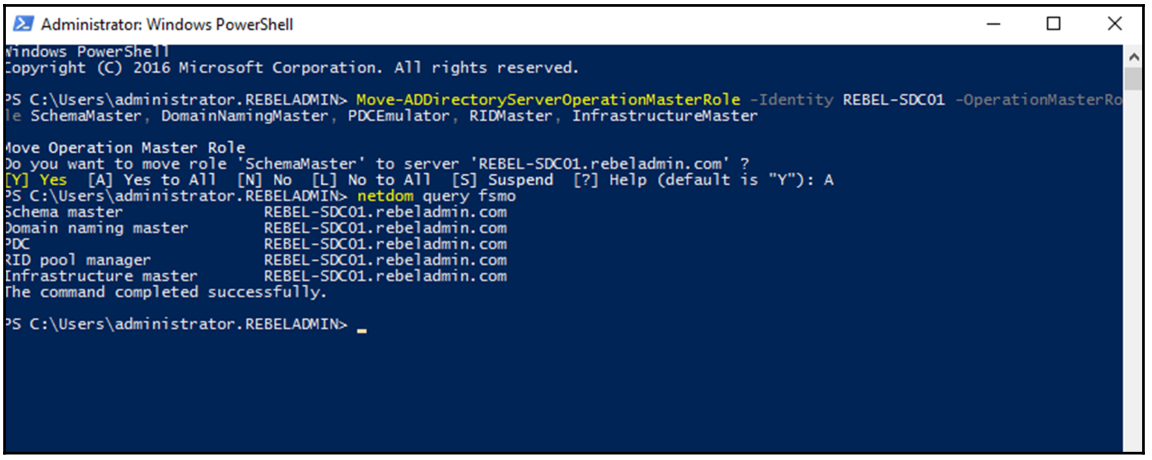

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADDomain europe
AllowedDNSSuffixes : {}
ChildDomains : {}
ComputersContainer : CN=Computers,DC=europe,DC=rebeladmin,DC=com
DeletedObjectsContainer : CN=Deleted Objects,DC=europe,DC=rebeladmin,DC=com
DistinguishedName : DC=europe,DC=rebeladmin,DC=com
DNSRoot : europe.rebeladmin.com
DomainControllersContainer : OU=Domain Controllers,DC=europe,DC=rebeladmin,DC=com
DomainMode : Windows2016Domain
DomainSID : S-1-5-21-3180055561-1022988146-4079519111
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=europe,DC=rebeladmin,DC=com
Forest : rebeladmin.com
InfrastructureMaster : REBEL-SDC-02.europe.rebeladmin.com
LastLogonReplicationInterval :
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=europe,DC=rebeladmin,DC=com}
LostAndFoundContainer : CN=LostAndFound,DC=europe,DC=rebeladmin,DC=com
ManagedBy :
Name : europe
NetBIOSName : EUROPE
ObjectClass : domainDNS
ObjectGUID : 11dd3c3b-d27a-49bb-b973-d238a004c27b
ParentDomain : rebeladmin.com
PDCEmulator : REBEL-SDC-02.europe.rebeladmin.com
PublicKeyRequiredPasswordRolling : True
QuotasContainer : CN=NTDS Quotas,DC=europe,DC=rebeladmin,DC=com
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers : {REBEL-SDC-02.europe.rebeladmin.com}
RIDMaster : REBEL-SDC-02.europe.rebeladmin.com
SubordinateReferences : {}
SystemsContainer : CN=System,DC=europe,DC=rebeladmin,DC=com
UsersContainer : CN=Users,DC=europe,DC=rebeladmin,DC=com
PS C:\Users\Administrator>

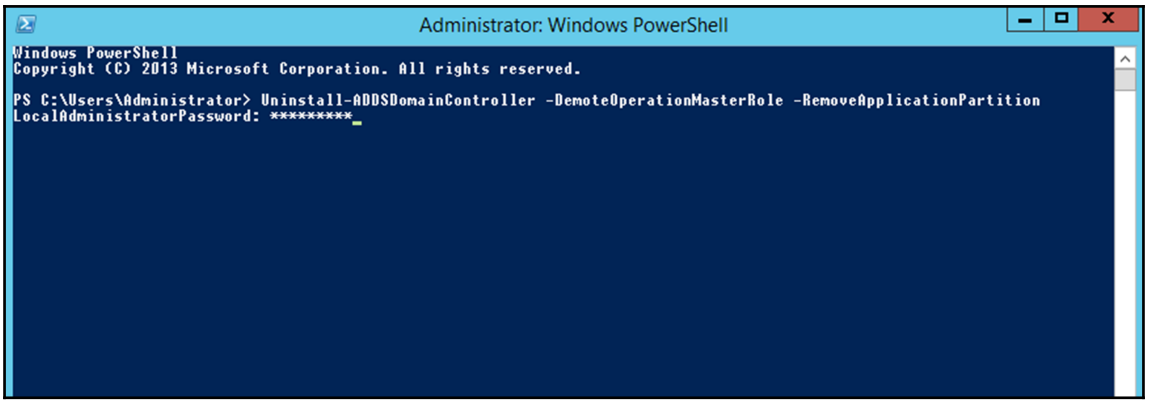

Audit
Plan
Implementation
Maintain

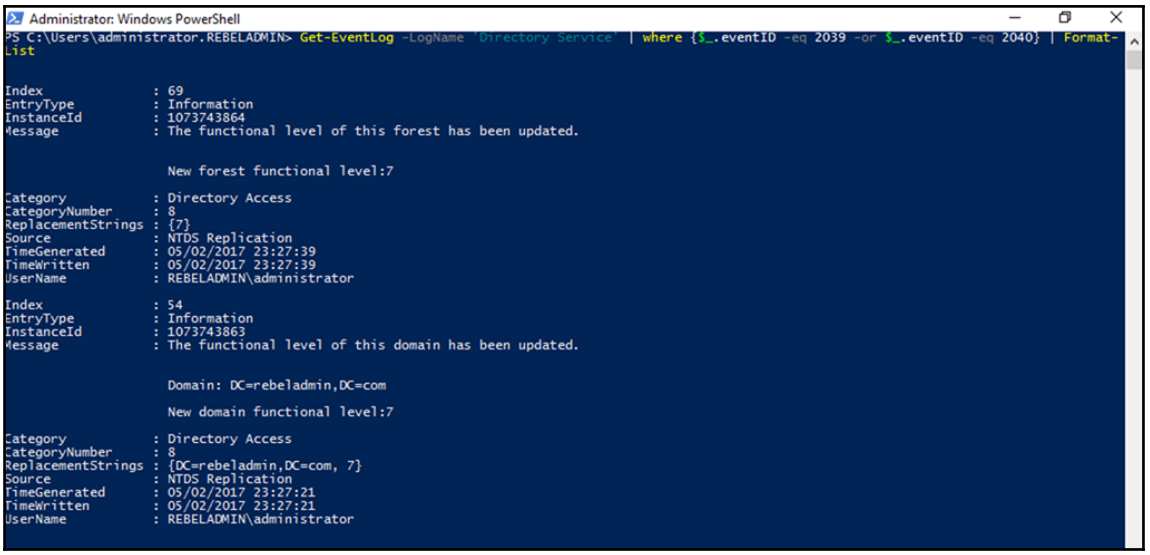
```
PS C:\Users\Administrator> repadmin /replsummary
Replication Summary Start Time: 2017-02-05 14:53:08

Beginning data collection for replication summary, this may take awhile:
  .......


Source DSA          largest delta    fails/total %%   error
 REBEL-PDC-01               54m:10s    0 /   6    0
 REBEL-SDC-02      02d.15h:05m:56s    4 /   4  100  (1908) Could not find the domain controller for this domain.
 REBEL-SDC-03               58m:42s    0 /   6    0


Destination DSA     largest delta    fails/total %%   error
 REBEL-PDC-01      02d.15h:05m:56s    4 /  10   40  (1908) Could not find the domain controller for this domain.
 REBEL-SDC-03               54m:10s    0 /   6    0


Experienced the following operational errors trying to retrieve replication information:
          58 - 9a145fff-4ea2-4595-ba37-1df8ddaf98ba._msdcs.rebeladmin.com
        8341 - REBEL-SDC-02.europe.rebeladmin.com
PS C:\Users\Administrator>
```



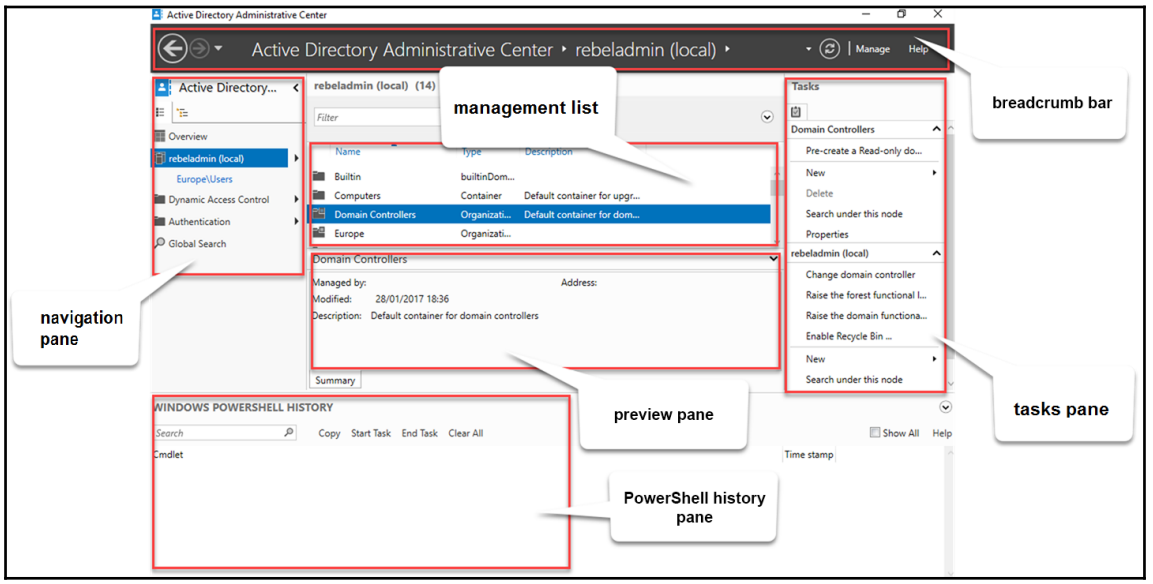

1) schema master
2) domain naming maste
3) PDC emulator
4) RID master
5) infrastructure master
domain controller
(2012R2)
domain controller
(2016)
rebeladmin.com

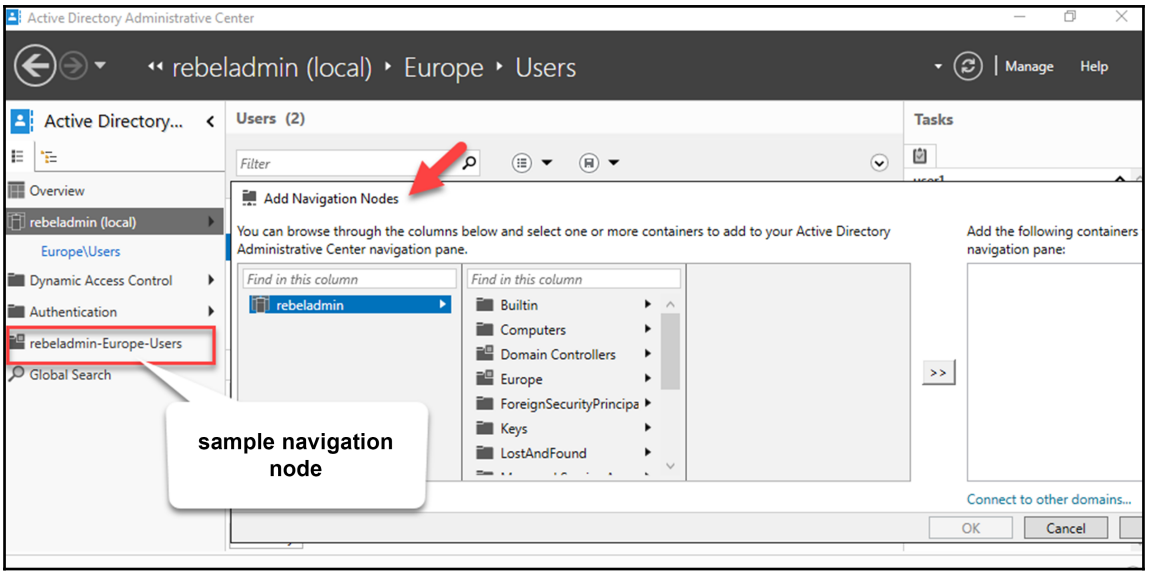

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\administrator.REBELADMIN> Move-ADDirectoryServerOperationMasterRole -Identity REBEL-SDC01 -OperationMasterRo
le SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster, InfrastructureMaster
Move Operation Master Role
Do you want to move role 'SchemaMaster' to server 'REBEL-SDC01.rebeladmin.com' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A
PS C:\Users\administrator.REBELADMIN> netdom query fsmo
Schema master REBEL-SDC01.rebeladmin.com
Domain naming master REBEL-SDC01.rebeladmin.com
PDC REBEL-SDC01.rebeladmin.com
RID pool manager REBEL-SDC01.rebeladmin.com
Infrastructure master REBEL-SDC01.rebeladmin.com
The command completed successfully.
PS C:\Users\administrator.REBELADMIN>

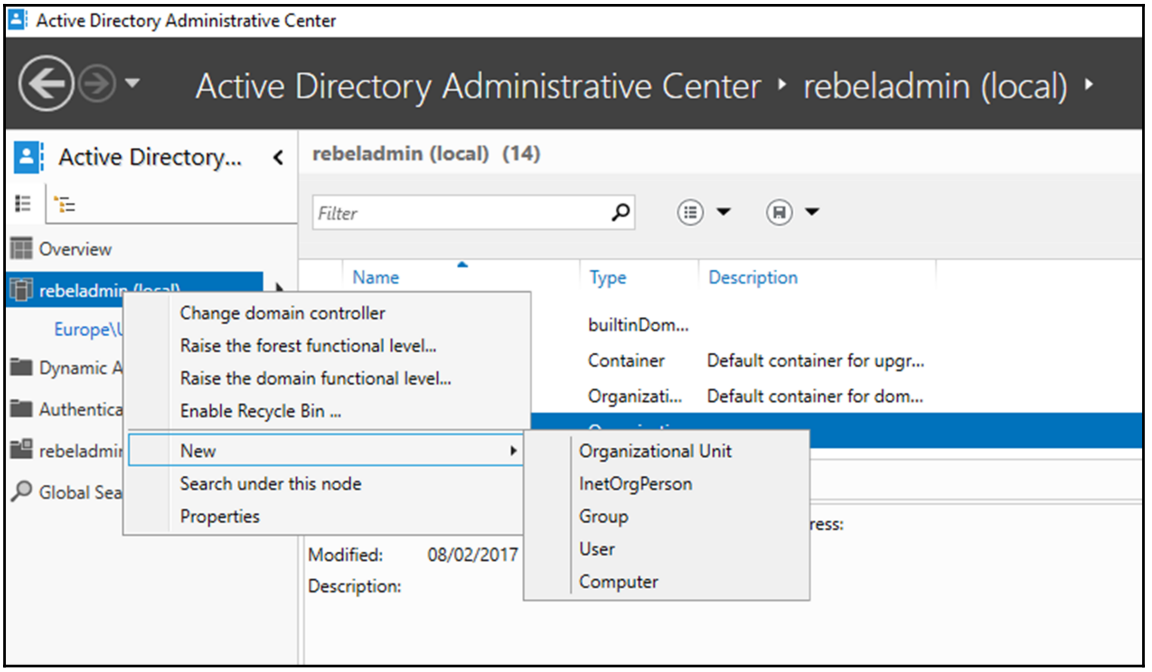

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> Uninstall-ADDSDomainController -DemoteOperationMasterRole -RemoveApplicationPartition
LocalAdministratorPassword: *********

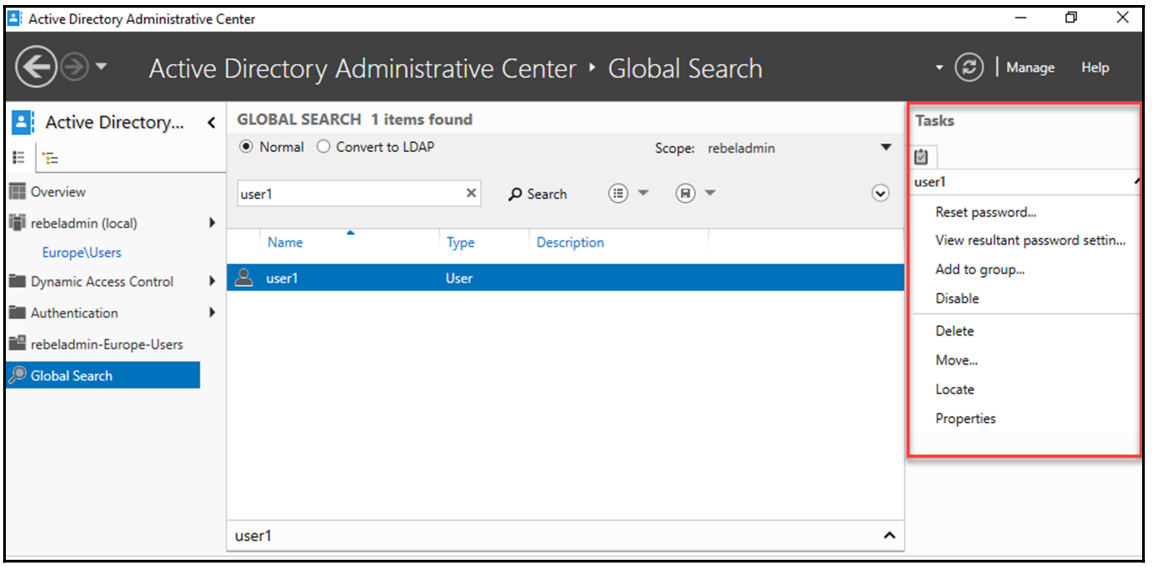

Administrator: Windows PowerShell
PS C:\Users\administrator.REBELADMIN> Get-EventLog -LogName 'Directory Service' | where {$_.eventID -eq 2039 -or $_.eventID -eq 2040} | Format-List
Index : 69
EntryType : Information
InstanceId : 1073743864
Message : The functional level of this forest has been updated.
New forest functional level:7
Category : Directory Access
CategoryNumber : 8
ReplacementStrings : {7}
Source : NTDS Replication
TimeGenerated : 05/02/2017 23:27:39
TimeWritten : 05/02/2017 23:27:39
UserName : REBELADMIN\administrator
Index : 54
EntryType : Information
InstanceId : 1073743863
Message : The functional level of this domain has been updated.
Domain: DC=rebeladmin,DC=com
New domain functional level:7
Category : Directory Access
CategoryNumber : 8
ReplacementStrings : {DC=rebeladmin,DC=com, 7}
Source : NTDS Replication
TimeGenerated : 05/02/2017 23:27:21
TimeWritten : 05/02/2017 23:27:21
UserName : REBELADMIN\administrator

Chapter 7: Managing Active Directory Objects

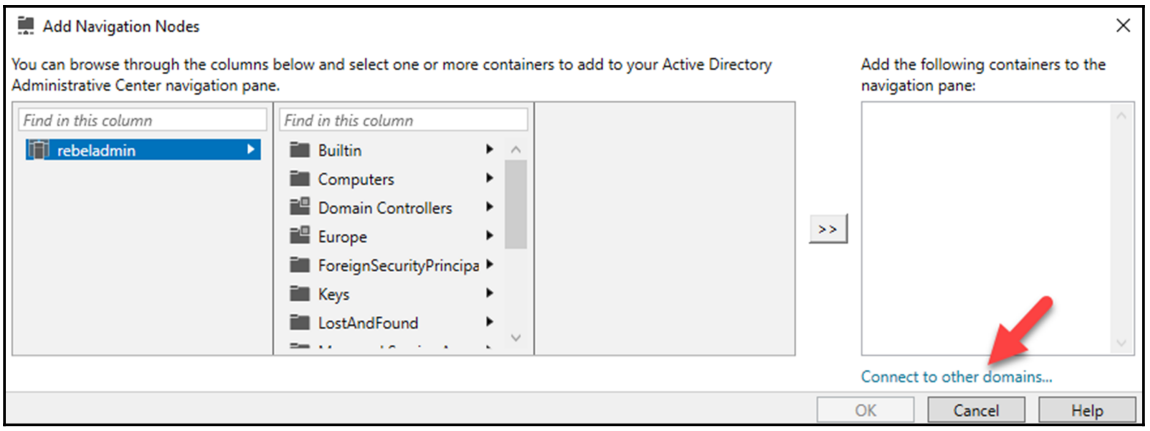


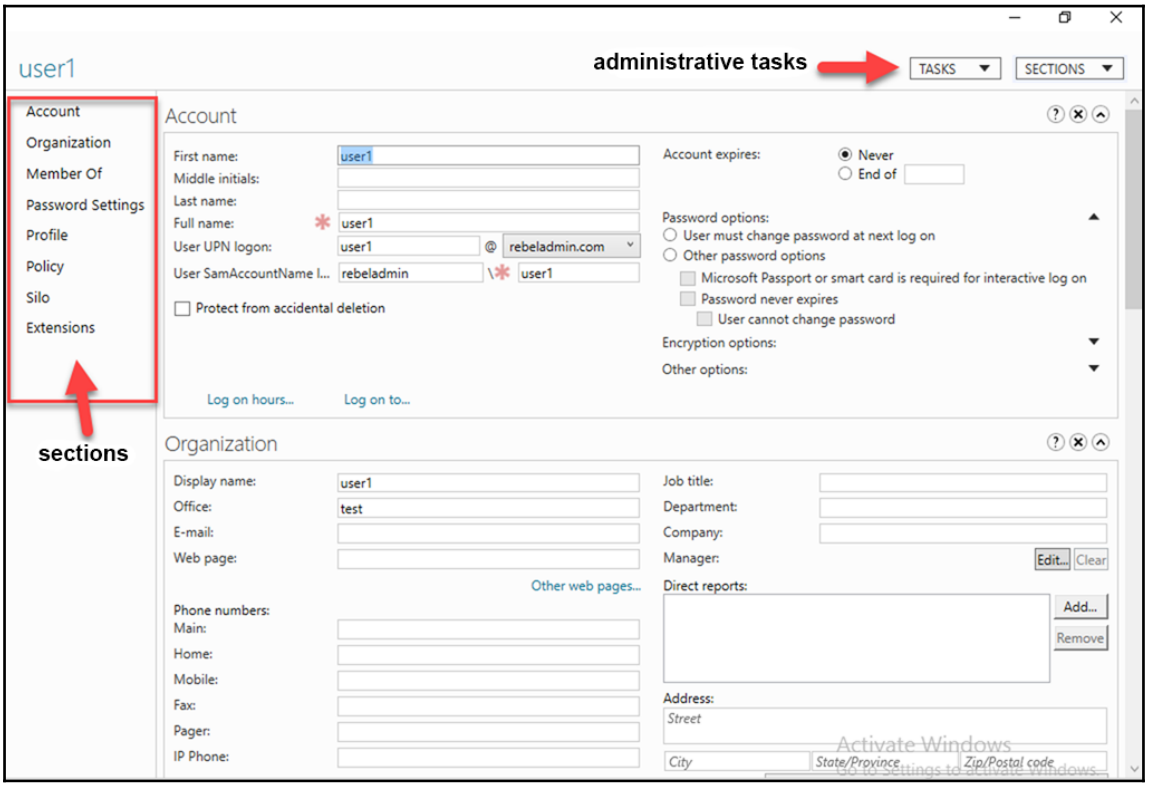

Active Directory Administrative Center
rebeladmin (local) ▸ Europe ▸ Users
Manage
Help
Active Directory...
Users (2)
Tasks
Filter
Overview
rebeladmin (local)
Europe\Users
Dynamic Access Control
Authentication
rebeladmin-Europe-Users
Global Search
Add Navigation Nodes
You can browse through the columns below and select one or more containers to add to your Active Directory Administrative Center navigation pane.
Add the following containers navigation pane:
Find in this column
rebeladmin
Builtin
Computers
Domain Controllers
Europe
ForeignSecurityPrincipa
Keys
LostAndFound
>>
Connect to other domains...
OK
Cancel
sample navigation node

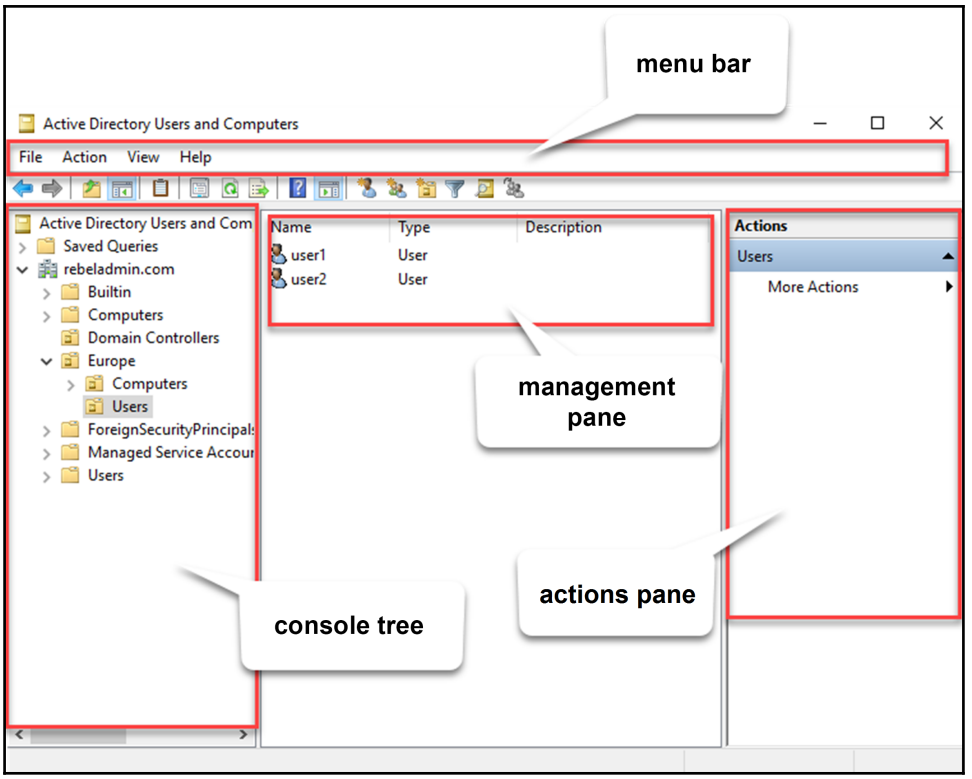

Active Directory Administrative Center
Active Directory Administrative Center ▸ rebeladmin (local) ▸
Active Directory...
rebeladmin (local) (14)
Filter
Overview
rebeladmin (local)
Europe\U
Dynamic A
Authentica
rebeladmi
Global Sea
Name
Type
Description
builtinDom...
Container
Default container for upgr...
Organizati...
Default container for dom...
Change domain controller
Raise the forest functional level...
Raise the domain functional level...
Enable Recycle Bin ...
New
Search under this node
Properties
Organizational Unit
InetOrgPerson
Group
User
Computer
Modified: 08/02/2017
Description:

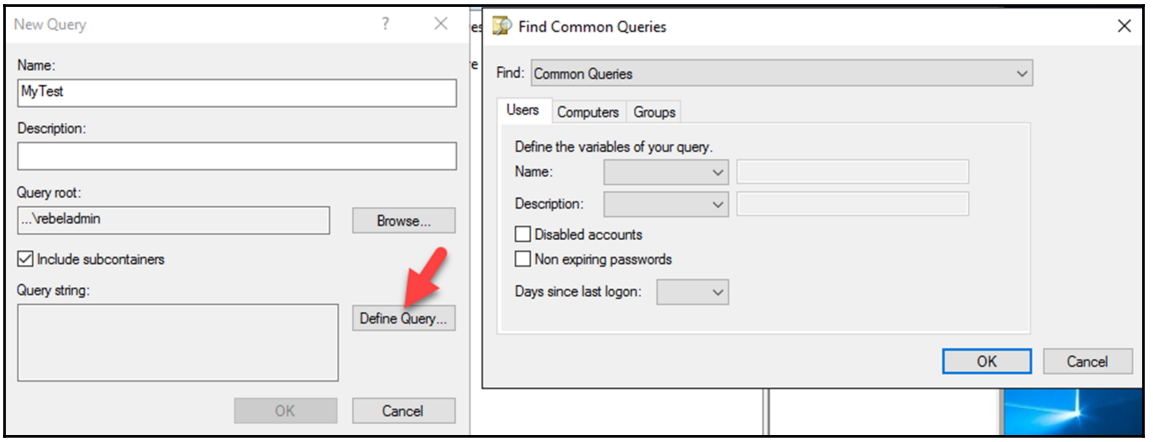

Active Directory Administrative Center
Active Directory Administrative Center ▸ Global Search
Manage
Help
Active Directory...
Overview
rebeladmin (local)
Europe\Users
Dynamic Access Control
Authentication
rebeladmin-Europe-Users
Global Search
GLOBAL SEARCH 1 items found
Normal
Convert to LDAP
Scope: rebeladmin
user1
Search
Name
Type
Description
user1
User
user1
Tasks
user1
Reset password...
View resultant password settin...
Add to group...
Disable
Delete
Move...
Locate
Properties

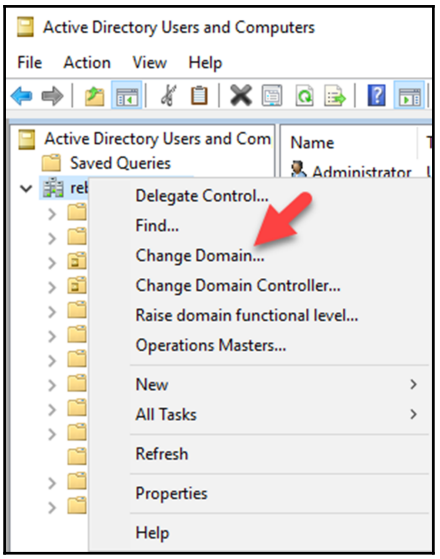

WINDOWS POWERSHELL HISTORY
Search
Copy
Start Task
End Task
Clear All
Show All
Help
Cmdlet
Time stamp
Get-ADDomainController -Discover:$true -DomainName:"REBELADMIN" -ForceDiscover:$true -Service:ADWS -Writable:$true
08/02/2017 23:56:05
New-PSDrive -Name:"ADDrive0" -PSProvider:"ActiveDirectory" -Root:"" -Server:"REBEL-PDC-01.rebeladmin.com"
08/02/2017 23:56:05
Get-ADRootDSE -Server:"REBEL-PDC-01.rebeladmin.com"
08/02/2017 23:56:06
Get-ADOptionalFeature -LDAPFilter:"(msDS-OptionalFeatureFlags=1)" -Server:"REBEL-PDC-01.rebeladmin.com"
08/02/2017 23:56:06
Get-ADRootDSE -Server:"REBEL-PDC-01.rebeladmin.com"
08/02/2017 23:56:06
Get-ADRootDSE -Server:"REBEL-PDC-01.rebeladmin.com"
08/02/2017 23:56:06
Get-ADOptionalFeature -LDAPFilter:"(msDS-OptionalFeatureFlags=1)" -Server:"REBEL-PDC-01.rebeladmin.com"
08/02/2017 23:56:06

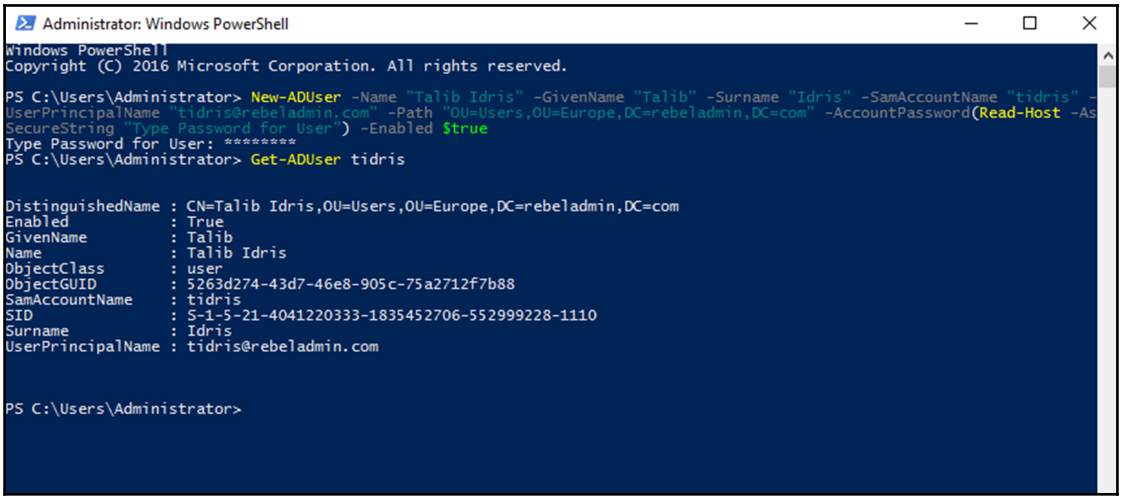

Add Navigation Nodes
You can browse through the columns below and select one or more containers to add to your Active Directory Administrative Center navigation pane.
Find in this column
rebeladmin
Find in this column
Builtin
Computers
Domain Controllers
Europe
ForeignSecurityPrincipa
Keys
LostAndFound
>>
Add the following containers to the navigation pane:
Connect to other domains...
OK
Cancel
Help

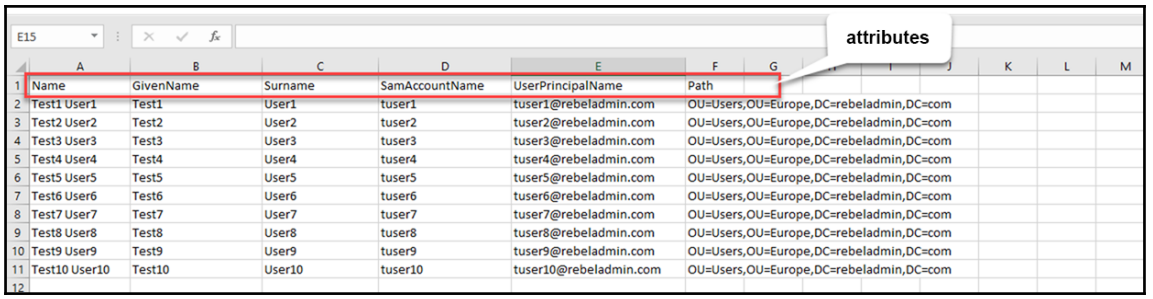

user1
administrative tasks
TASKS
SECTIONS
Account
Organization
Member Of
Password Settings
Profile
Policy
Silo
Extensions
sections
Account
First name: user1
Middle initials:
Last name:
Full name: user1
User UPN logon: user1 @ rebeladmin.com
User SamAccountName l... rebeladmin \ user1
Protect from accidental deletion
Log on hours...
Log on to...
Account expires: Never End of
Password options:
User must change password at next log on
Other password options
Microsoft Passport or smart card is required for interactive log on
Password never expires
User cannot change password
Encryption options:
Other options:
Organization
Display name: user1
Office: test
E-mail:
Web page:
Other web pages...
Phone numbers:
Main:
Home:
Mobile:
Fax:
Pager:
IP Phone:
Job title:
Department:
Company:
Manager:
Edit...
Clear
Direct reports:
Add...
Remove
Address:
Street
City
State/Province
Zip/Postal code
Activate Windows


menu bar
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
rebeladmin.com
Builtin
Computers
Domain Controllers
Europe
Computers
Users
ForeignSecurityPrincipal
Managed Service Accou
Users
Name Type Description
user1 User
user2 User
Actions
Users
More Actions
management pane
console tree
actions pane

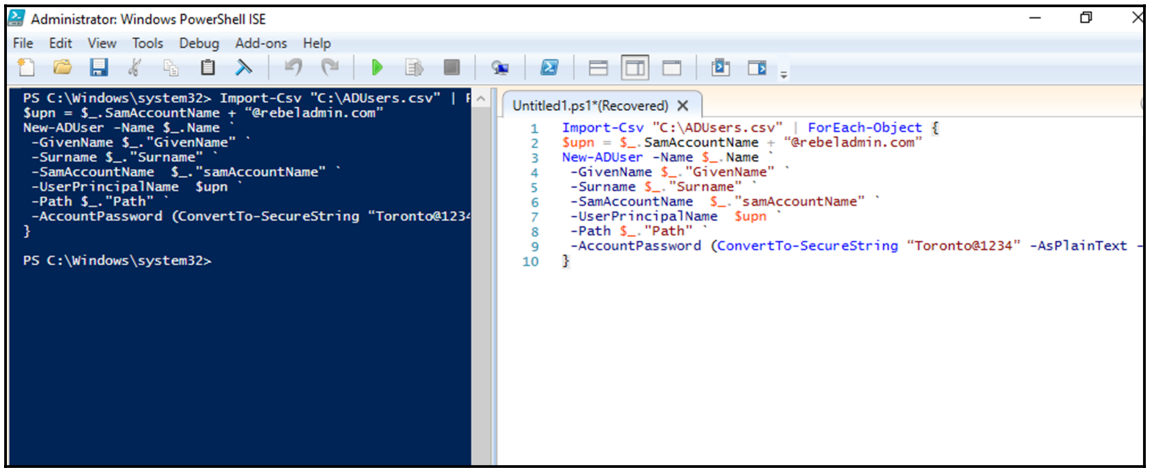

New Query
Name:
MyTest
Description:
Query root:
...\rebeladmin
Browse...
Include subcontainers
Query string:
Define Query...
OK
Cancel
Find Common Queries
Find: Common Queries
Users Computers Groups
Define the variables of your query.
Name:
Description:
Disabled accounts
Non expiring passwords
Days since last logon:
OK
Cancel

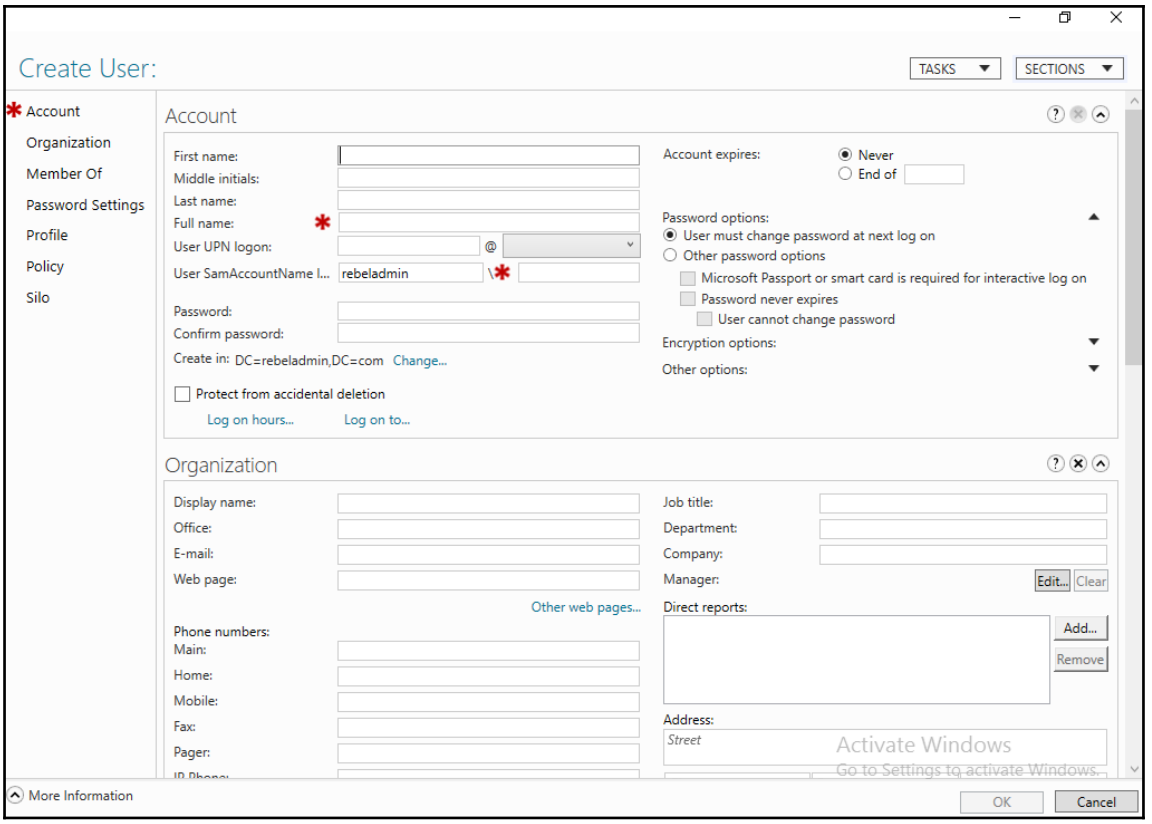

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
Name
Administrator
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
Refresh
Properties
Help

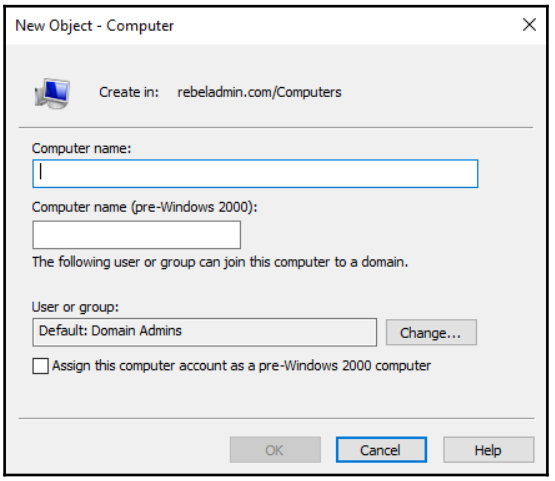

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> New-ADUser -Name "Talib Idris" -GivenName "Talib" -Surname "Idris" -SamAccountName "tidris" -
UserPrincipalName "tidris@rebeladmin.com" -Path "OU=Users,OU=Europe,DC=rebeladmin,DC=com" -AccountPassword(Read-Host -As
SecureString "Type Password for User") -Enabled $true
Type Password for User: ********
PS C:\Users\Administrator> Get-ADUser tidris
DistinguishedName : CN=Talib Idris,OU=Users,OU=Europe,DC=rebeladmin,DC=com
Enabled : True
GivenName : Talib
Name : Talib Idris
ObjectClass : user
ObjectGUID : 5263d274-43d7-46e8-905c-75a2712f7b88
SamAccountName : tidris
SID : S-1-5-21-4041220333-1835452706-552999228-1110
Surname : Idris
UserPrincipalName : tidris@rebeladmin.com
PS C:\Users\Administrator>

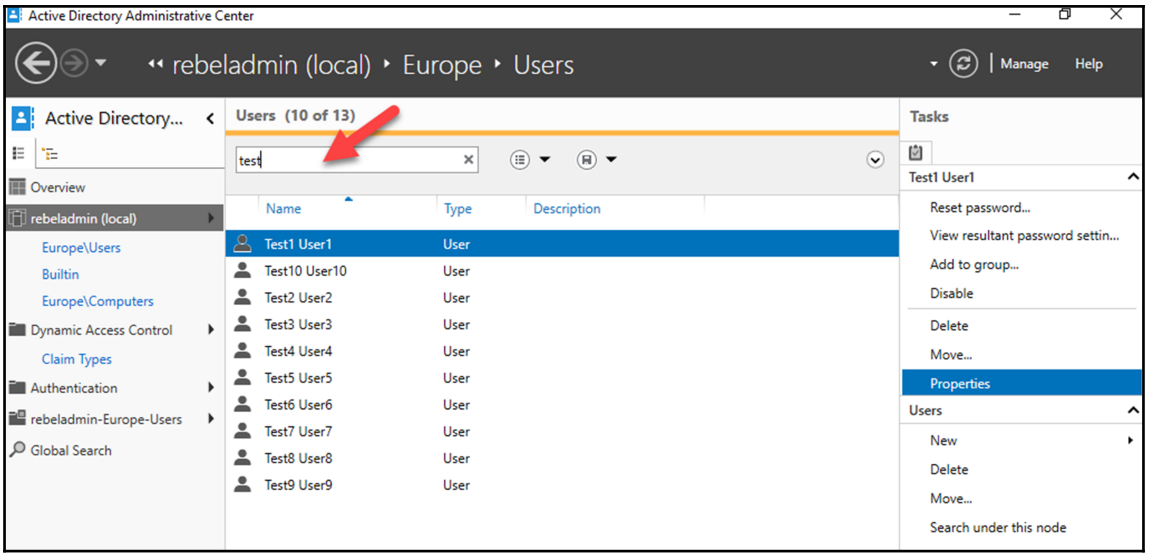


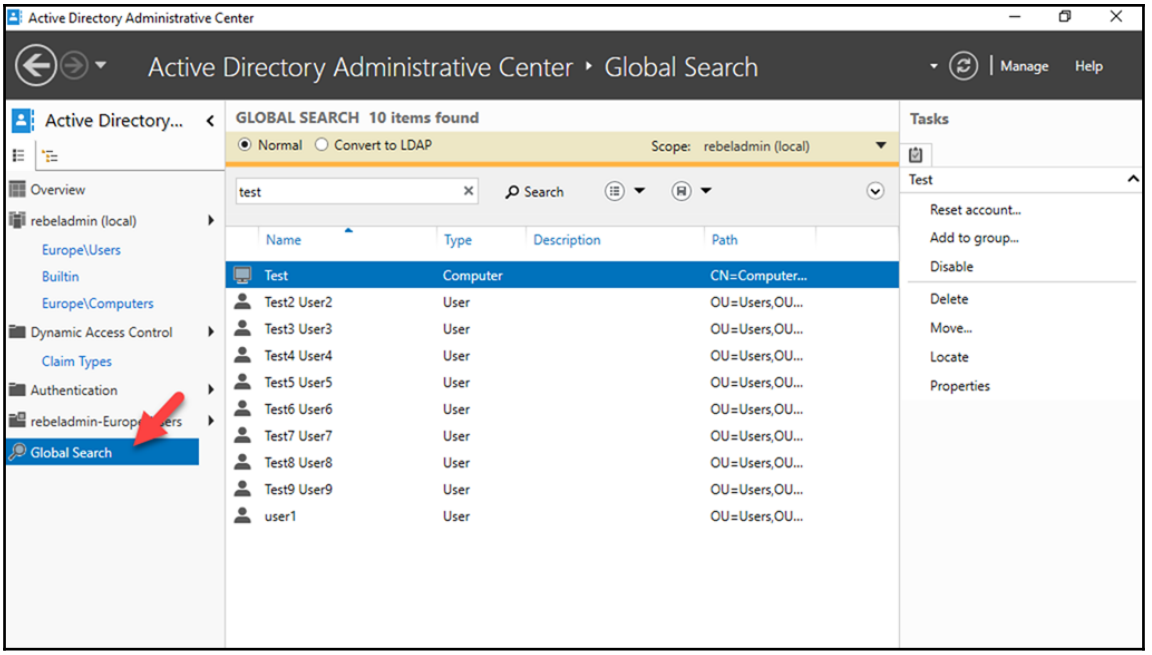
	A	B	C	D	E	F
1	Name	GivenName	Surname	SamAccountName	UserPrincipalName	Path
2	Test1 User1	Test1	User1	tuser1	tuser1@rebeladmin.com	OU=Users,OU=Europe,DC=rebeladmin,DC=com
3	Test2 User2	Test2	User2	tuser2	tuser2@rebeladmin.com	OU=Users,OU=Europe,DC=rebeladmin,DC=com
4	Test3 User3	Test3	User3	tuser3	tuser3@rebeladmin.com	OU=Users,OU=Europe,DC=rebeladmin,DC=com
5	Test4 User4	Test4	User4	tuser4	tuser4@rebeladmin.com	OU=Users,OU=Europe,DC=rebeladmin,DC=com
6	Test5 User5	Test5	User5	tuser5	tuser5@rebeladmin.com	OU=Users,OU=Europe,DC=rebeladmin,DC=com
7	Test6 User6	Test6	User6	tuser6	tuser6@rebeladmin.com	OU=Users,OU=Europe,DC=rebeladmin,DC=com
8	Test7 User7	Test7	User7	tuser7	tuser7@rebeladmin.com	OU=Users,OU=Europe,DC=rebeladmin,DC=com
9	Test8 User8	Test8	User8	tuser8	tuser8@rebeladmin.com	OU=Users,OU=Europe,DC=rebeladmin,DC=com
10	Test9 User9	Test9	User9	tuser9	tuser9@rebeladmin.com	OU=Users,OU=Europe,DC=rebeladmin,DC=com
11	Test10 User10	Test10	User10	tuser10	tuser10@rebeladmin.com	OU=Users,OU=Europe,DC=rebeladmin,DC=com
12						

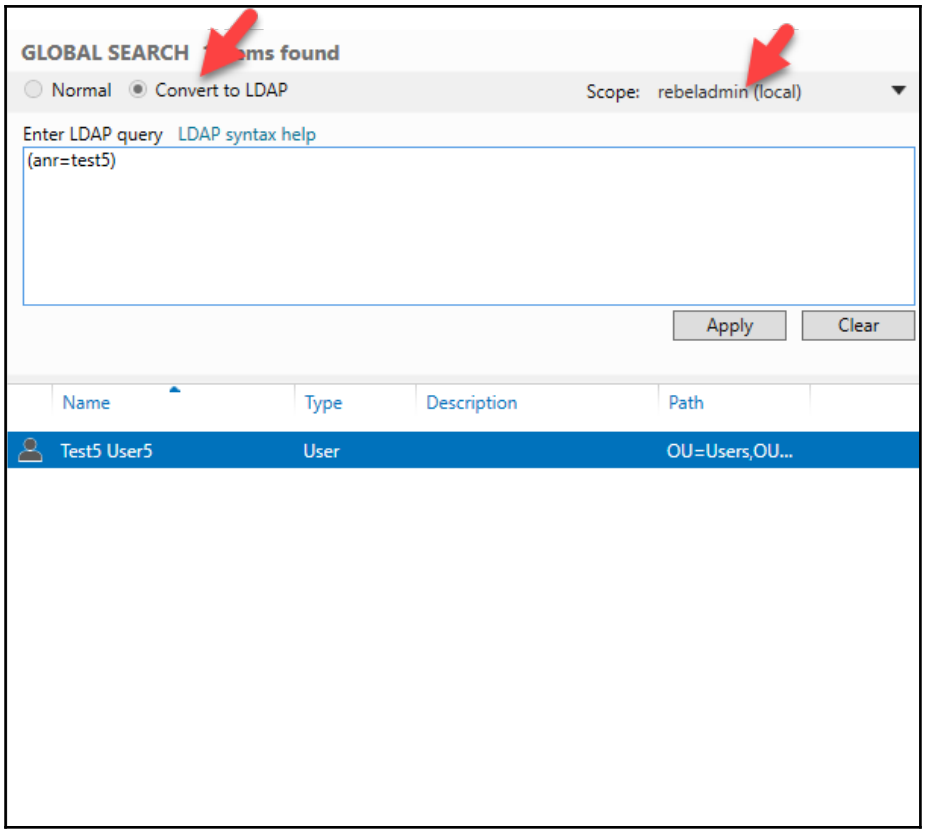


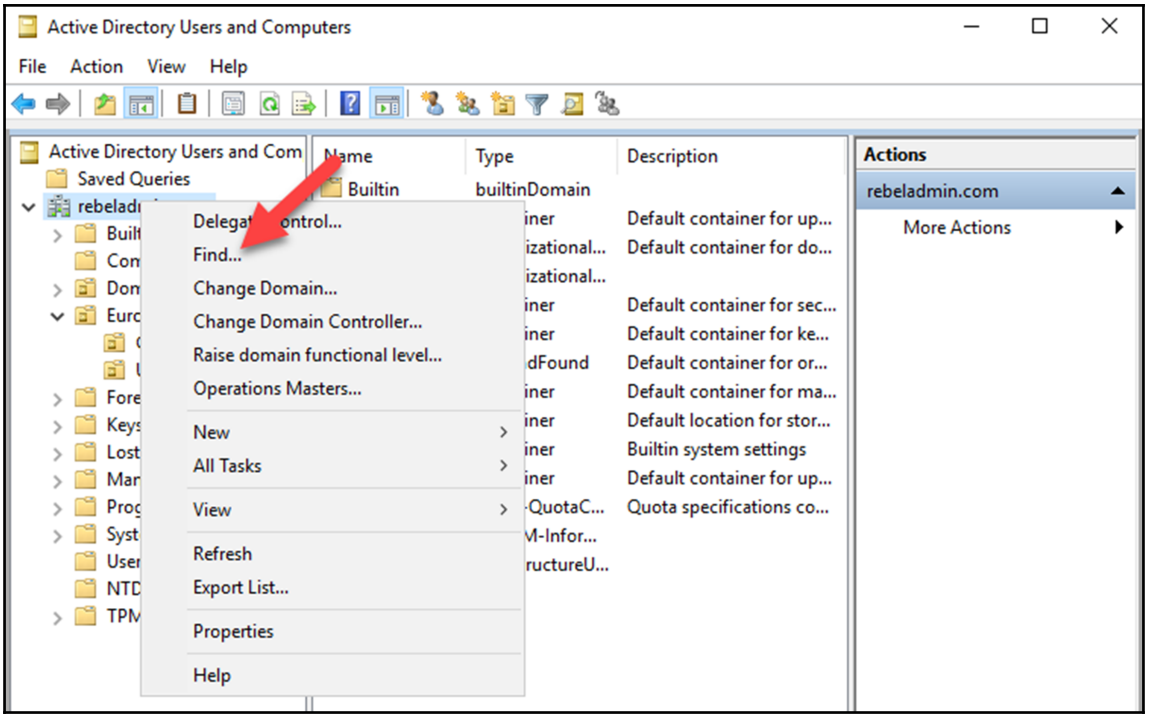

Create User:
TASKS
SECTIONS
Account
Organization
Member Of
Password Settings
Profile
Policy
Silo
Account
First name:
Middle initials:
Last name:
Full name:
User UPN logon:
User SamAccountName l...
rebeladmin
Password:
Confirm password:
Create in: DC=rebeladmin,DC=com Change...
Protect from accidental deletion
Log on hours...
Log on to...
Account expires:
Never
End of
Password options:
User must change password at next log on
Other password options
Microsoft Passport or smart card is required for interactive log on
Password never expires
User cannot change password
Encryption options:
Other options:
Organization
Display name:
Office:
E-mail:
Web page:
Other web pages...
Phone numbers:
Main:
Home:
Mobile:
Fax:
Pager:
Job title:
Department:
Company:
Manager:
Edit...
Clear
Direct reports:
Add...
Remove
Address:
Street
Activate Windows
Go to Settings to activate Windows.
More Information
OK
Cancel

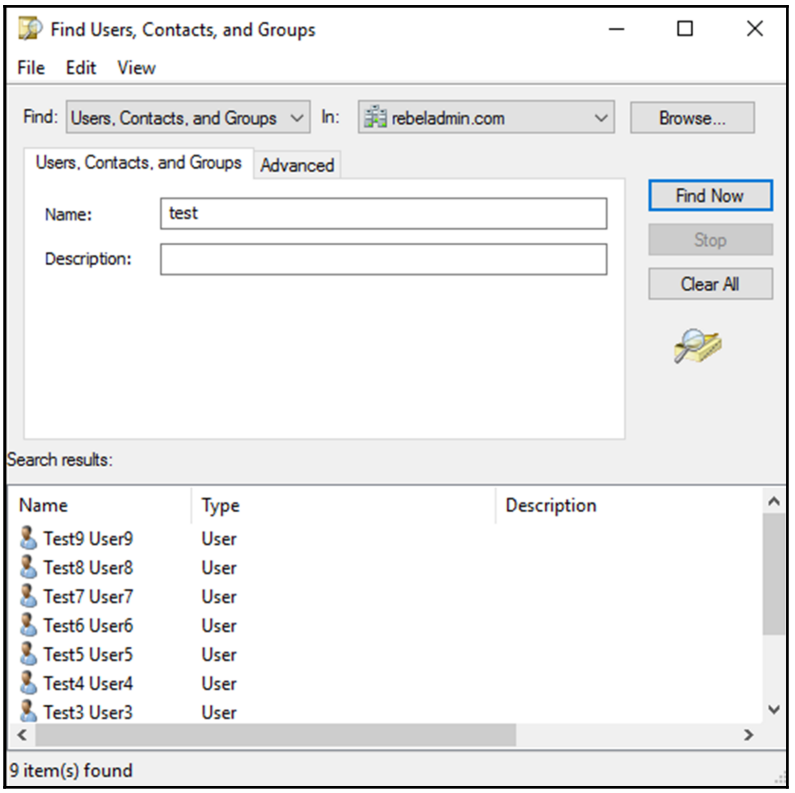

New Object - Computer
Create in: rebeladmin.com/Computers
Computer name:
Computer name (pre-Windows 2000):
The following user or group can join this computer to a domain.
User or group:
Default: Domain Admins
Change...
Assign this computer account as a pre-Windows 2000 computer
OK
Cancel
Help


Active Directory Administrative Center
rebeladmin (local) ▸ Europe ▸ Users
Manage
Help
Active Directory...
Overview
rebeladmin (local)
Europe\Users
Builtin
Europe\Computers
Dynamic Access Control
Claim Types
Authentication
rebeladmin-Europe-Users
Global Search
Users (10 of 13)
test
Name
Type
Description
Test1 User1 User
Test10 User10 User
Test2 User2 User
Test3 User3 User
Test4 User4 User
Test5 User5 User
Test6 User6 User
Test7 User7 User
Test8 User8 User
Test9 User9 User
Tasks
Test1 User1
Reset password...
View resultant password settin...
Add to group...
Disable
Delete
Move...
Properties
Users
New
Delete
Move...
Search under this node


Active Directory Administrative Center
Active Directory Administrative Center ▸ Global Search
Manage
Help
Active Directory...
Overview
rebeladmin (local)
Europe\Users
Builtin
Europe\Computers
Dynamic Access Control
Claim Types
Authentication
Global Search
GLOBAL SEARCH 10 items found
Normal
Convert to LDAP
Scope: rebeladmin (local)
test
Search
Name
Type
Description
Path
Test Computer CN=Computer...
Test2 User2 User OU=Users,OU...
Test3 User3 User OU=Users,OU...
Test4 User4 User OU=Users,OU...
Test5 User5 User OU=Users,OU...
Test6 User6 User OU=Users,OU...
Test7 User7 User OU=Users,OU...
Test8 User8 User OU=Users,OU...
Test9 User9 User OU=Users,OU...
user1 User OU=Users,OU...
Tasks
Test
Reset account...
Add to group...
Disable
Delete
Move...
Locate
Properties

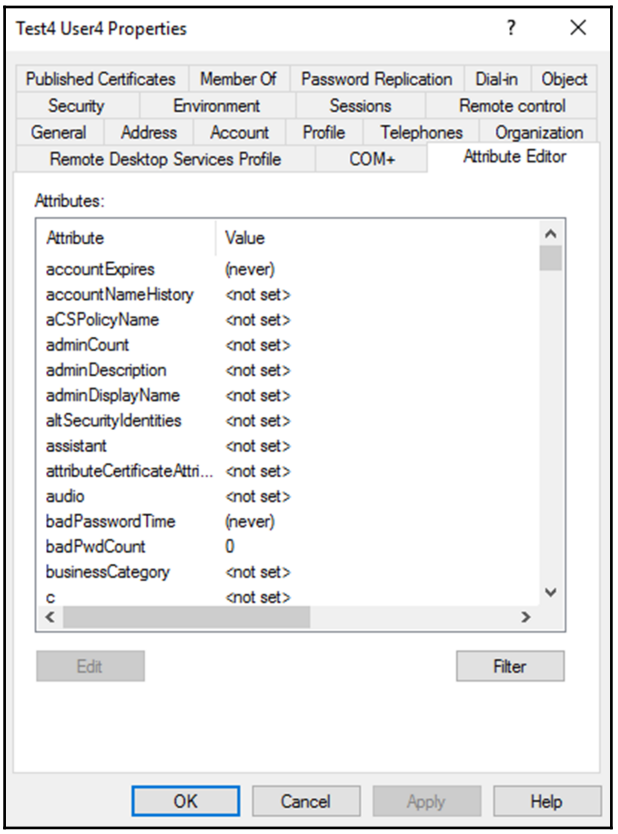

GLOBAL SEARCH
Normal
Convert to LDAP
Scope:
rebeladmin (local)
Enter LDAP query
LDAP syntax help
(anr=test5)
Apply
Clear
Name
Type
Description
Path
Test5 User5
User
OU=Users,OU...

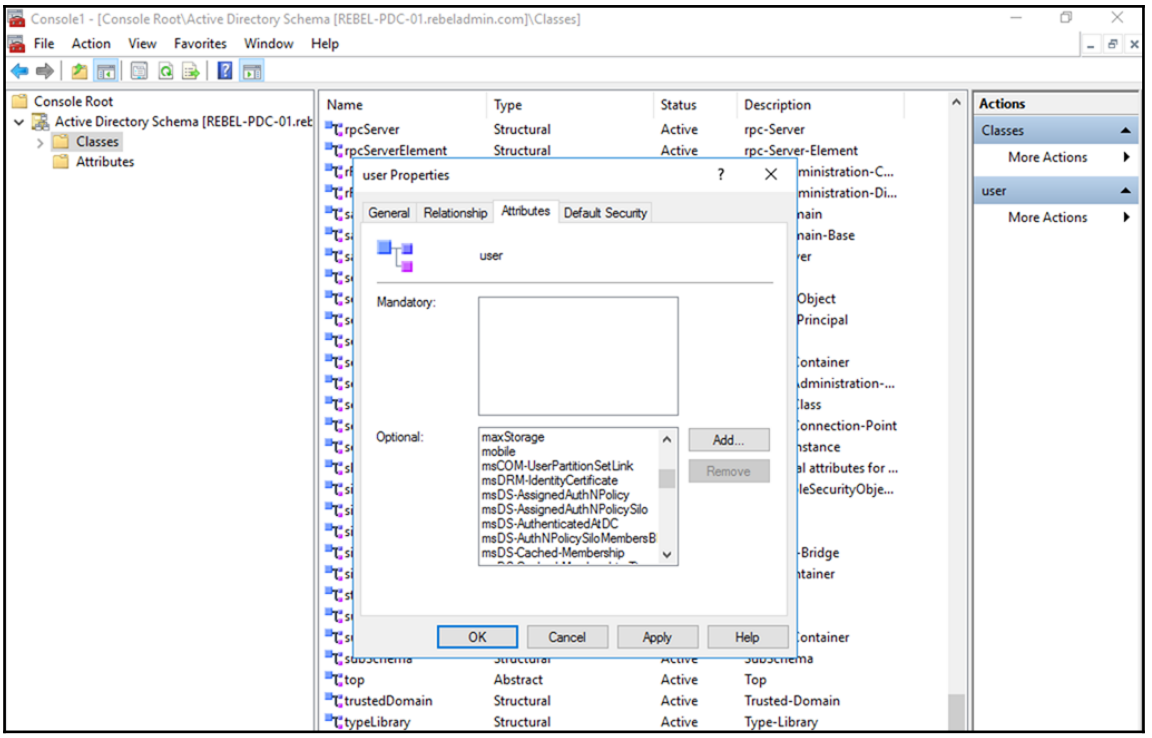

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
Name
Type
Description
Builtin
builtinDomain
Delegate control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
View
Refresh
Export List...
Properties
Help
Default container for up...
Default container for do...
Default container for sec...
Default container for ke...
Default container for or...
Default container for ma...
Default location for stor...
Builtin system settings
Default container for up...
Quota specifications co...
Actions
rebeladmin.com
More Actions

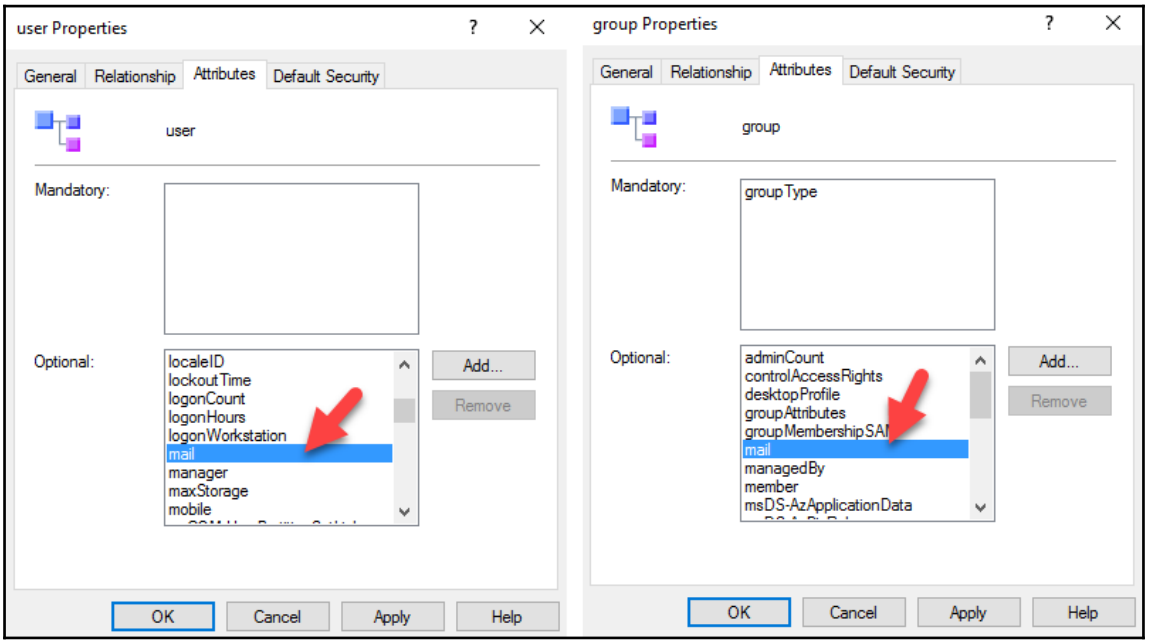


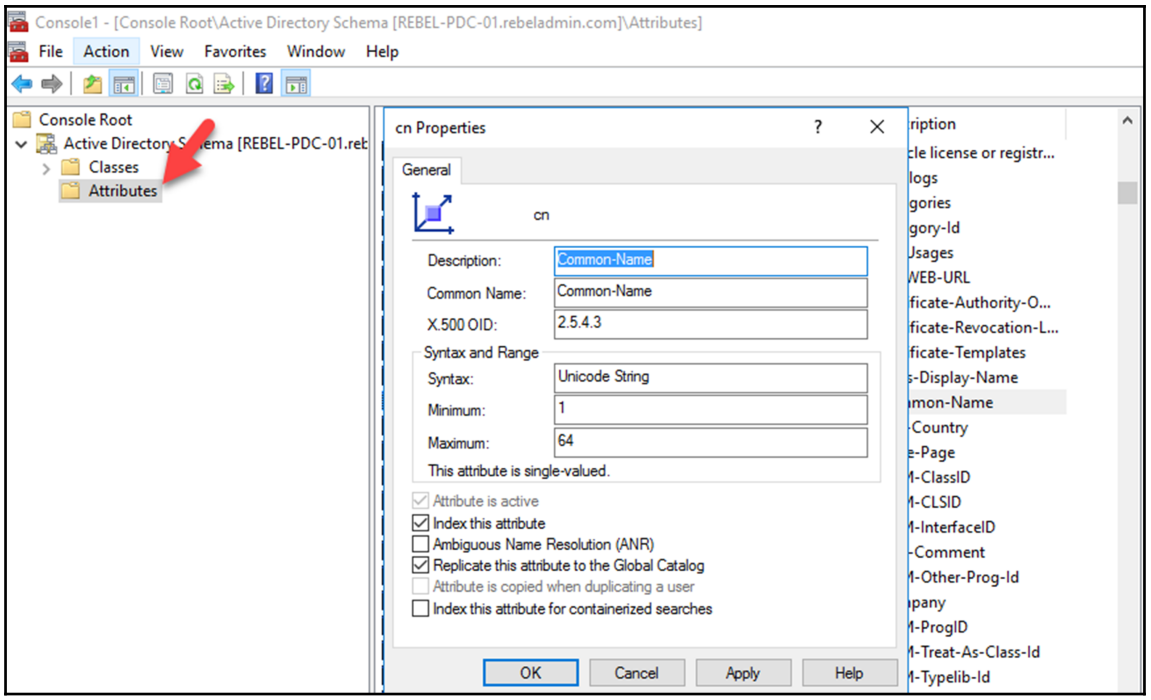

```
PS C:\Users\Administrator> Get-ADUser -Filter * -Properties Name,UserPrincipalName,Modified | ft Name,UserPrincipalName,Modified

Name           UserPrincipalName     Modified
----           -----------------     --------
Administrator                        07/02/2017 21:54:21
Guest                                28/01/2017 18:36:54
DefaultAccount                       28/01/2017 18:36:54
krbtgt                               28/01/2017 18:53:28
user1          user1@rebeladmin.com  11/02/2017 19:04:55
user2          user2@rebeladmin.com  11/02/2017 19:04:55
UserA                                11/02/2017 12:03:28
Test2 User2    tuser2@rebeladmin.com 11/02/2017 19:04:55
Test3 User3    tuser3@rebeladmin.com 11/02/2017 19:04:55
Test4 User4    tuser4@rebeladmin.com 11/02/2017 19:04:55
Test5 User5    tuser5@rebeladmin.com 11/02/2017 19:04:55
Test6 User6    tuser6@rebeladmin.com 11/02/2017 19:04:55
Test7 User7    tuser7@rebeladmin.com 11/02/2017 19:04:55
Test8 User8    tuser8@rebeladmin.com 11/02/2017 19:04:55
Test9 User9    tuser9@rebeladmin.com 11/02/2017 19:04:55
```

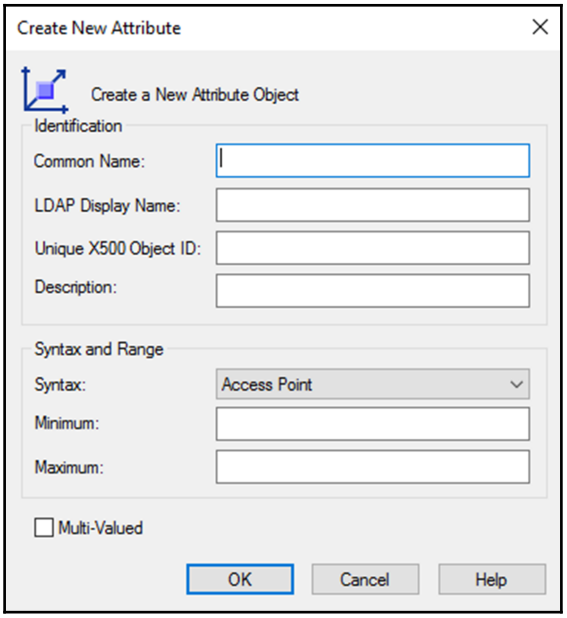
Chapter 8: Managing Users, Groups, and Devices

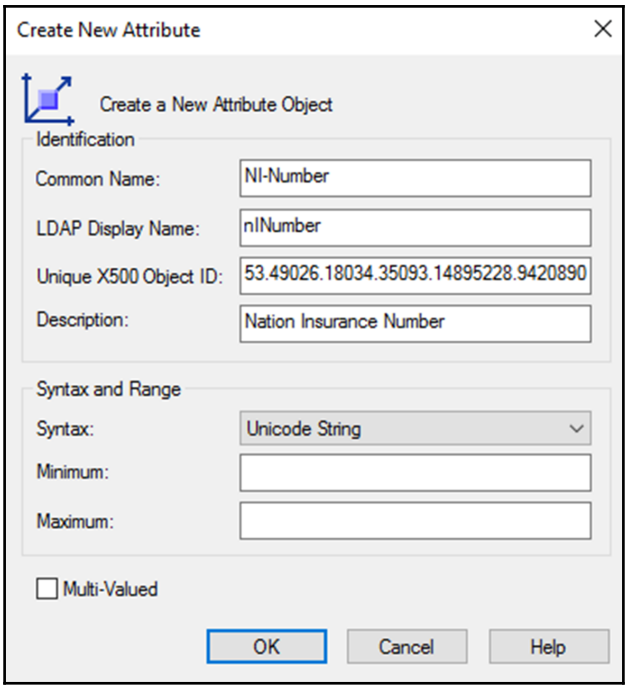


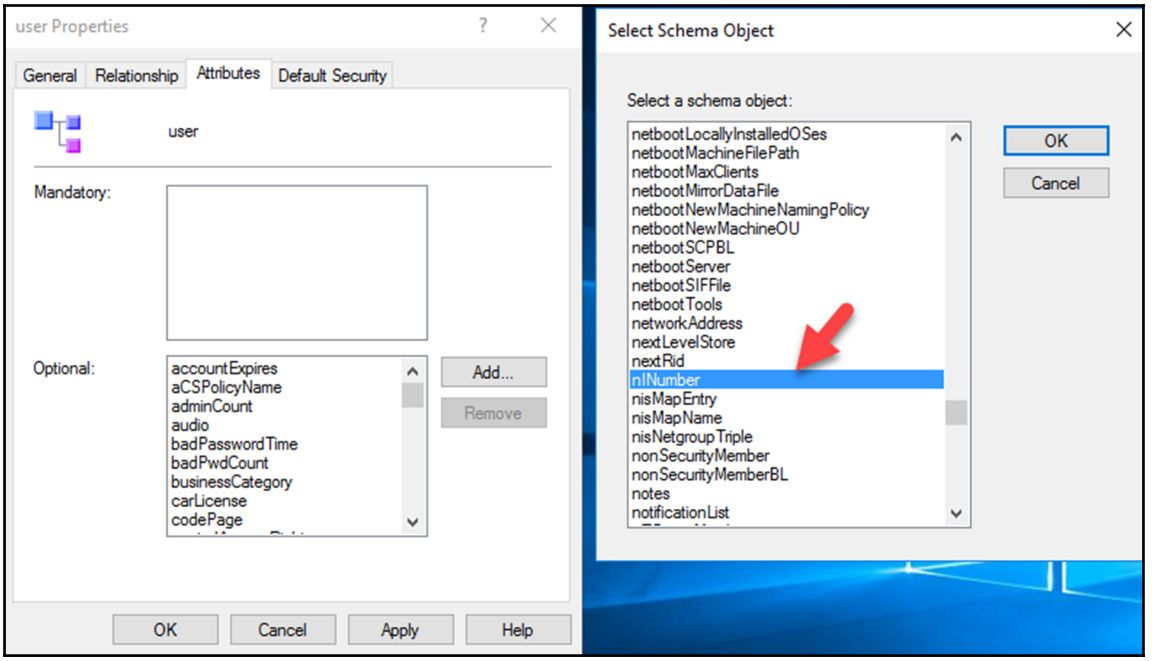

Console1 - [Console Root\Active Directory Schema [REBEL-PDC-01.rebeladmin.com]\Classes]
File Action View Favorites Window Help
Console Root
Active Directory Schema [REBEL-PDC-01.reb
Classes
Attributes
Name Type Status Description
rpcServer Structural Active rpc-Server
rpcServerElement Structural Active rpc-Server-Element
user Properties
General Relationship Attributes Default Security
user
Mandatory:
Optional:
maxStorage
mobile
msCOM-UserPartitionSetLink
msDRM-IdentityCertificate
msDS-AssignedAuthNPolicy
msDS-AssignedAuthNPolicySilo
msDS-AuthenticatedAtDC
msDS-AuthNPolicySiloMembersB
msDS-Cached-Membership
Add...
Remove
OK Cancel Apply Help
top Abstract Active Top
trustedDomain Structural Active Trusted-Domain
typeLibrary Structural Active Type-Library
Actions
Classes
More Actions
user
More Actions

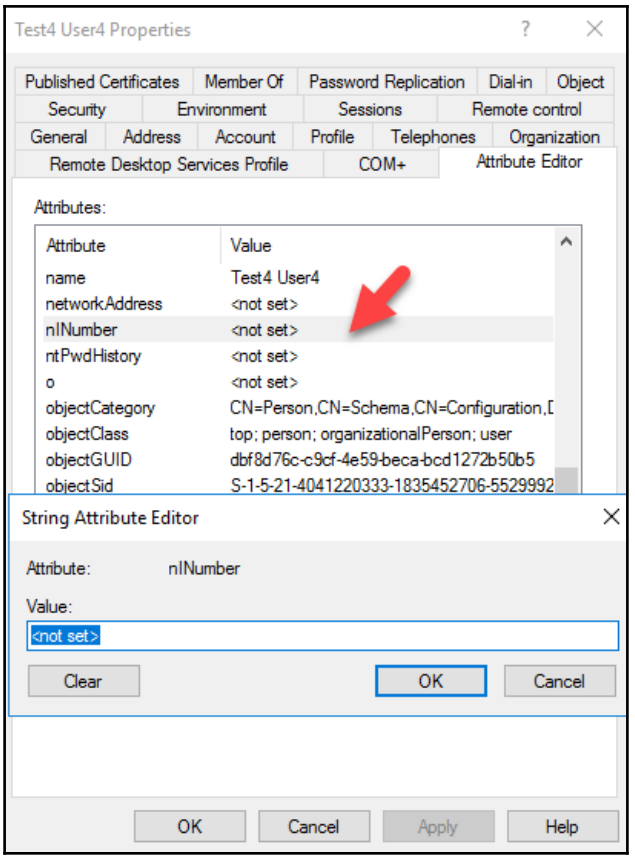

user Properties
General Relationship Attributes Default Security
user
Mandatory:
Optional:
localeID
lockoutTime
logonCount
logonHours
logonWorkstation
mail
manager
maxStorage
mobile
Add...
Remove
OK Cancel Apply Help
group Properties
General Relationship Attributes Default Security
group
Mandatory:
groupType
Optional:
adminCount
controlAccessRights
desktopProfile
groupAttributes
groupMembershipSAM
mail
managedBy
member
msDS-AzApplicationData
Add...
Remove
OK Cancel Apply Help


Console1 - [Console Root\Active Directory Schema [REBEL-PDC-01.rebeladmin.com]\Attributes]
File
Action
View
Favorites
Window
Help
Console Root
Classes
Attributes
cn Properties
General
cn
Description:
Common-Name
Common Name:
Common-Name
X.500 OID:
2.5.4.3
Syntax and Range
Syntax:
Unicode String
Minimum:
1
Maximum:
64
This attribute is single-valued.
Attribute is active
Index this attribute
Ambiguous Name Resolution (ANR)
Replicate this attribute to the Global Catalog
Attribute is copied when duplicating a user
Index this attribute for containerized searches
OK
Cancel
Apply
Help

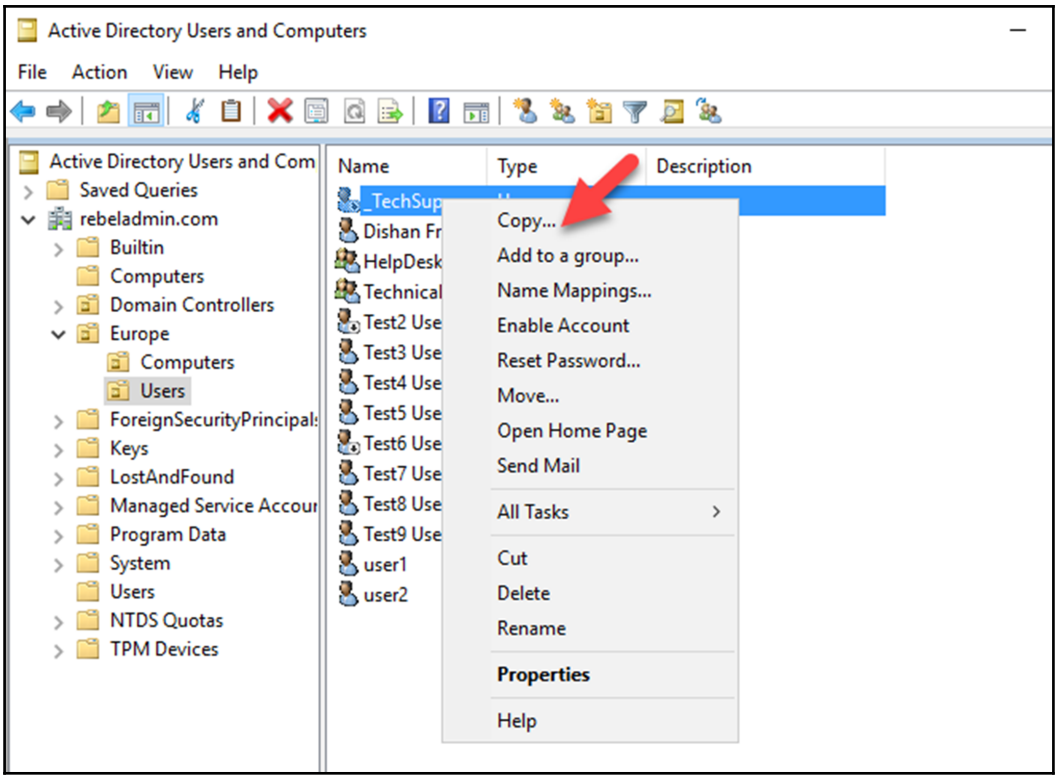

Create New Attribute
Create a New Attribute Object
Identification
Common Name:
LDAP Display Name:
Unique X500 Object ID:
Description:
Syntax and Range
Syntax:
Access Point
Minimum:
Maximum:
Multi-Valued
OK
Cancel
Help


Create New Attribute
Create a New Attribute Object
Identification
Common Name:
NI-Number
LDAP Display Name:
nINumber
Unique X500 Object ID:
53.49026.18034.35093.14895228.9420890
Description:
Nation Insurance Number
Syntax and Range
Syntax:
Unicode String
Minimum:
Maximum:
Multi-Valued
OK
Cancel
Help


user Properties
General
Relationship
Attributes
Default Security
user
Mandatory:
Optional:
accountExpires
aCSPolicyName
adminCount
audio
badPasswordTime
badPwdCount
businessCategory
carLicense
codePage
Add...
Remove
OK
Cancel
Apply
Help
Select Schema Object
Select a schema object:
netbootLocallyInstalledOSes
netbootMachineFilePath
netbootMaxClients
netbootMirrorDataFile
netbootNewMachineNamingPolicy
netbootNewMachineOU
netbootSCPBL
netbootServer
netbootSIFFile
netbootTools
networkAddress
nextLevelStore
nextRid
nINumber
nisMapEntry
nisMapName
nisNetgroupTriple
nonSecurityMember
nonSecurityMemberBL
notes
notificationList
OK
Cancel




```
PS C:\Users\Administrator> Get-ADUser "tuser4" -Properties nINumber | ft nINumber

nINumber
--------
2234553786
```



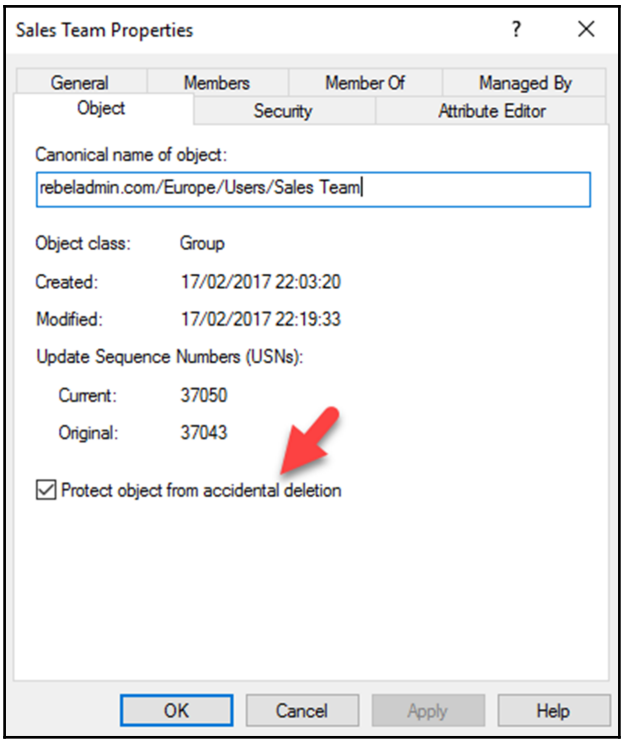

```
PS C:\Users\Administrator> Get-ADUser "sbrewer" -Properties * | ft Name,Memberof,Enabled

Name         Memberof                                                                Enabled
----         --------                                                                -------
Scott Brewer {CN=Technical Department,OU=Users,OU=Europe,DC=rebeladmin,DC=com}         True
```

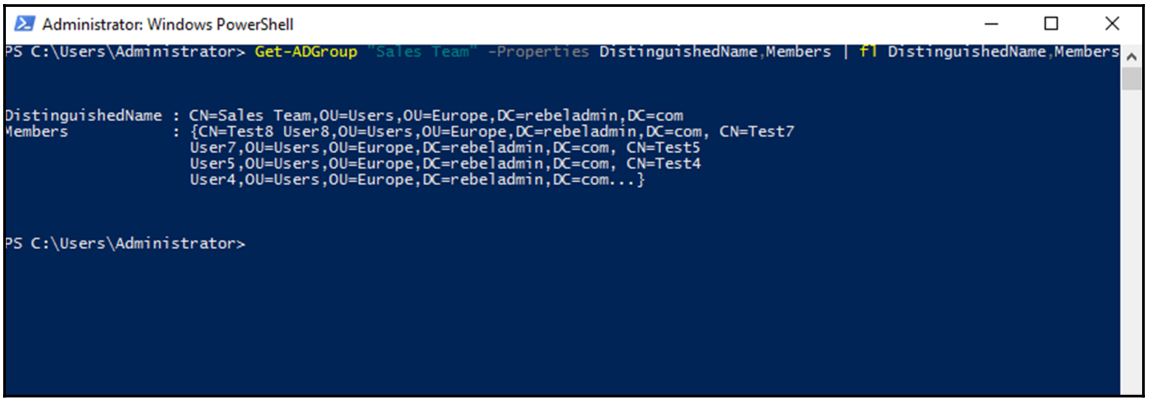
```
Administrator: Windows PowerShell
PS C:\Users\administrator.REBELADMIN> Install-ADServiceAccount -Identity "MyAcc1"
PS C:\Users\administrator.REBELADMIN> Test-ADServiceAccount "MyAcc1"
True
PS C:\Users\administrator.REBELADMIN>
```

```
PS C:\Users\Administrator> Get-ADServiceAccount "MyAcc1"


DistinguishedName : CN=MyAcc1,CN=Managed Service Accounts,DC=rebeladmin,DC=com
Enabled           : True
Name              : MyAcc1
ObjectClass       : msDS-ManagedServiceAccount
ObjectGUID        : e72809fe-2b55-41d6-98de-85c62c9f5fc6
SamAccountName    : MyAcc1$
SID               : S-1-5-21-4041220333-1835452706-552999228-1203
UserPrincipalName :
```

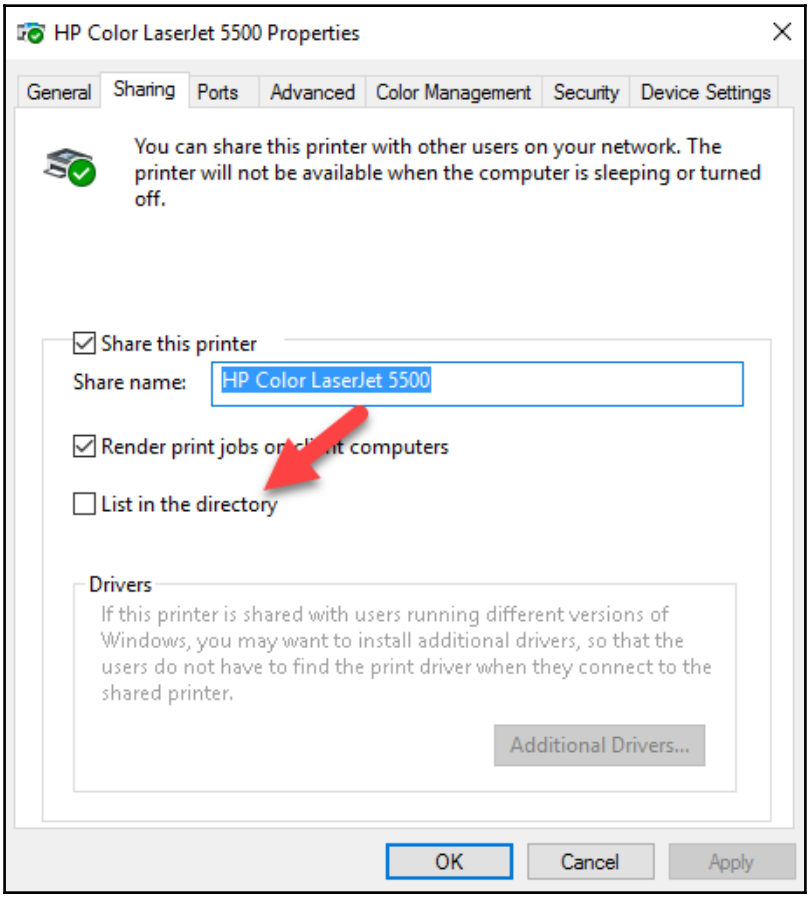
```
PS C:\Users\Administrator> Get-ADServiceAccount "Mygmsa1"


DistinguishedName : CN=Mygmsa1,CN=Managed Service Accounts,DC=rebeladmin,DC=com
Enabled           : True
Name              : Mygmsa1
ObjectClass       : msDS-GroupManagedServiceAccount
ObjectGUID        : 6b39efa1-19b8-4690-a477-858873f0aa40
SamAccountName    : Mygmsa1$
SID               : S-1-5-21-4041220333-1835452706-552999228-1205
UserPrincipalName :
```

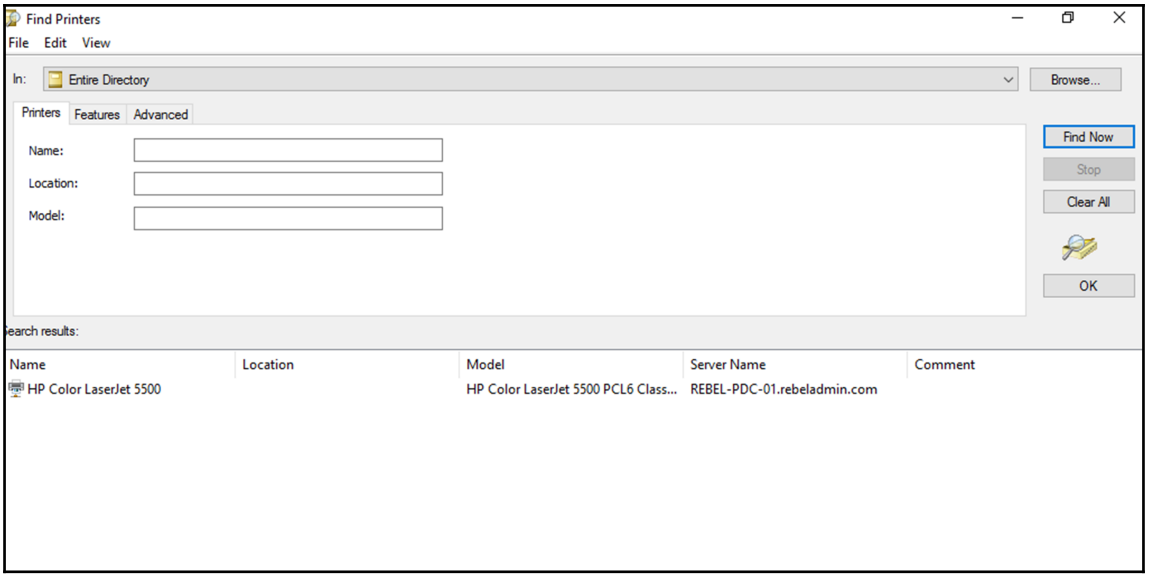
```
Administrator: Windows PowerShell
PS C:\Users\administrator.REBELADMIN> Install-ADServiceAccount -Identity " Mygmsa1"
PS C:\Users\administrator.REBELADMIN> Test-ADServiceAccount " Mygmsa1"
True
PS C:\Users\administrator.REBELADMIN>
```


Sales Team Properties
General
Members
Member Of
Managed By
Object
Security
Attribute Editor
Canonical name of object:
rebeladmin.com/Europe/Users/Sales Team
Object class: Group
Created: 17/02/2017 22:03:20
Modified: 17/02/2017 22:19:33
Update Sequence Numbers (USNs):
Current: 37050
Original: 37043
Protect object from accidental deletion
OK
Cancel
Apply
Help


Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADGroup "Sales Team" -Properties DistinguishedName,Members | fl DistinguishedName,Members
DistinguishedName : CN=Sales Team,OU=Users,OU=Europe,DC=rebeladmin,DC=com
Members : {CN=Test8 User8,OU=Users,OU=Europe,DC=rebeladmin,DC=com, CN=Test7
User7,OU=Users,OU=Europe,DC=rebeladmin,DC=com, CN=Test5
User5,OU=Users,OU=Europe,DC=rebeladmin,DC=com, CN=Test4
User4,OU=Users,OU=Europe,DC=rebeladmin,DC=com...}
PS C:\Users\Administrator>

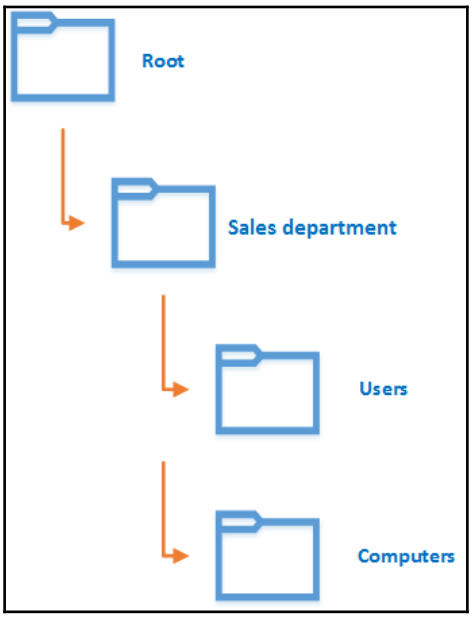
```
PS C:\Users\Administrator> Set-ADGroup "Sales Team" -GroupScope Universal
PS C:\Users\Administrator> Get-ADGroup "Sales Team"


DistinguishedName : CN=Sales Team,OU=Users,OU=Europe,DC=rebeladmin,DC=com
GroupCategory     : Security
GroupScope        : Universal
Name              : Sales Team
ObjectClass       : group
ObjectGUID        : a70e28d9-be49-4f6a-9c88-2ca0dbd4bcbf
SamAccountName    : Sales Team
SID               : S-1-5-21-4041220333-1835452706-552999228-1208


PS C:\Users\Administrator> _
```

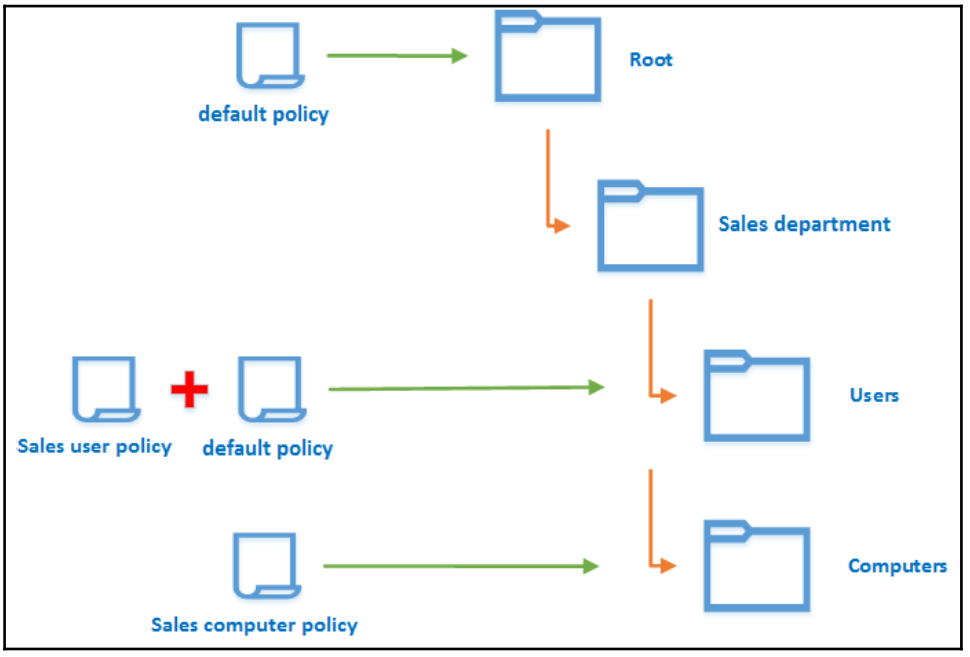


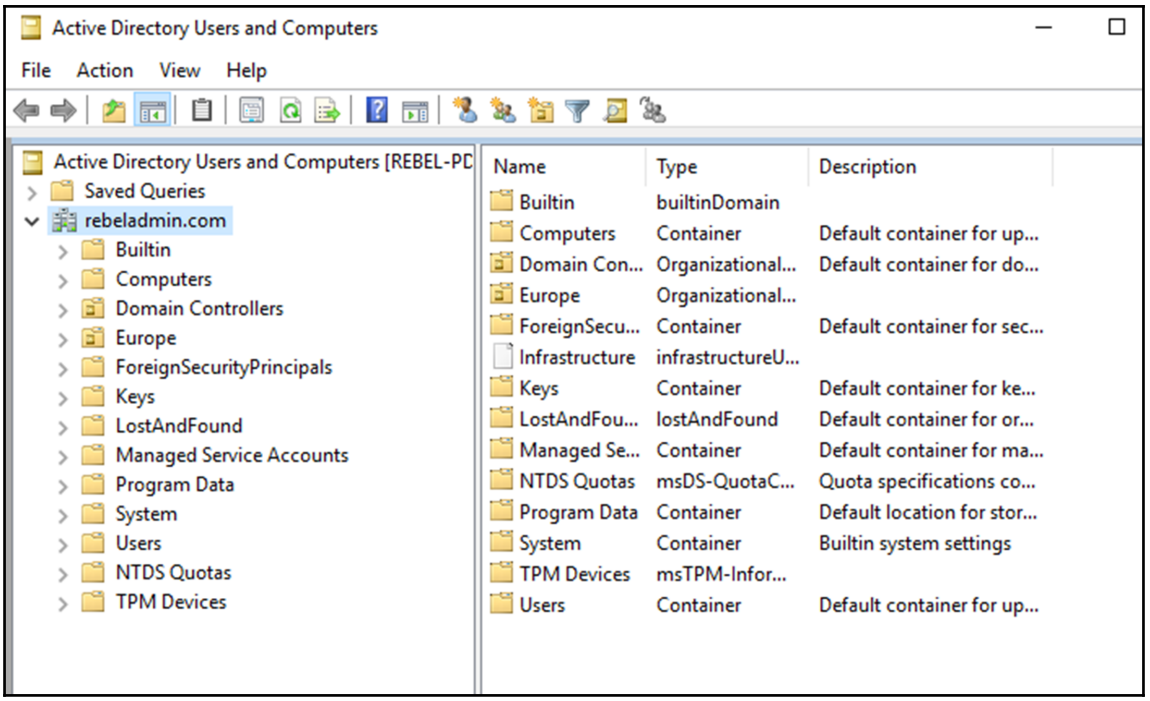


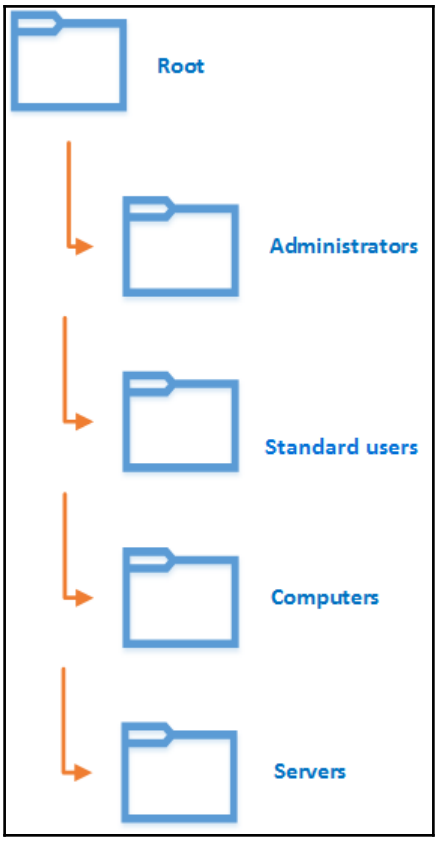

```
PS C:\Users\Administrator> Set-ADUser "inetuser1" -Remove @{objectClass='inetOrgPerson'}^M
PS C:\Users\Administrator> Get-ADUser "inetuser1"


DistinguishedName : CN=Inet User1,OU=Users,OU=Europe,DC=rebeladmin,DC=com
Enabled           : True
GivenName         : Inet
Name              : Inet U    1
ObjectClass       : user
ObjectGUID        : 7c4ba922-b0f7-495a-977f-e62e4f181177
SamAccountName    : inetuser1
SID               : S-1-5-21-4041220333-1835452706-552999228-1210
Surname           : User1
UserPrincipalName : isuer1@rebeladmin.com


PS C:\Users\Administrator> _
```

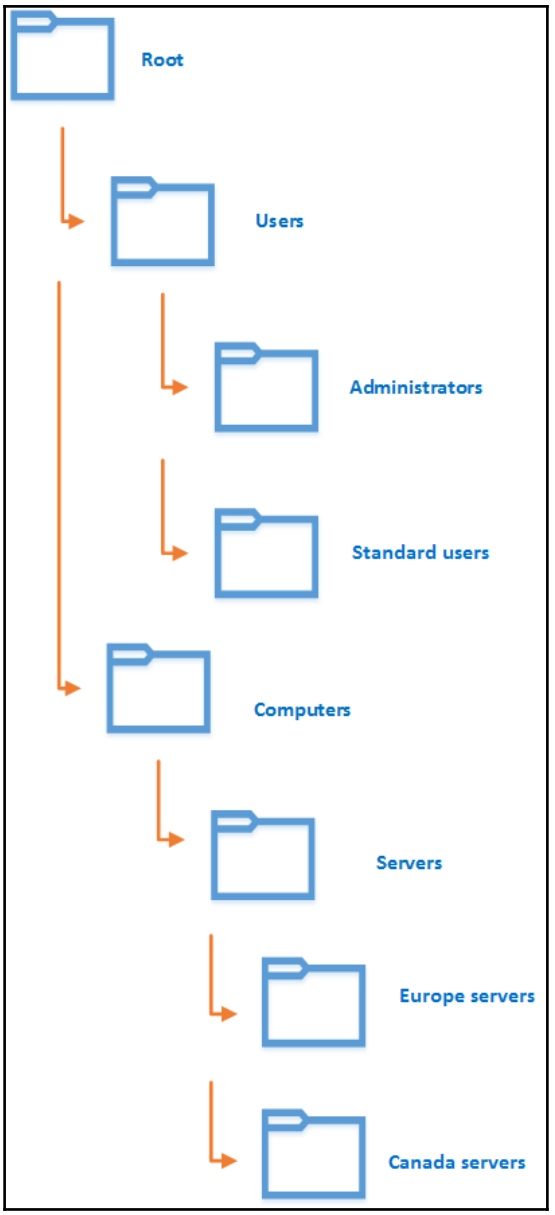
Chapter 9: Designing the OU Structure

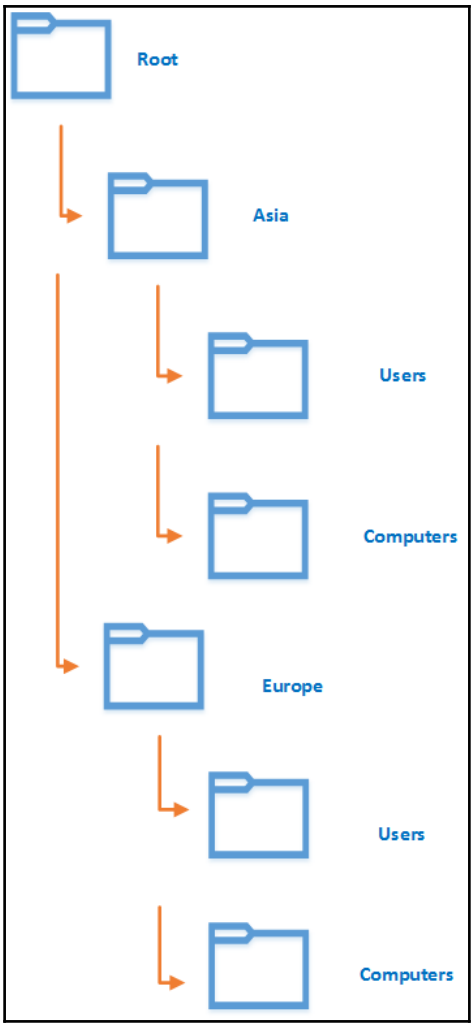


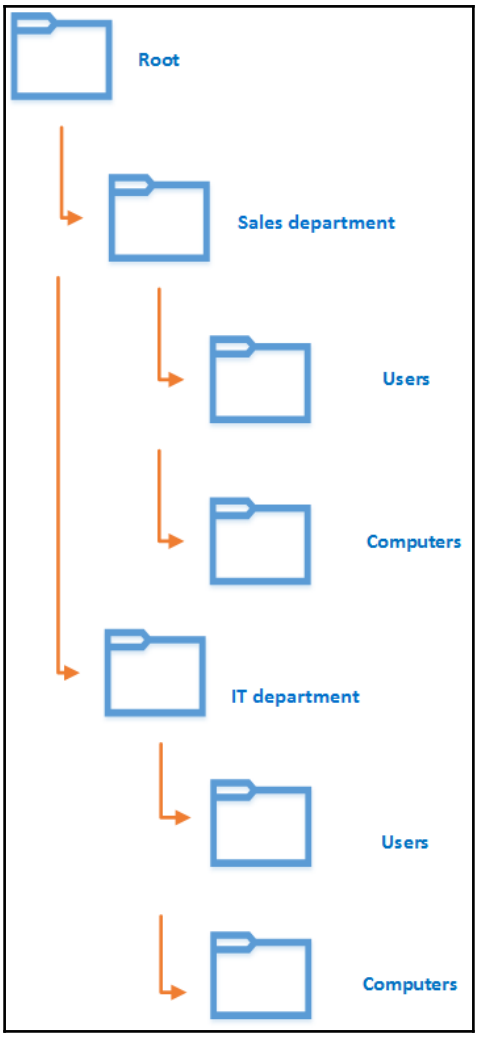



Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [REBEL-PD
Saved Queries
rebeladmin.com
Builtin
Computers
Domain Controllers
Europe
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Program Data
System
Users
NTDS Quotas
TPM Devices
Name Type Description
Builtin builtinDomain
Computers Container Default container for up...
Domain Con... Organizational... Default container for do...
Europe Organizational...
ForeignSecu... Container Default container for sec...
Infrastructure infrastructureU...
Keys Container Default container for ke...
LostAndFou... lostAndFound Default container for or...
Managed Se... Container Default container for ma...
NTDS Quotas msDS-QuotaC... Quota specifications co...
Program Data Container Default location for stor...
System Container Builtin system settings
TPM Devices msTPM-Infor...
Users Container Default container for up...

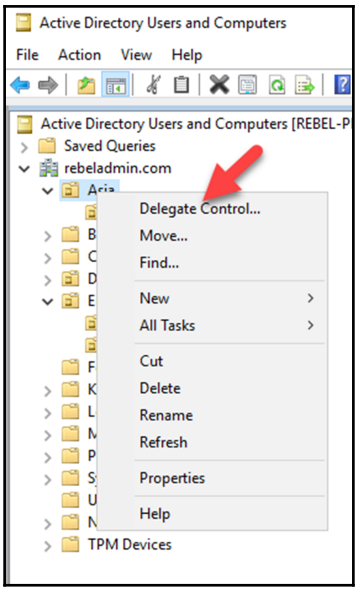

Root
Administrators
Standard users
Computers
Servers

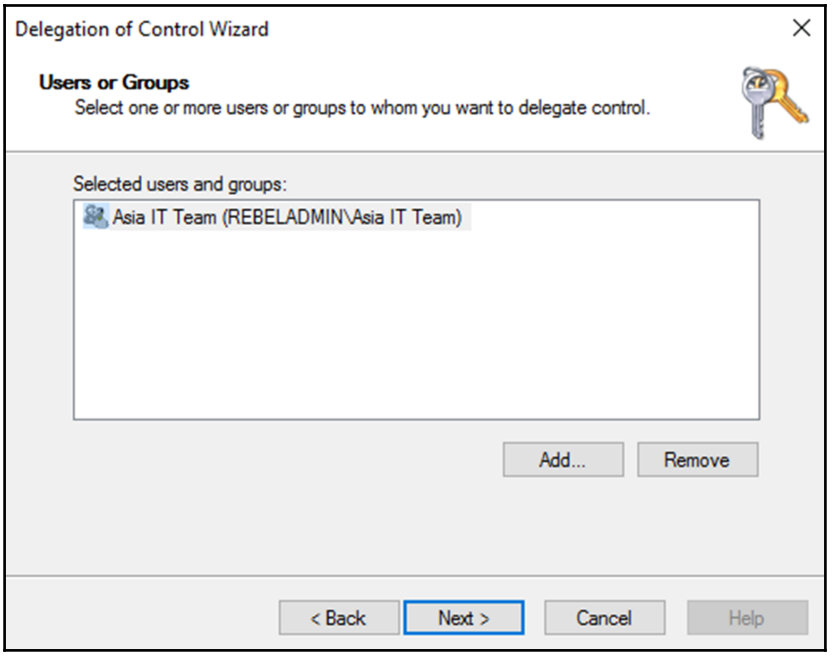

Root
Users
Administrators
Standard users
Computers
Servers
Europe servers
Canada servers

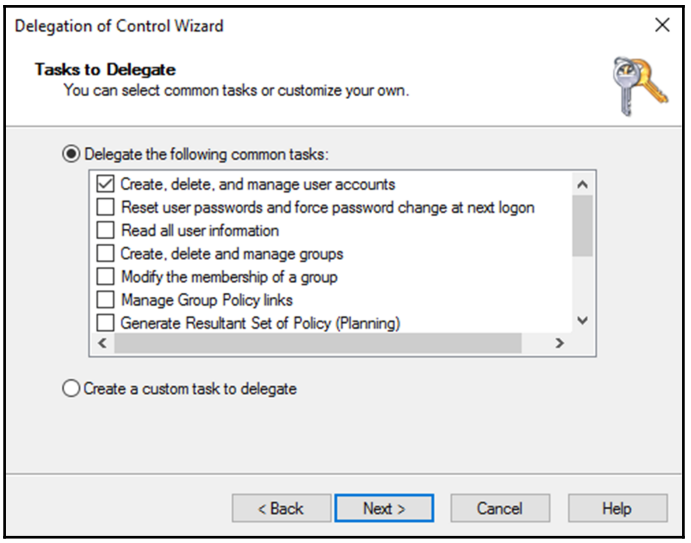

Root
Asia
Users
Computers
Europe
Users
Computers

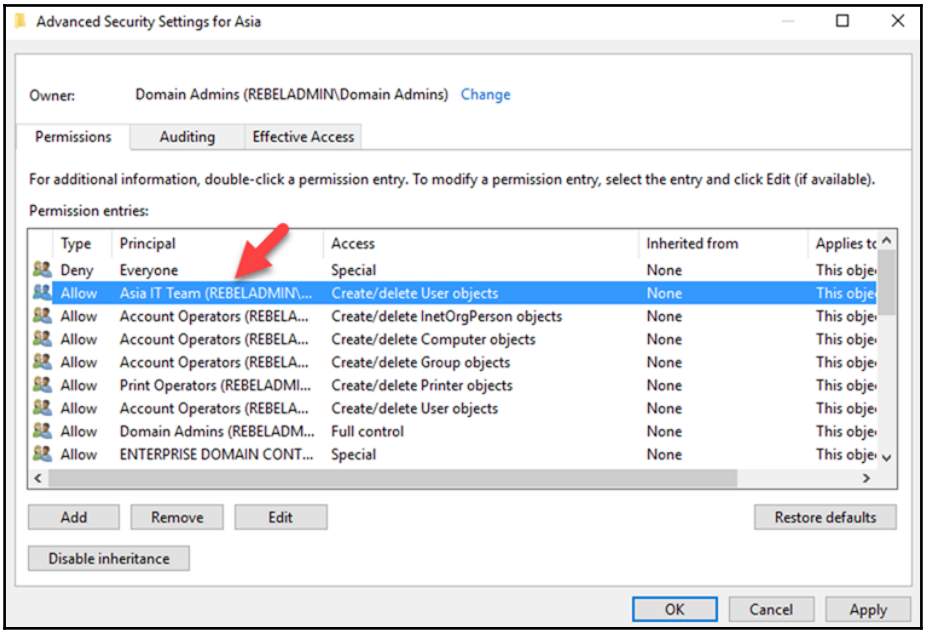



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADOrganizationalUnit -Identity "OU=Asia,DC=rebeladmin,DC=com"


City                            :
Country                         :
DistinguishedName               : OU=Asia,DC=rebeladmin,DC=com
LinkedGroupPolicyObjects        : {}
ManagedBy                       :
Name                            : Asia
ObjectClass                     : organizationalUnit
ObjectGUID                      : bd86da23-eabf-4f57-abb0-21993afa4c51
PostalCode                      :
State                           :
StreetAddress                   :
```

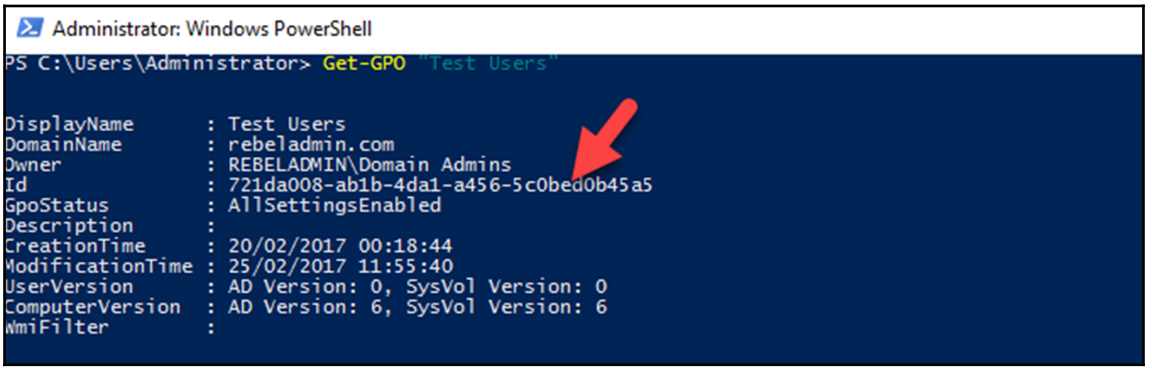

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [REBEL-P
Saved Queries
rebeladmin.com
Delegate Control...
Move...
Find...
New
All Tasks
Cut
Delete
Rename
Refresh
Properties
Help
TPM Devices

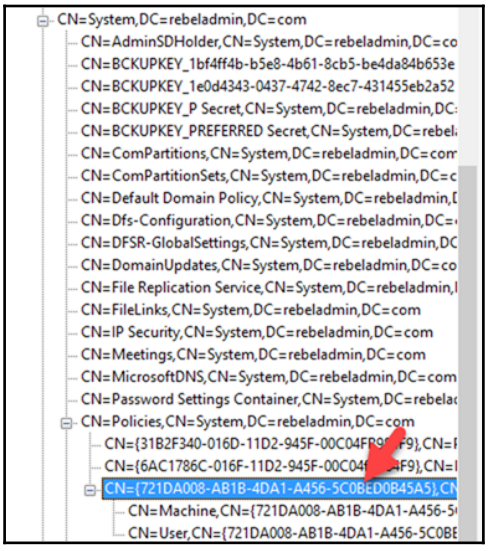

Delegation of Control Wizard
Users or Groups
Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
Asia IT Team (REBELADMIN\Asia IT Team)
Add...
Remove
< Back
Next >
Cancel
Help


Delegation of Control Wizard
Tasks to Delegate
You can select common tasks or customize your own.
Delegate the following common tasks:
Create, delete, and manage user accounts
Reset user passwords and force password change at next logon
Read all user information
Create, delete and manage groups
Modify the membership of a group
Manage Group Policy links
Generate Resultant Set of Policy (Planning)
Create a custom task to delegate
< Back
Next >
Cancel
Help


Advanced Security Settings for Asia
Owner:
Domain Admins (REBELADMIN\Domain Admins)
Change
Permissions
Auditing
Effective Access
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).
Permission entries:
Type
Principal
Access
Inherited from
Applies to
Deny Everyone Special None This obje
Allow Asia IT Team (REBELADMIN\... Create/delete User objects None This obje
Allow Account Operators (REBELA... Create/delete InetOrgPerson objects None This obje
Allow Account Operators (REBELA... Create/delete Computer objects None This obje
Allow Account Operators (REBELA... Create/delete Group objects None This obje
Allow Print Operators (REBELADMI... Create/delete Printer objects None This obje
Allow Account Operators (REBELA... Create/delete User objects None This obje
Allow Domain Admins (REBELADM... Full control None This obje
Allow ENTERPRISE DOMAIN CONT... Special None This obje
Add
Remove
Edit
Restore defaults
Disable inheritance
OK
Cancel
Apply

Chapter 10: Managing Group Policies





```
Dn: CN={721DA008-AB1B-4DA1-A456-5C0BED0B45A5},CN=Policies,CN=System,DC=rebeladmin,DC=com
    cn: {721DA008-AB1B-4DA1-A456-5C0BED0B45A5};
    displayName: Test Users;
    distinguishedName: CN={721DA008-AB1B-4DA1-
        A456-5C0BED0B45A5},CN=Policies,CN=System,DC=rebeladmin,DC=com;
    dSCorePropagationData: 0x0 = ( );
    flags: 0;
    gPCFileSysPath: \\rebeladmin.com\SysVol\rebeladmin.com\Policies\{721DA008-AB1B-4DA1-A456-5C0BED0B45A5};
    gPCFunctionalityVersion: 2;
    gPCMachineExtensionNames: [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{53D6AB1D-2488-11D1-
        A28C-00C04FB94F17}{B3408A2F-8DDA-1197-FBD5-2CE69A2DEFC0}][{B1BE8D72-6EAC-11D2-
        A4EA-00C04F79F83A}{53D6AB1D-2488-11D1-A28C-00C04FB94F17}][{FB2CA36D-0B40-4307-821B-
        A13B252DE56C}{B3408A2F-8DDA-1197-FBD5-2CE69A2DEFC0}];
    instanceType: 0x4 = ( WRITE );
    name: {721DA008-AB1B-4DA1-A456-5C0BED0B45A5};
    objectCategory: CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=rebeladmin,DC=com;
    objectClass (3): top; container; groupPolicyContainer;
    objectGUID: 27b2e0b8-bc2d-46a8-af1a-cb98a33e994c;
    showInAdvancedViewOnly: TRUE;
    uSNChanged: 37710;
    uSNCreated: 37283;
    versionNumber: 6;
    whenChanged: 25/02/2017 11:55:40 GMT Standard Time;
    whenCreated: 20/02/2017 00:18:44 GMT Standard Time;

-----------
```

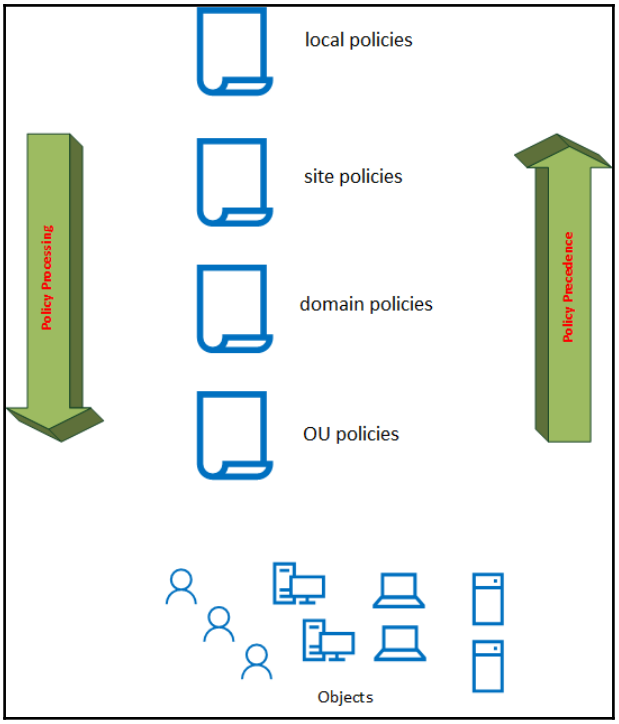
```
PS Microsoft.PowerShell.Core\FileSystem::\\rebeladmin.com\SYSVOL\rebeladmin.com\Policies\{721DA008-AB1B-4DA1-A456-5C0BED
0B45A5}> dir


    Directory: \\rebeladmin.com\SYSVOL\rebeladmin.com\Policies\{721DA008-AB1B-4DA1-A456-5C0BED0B45A5}


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        25/02/2017     11:55                Machine
d-----        20/02/2017     00:18                User
-a----        25/02/2017     11:55             59 GPT.INI
```

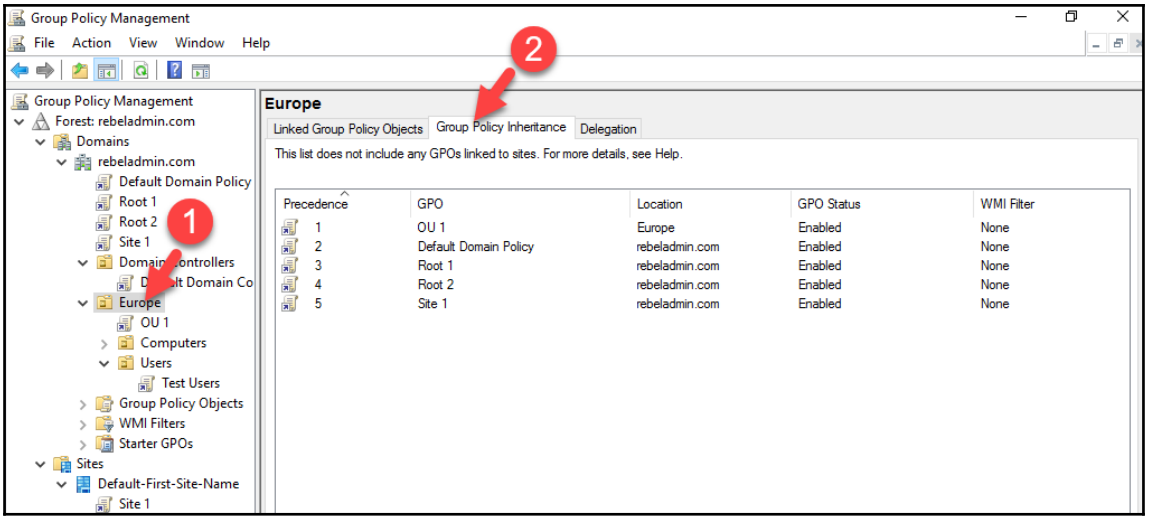
GPT - Notepad

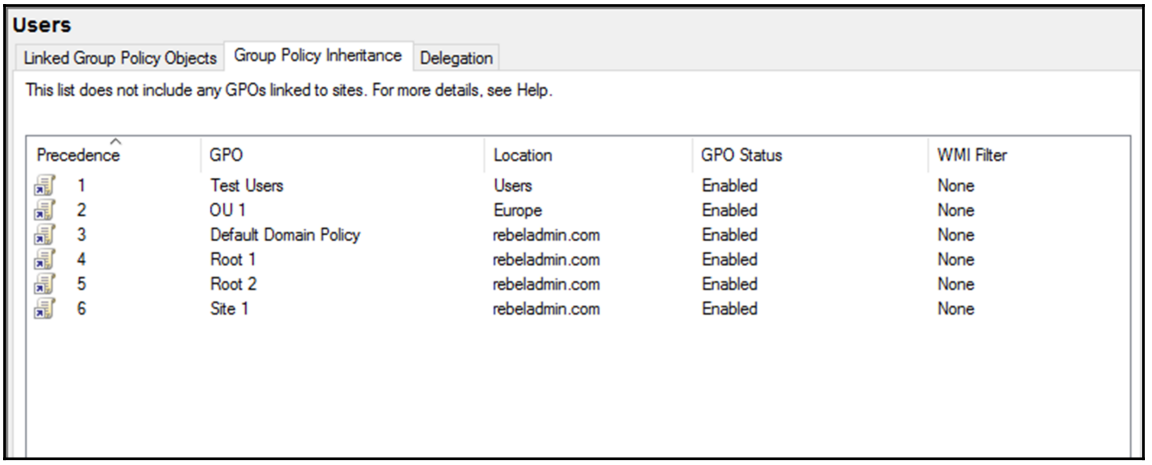
File Edit Format View Help

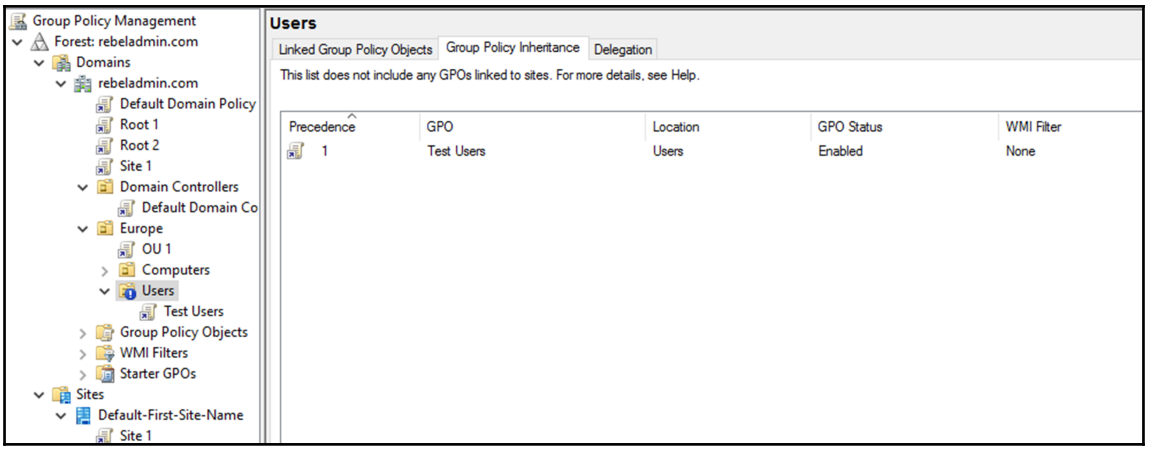
```
[General]
Version=6
displayName=New Group Policy Object
```

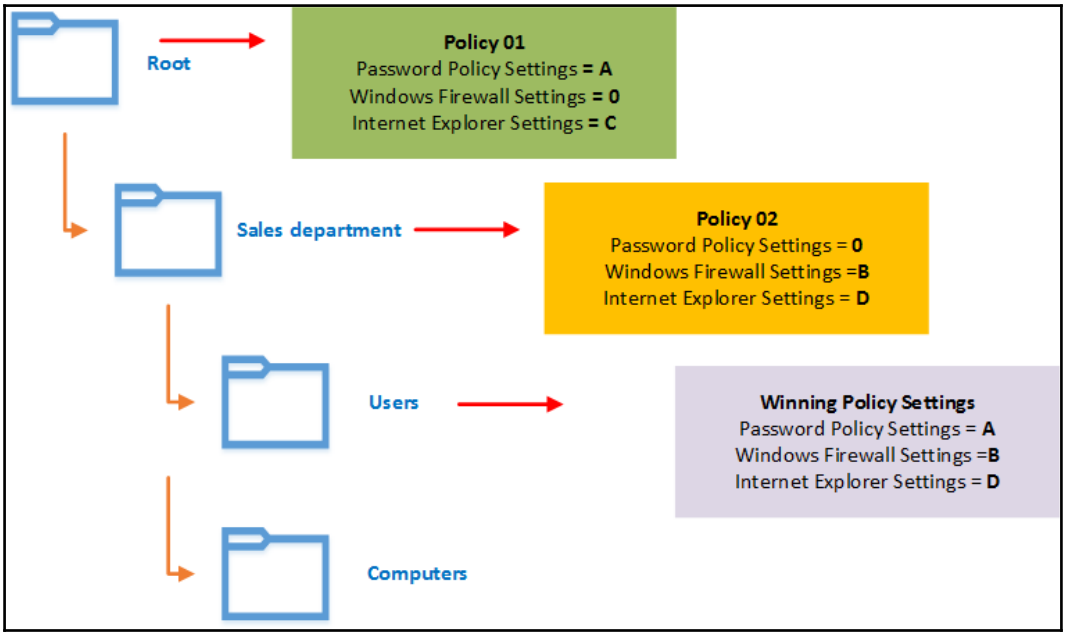
```
PS Microsoft.PowerShell.Core\FileSystem::\\rebeladmin.com\SYSVOL\rebeladmin.com\Policies\{721DA008-AB1B-4DA1-A456-5C0BED
0B45A5}\Machine> dir


    Directory: \\rebeladmin.com\SYSVOL\rebeladmin.com\Policies\{721DA008-AB1B-4DA1-A456-5C0BED0B45A5}\Machine


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        25/02/2017     09:52                Applications
d-----        25/02/2017     09:53                Microsoft
d-----        25/02/2017     09:52                Scripts
-a----        25/02/2017     11:55           8046 Registry.pol


PS Microsoft.PowerShell.Core\FileSystem::\\rebeladmin.com\SYSVOL\rebeladmin.com\Policies\{721DA008-AB1B-4DA1-A456-5C0BED
0B45A5}\Machine> cd ..
PS Microsoft.PowerShell.Core\FileSystem::\\rebeladmin.com\SYSVOL\rebeladmin.com\Policies\{721DA008-AB1B-4DA1-A456-5C0BED
0B45A5}> cd User
PS Microsoft.PowerShell.Core\FileSystem::\\rebeladmin.com\SYSVOL\rebeladmin.com\Policies\{721DA008-AB1B-4DA1-A456-5C0BED
0B45A5}\User> dir


    Directory: \\rebeladmin.com\SYSVOL\rebeladmin.com\Policies\{721DA008-AB1B-4DA1-A456-5C0BED0B45A5}\User


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        25/02/2017     12:35                Applications
d-----        25/02/2017     12:17                Documents & Settings
d-----        25/02/2017     12:17                Scripts
```

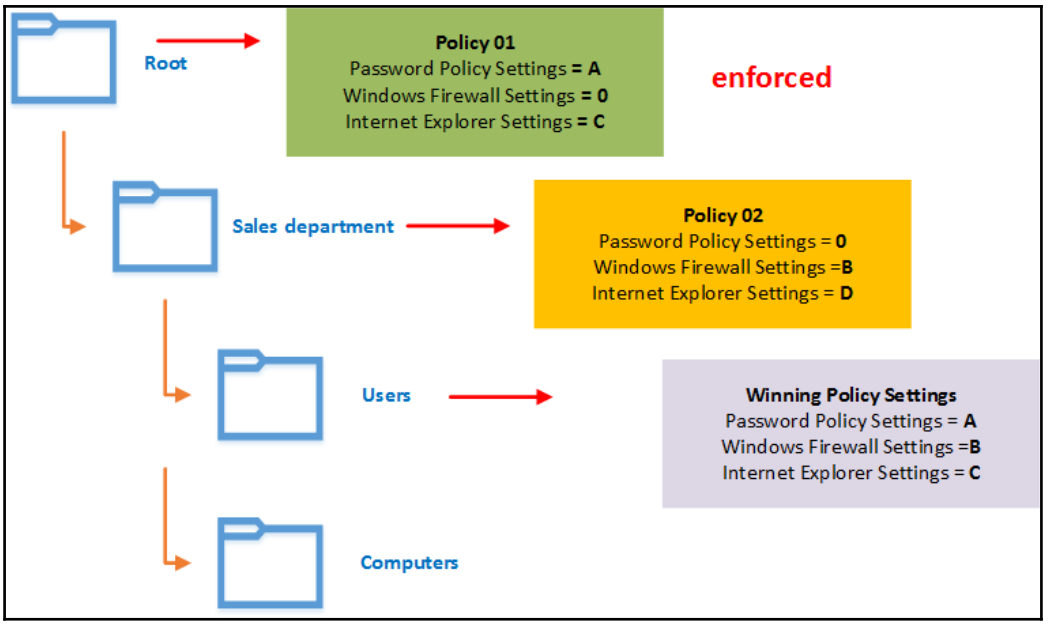


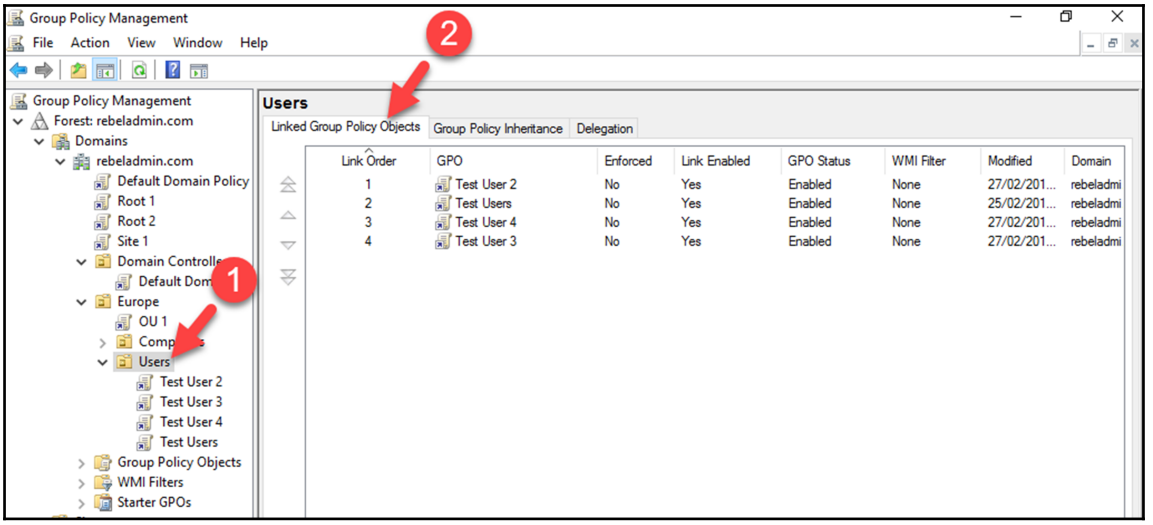

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: rebeladmin.com
Domains
rebeladmin.com
Default Domain Policy
Root 1
Root 2
Site 1
Domain Controllers
Europe
OU 1
Computers
Users
Test Users
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Default-First-Site-Name
Site 1
1
2
Europe
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This list does not include any GPOs linked to sites. For more details, see Help.
Precedence
GPO
Location
GPO Status
WMI Filter
1 OU 1 Europe Enabled None
2 Default Domain Policy rebeladmin.com Enabled None
3 Root 1 rebeladmin.com Enabled None
4 Root 2 rebeladmin.com Enabled None
5 Site 1 rebeladmin.com Enabled None

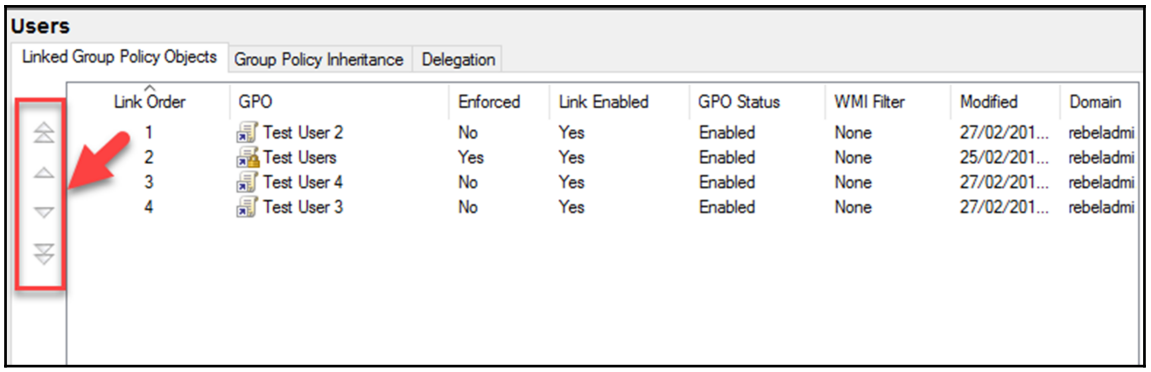

Users
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This list does not include any GPOs linked to sites. For more details, see Help.
Precedence
GPO
Location
GPO Status
WMI Filter
1 Test Users Users Enabled None
2 OU 1 Europe Enabled None
3 Default Domain Policy rebeladmin.com Enabled None
4 Root 1 rebeladmin.com Enabled None
5 Root 2 rebeladmin.com Enabled None
6 Site 1 rebeladmin.com Enabled None

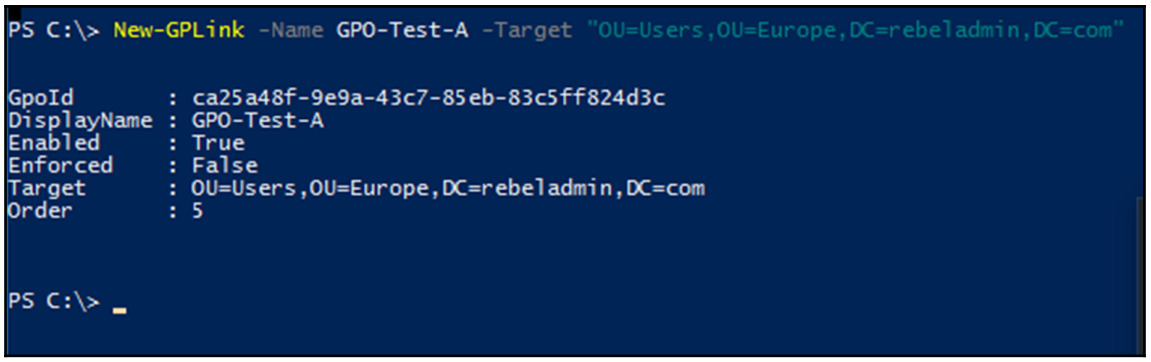

Group Policy Management
Forest: rebeladmin.com
Domains
rebeladmin.com
Default Domain Policy
Root 1
Root 2
Site 1
Domain Controllers
Default Domain Co
Europe
OU 1
Computers
Users
Test Users
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Default-First-Site-Name
Site 1
Users
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This list does not include any GPOs linked to sites. For more details, see Help.
Precedence
GPO
Location
GPO Status
WMI Filter
1
Test Users
Users
Enabled
None

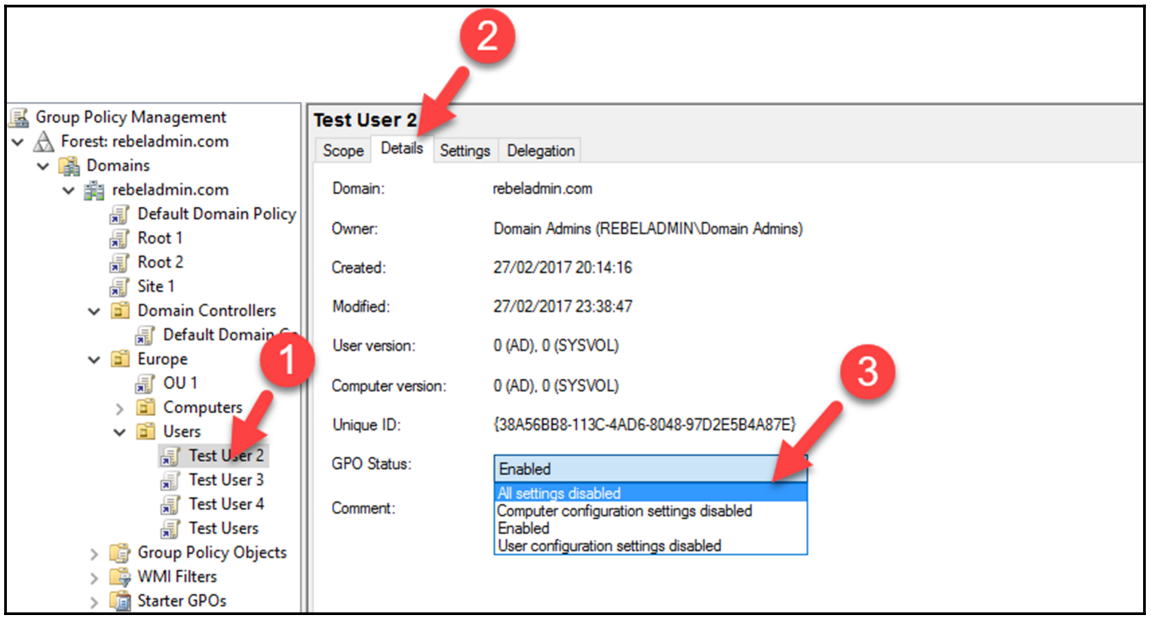

Root
Policy 01
Password Policy Settings = A
Windows Firewall Settings = 0
Internet Explorer Settings = C
Sales department
Policy 02
Password Policy Settings = 0
Windows Firewall Settings =B
Internet Explorer Settings = D
Users
Winning Policy Settings
Password Policy Settings = A
Windows Firewall Settings =B
Internet Explorer Settings = D
Computers

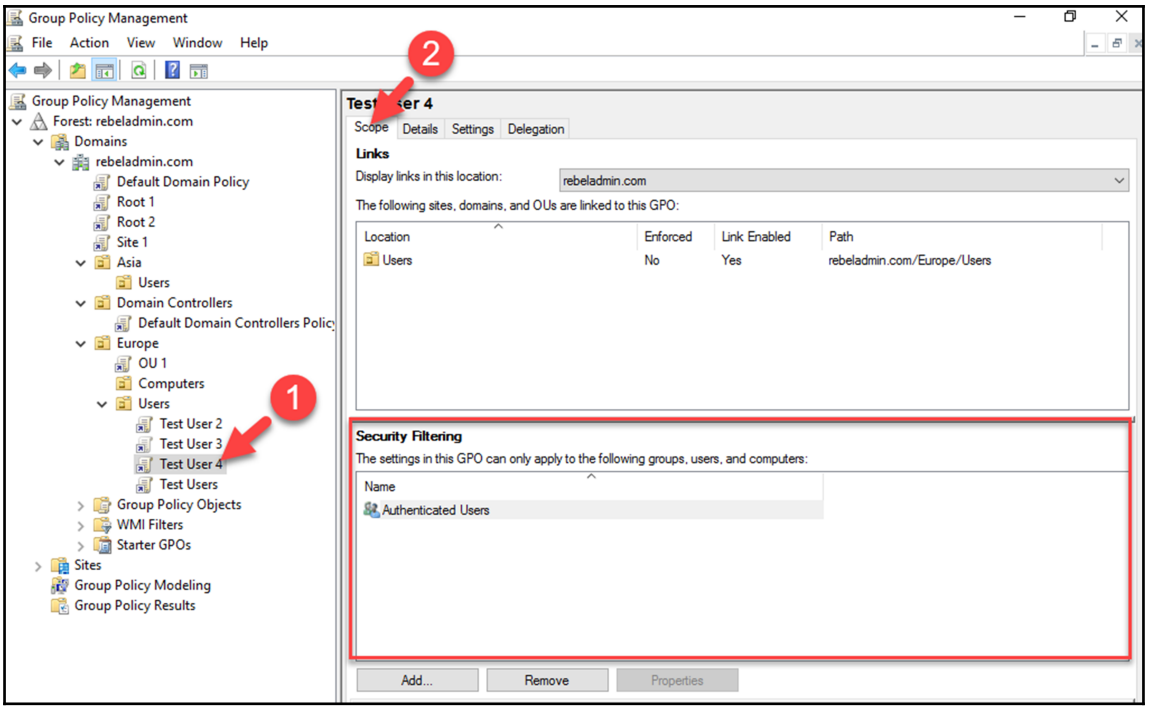

Root
Policy 01
Password Policy Settings = A
Windows Firewall Settings = 0
Internet Explorer Settings = C
enforced
Sales department
Policy 02
Password Policy Settings = 0
Windows Firewall Settings =B
Internet Explorer Settings = D
Users
Winning Policy Settings
Password Policy Settings = A
Windows Firewall Settings =B
Internet Explorer Settings = C
Computers

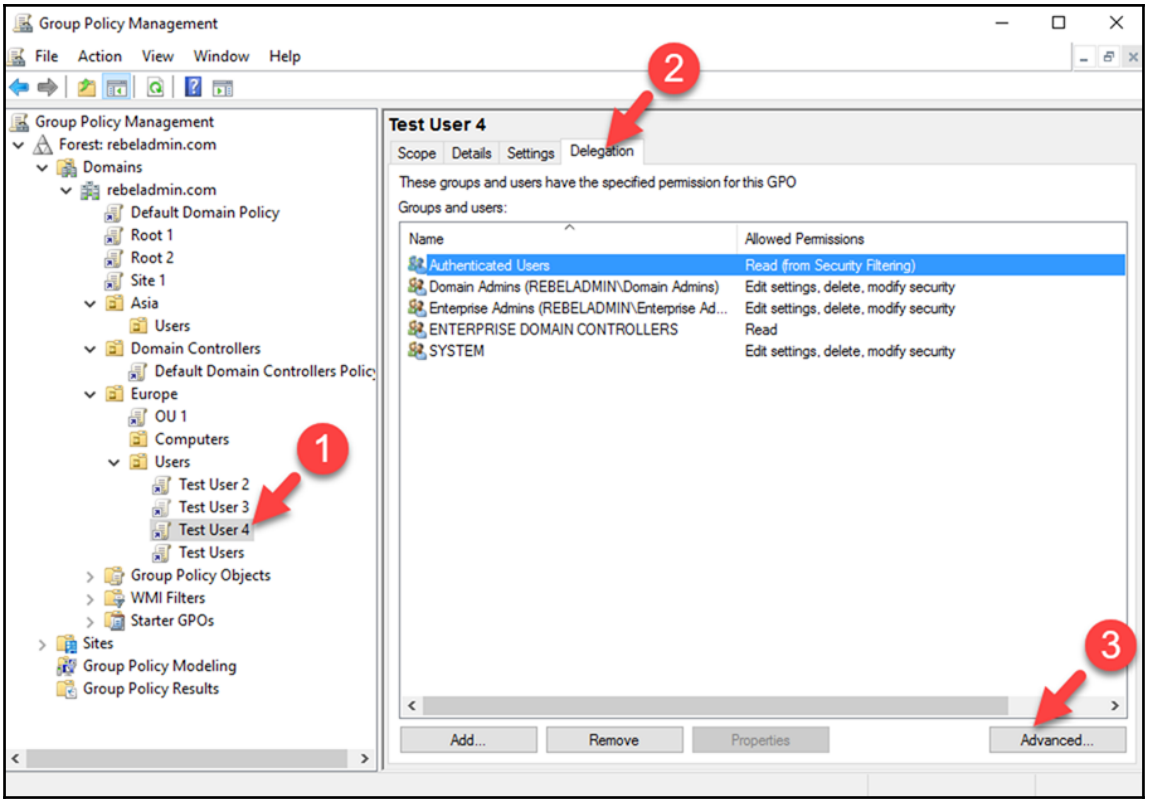

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: rebeladmin.com
Domains
rebeladmin.com
Default Domain Policy
Root 1
Root 2
Site 1
Domain Controllers
Default Dom
Europe
OU 1
Comp
Users
Test User 2
Test User 3
Test User 4
Test Users
Group Policy Objects
WMI Filters
Starter GPOs
1
2
Users
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
WMI Filter
Modified
Domain
1 Test User 2 No Yes Enabled None 27/02/201... rebeladmi
2 Test Users No Yes Enabled None 25/02/201... rebeladmi
3 Test User 4 No Yes Enabled None 27/02/201... rebeladmi
4 Test User 3 No Yes Enabled None 27/02/201... rebeladmi

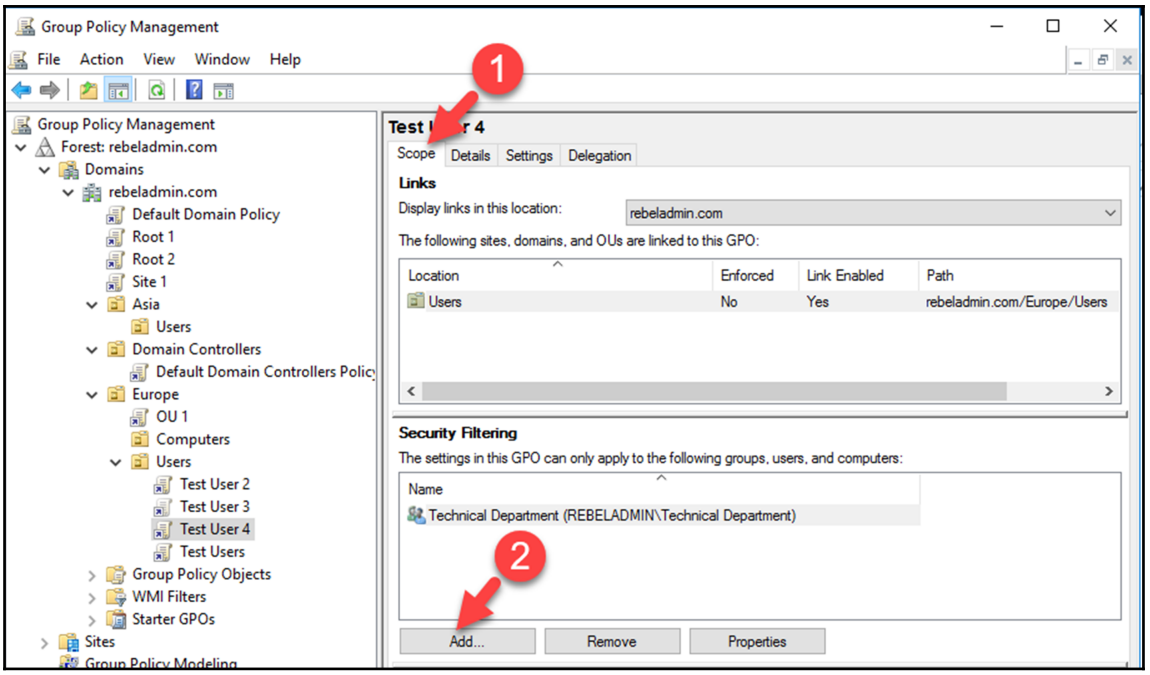

Users
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
WMI Filter
Modified
Domain
1 Test User 2 No Yes Enabled None 27/02/201... rebeladmi
2 Test Users Yes Yes Enabled None 25/02/201... rebeladmi
3 Test User 4 No Yes Enabled None 27/02/201... rebeladmi
4 Test User 3 No Yes Enabled None 27/02/201... rebeladmi

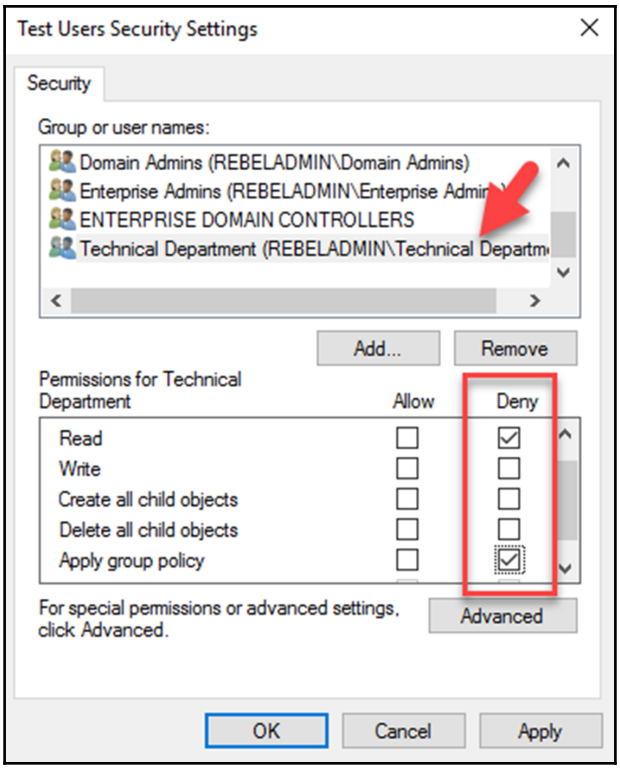

PS C:\> New-GPLink -Name GPO-Test-A -Target "OU=Users,OU=Europe,DC=rebeladmin,DC=com"
GpoId : ca25a48f-9e9a-43c7-85eb-83c5ff824d3c
DisplayName : GPO-Test-A
Enabled : True
Enforced : False
Target : OU=Users,OU=Europe,DC=rebeladmin,DC=com
Order : 5
PS C:\>

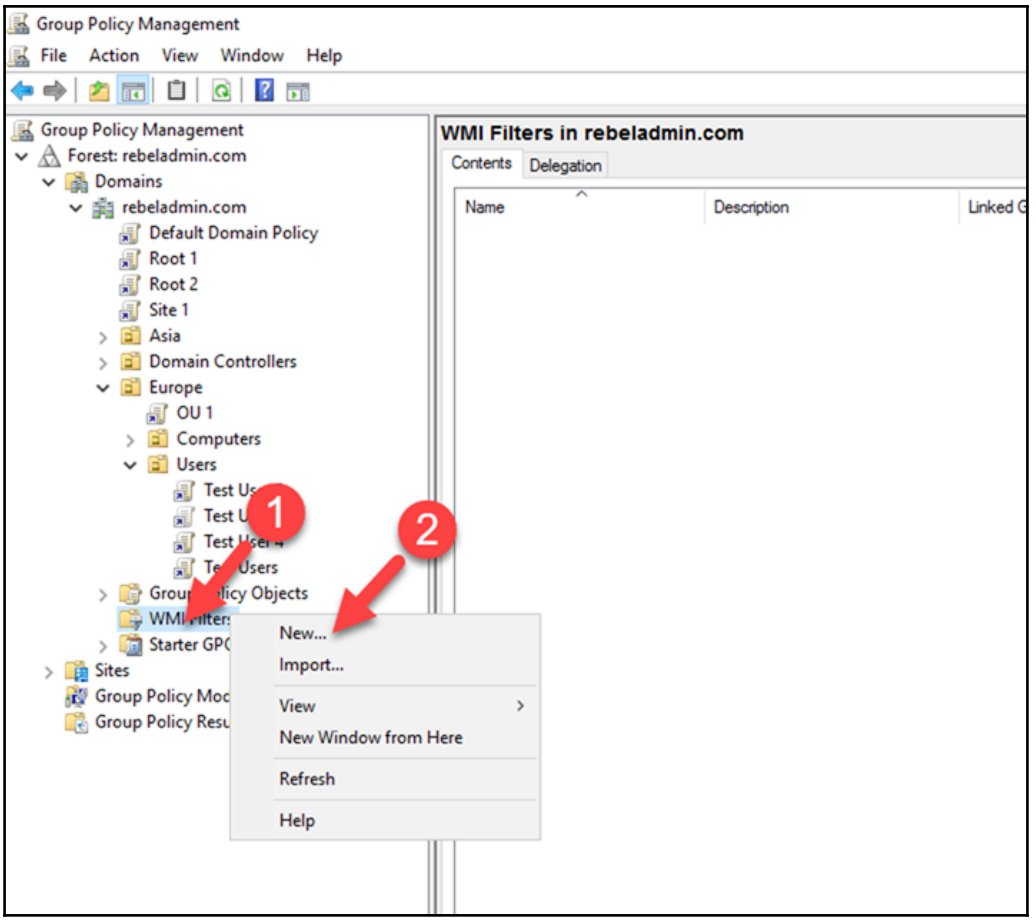

Group Policy Management
Forest: rebeladmin.com
Domains
rebeladmin.com
Default Domain Policy
Root 1
Root 2
Site 1
Domain Controllers
Europe
OU 1
Computers
Users
Test User 2
Test User 3
Test User 4
Test Users
Group Policy Objects
WMI Filters
Starter GPOs
1
2
3
Test User 2
Scope
Details
Settings
Delegation
Domain: rebeladmin.com
Owner: Domain Admins (REBELADMIN\Domain Admins)
Created: 27/02/2017 20:14:16
Modified: 27/02/2017 23:38:47
User version: 0 (AD), 0 (SYSVOL)
Computer version: 0 (AD), 0 (SYSVOL)
Unique ID: {38A56BB8-113C-4AD6-8048-97D2E5B4A87E}
GPO Status: Enabled
Comment:
All settings disabled
Computer configuration settings disabled
Enabled
User configuration settings disabled

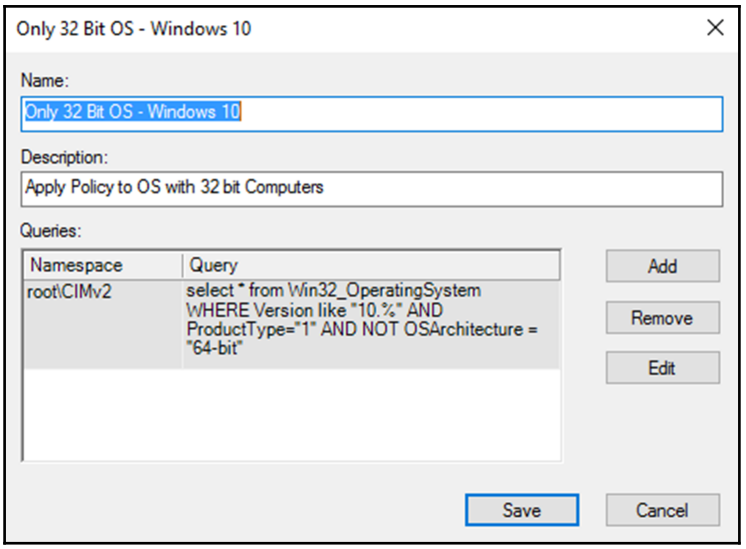

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: rebeladmin.com
Domains
rebeladmin.com
Default Domain Policy
Root 1
Root 2
Site 1
Asia
Users
Domain Controllers
Default Domain Controllers Policy
Europe
OU 1
Computers
Users
Test User 2
Test User 3
Test User 4
Test Users
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
1
2
Scope
Details
Settings
Delegation
Links
Display links in this location:
rebeladmin.com
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
Users
No
Yes
rebeladmin.com/Europe/Users
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties

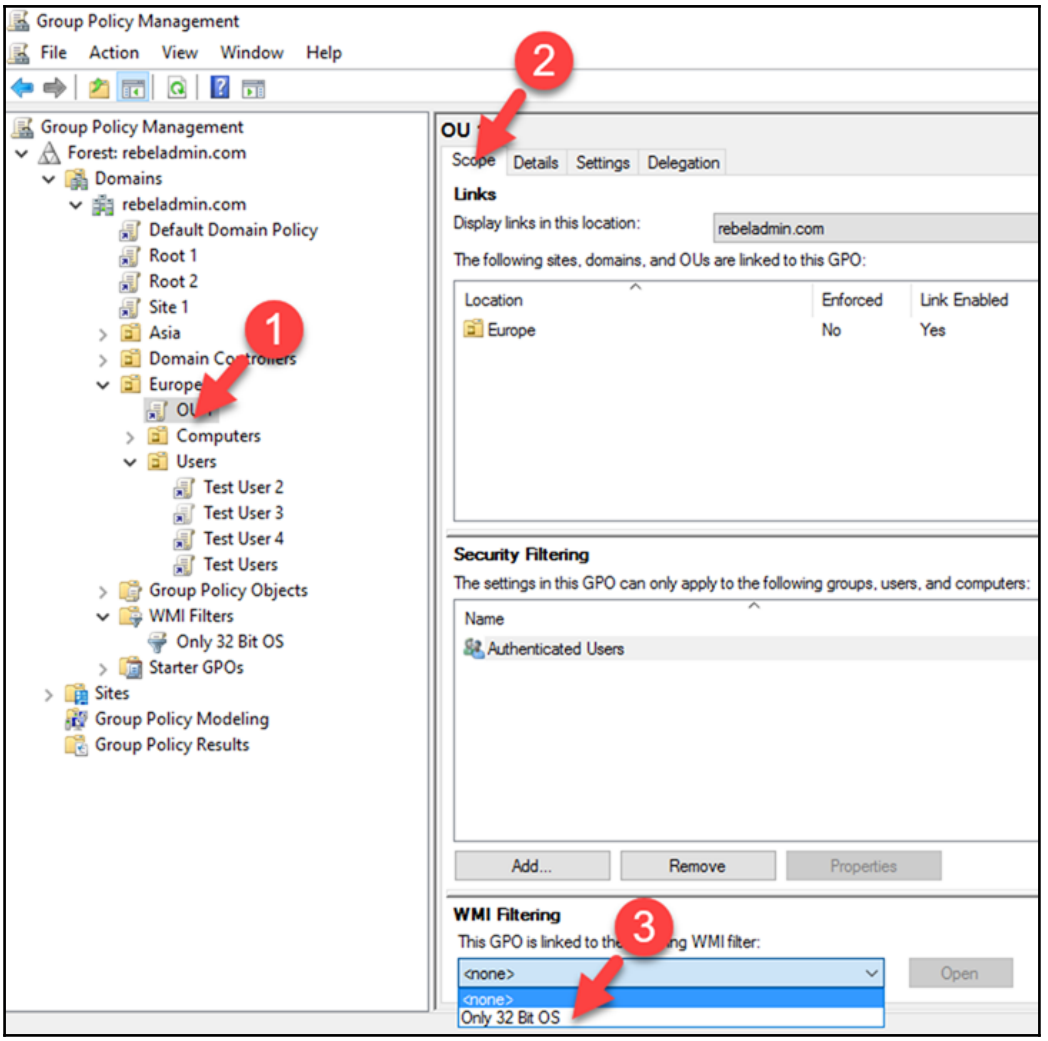

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: rebeladmin.com
Domains
rebeladmin.com
Default Domain Policy
Root 1
Root 2
Site 1
Asia
Users
Domain Controllers
Default Domain Controllers Policy
Europe
OU 1
Computers
Users
Test User 2
Test User 3
Test User 4
Test Users
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
1
2
Test User 4
Scope Details Settings Delegation
These groups and users have the specified permission for this GPO
Groups and users:
Name
Allowed Permissions
Authenticated Users
Read (from Security Filtering)
Domain Admins (REBELADMIN\Domain Admins)
Edit settings, delete, modify security
Enterprise Admins (REBELADMIN\Enterprise Ad...
Edit settings, delete, modify security
ENTERPRISE DOMAIN CONTROLLERS
Read
SYSTEM
Edit settings, delete, modify security
3
Add...
Remove
Properties
Advanced...

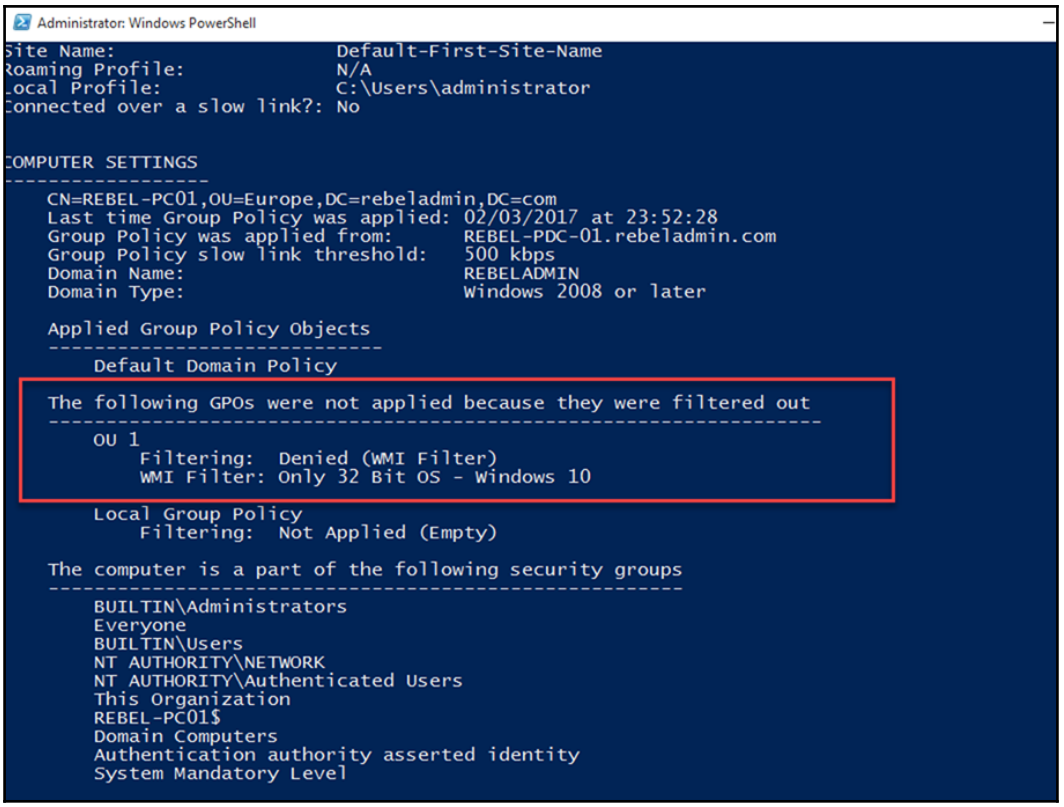

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: rebeladmin.com
Domains
rebeladmin.com
Default Domain Policy
Root 1
Root 2
Site 1
Asia
Users
Domain Controllers
Default Domain Controllers Policy
Europe
OU 1
Computers
Users
Test User 2
Test User 3
Test User 4
Test Users
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Scope
Details
Settings
Delegation
Links
Display links in this location:
rebeladmin.com
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
Users
No
Yes
rebeladmin.com/Europe/Users
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Technical Department (REBELADMIN\Technical Department)
Add...
Remove
Properties
1
2

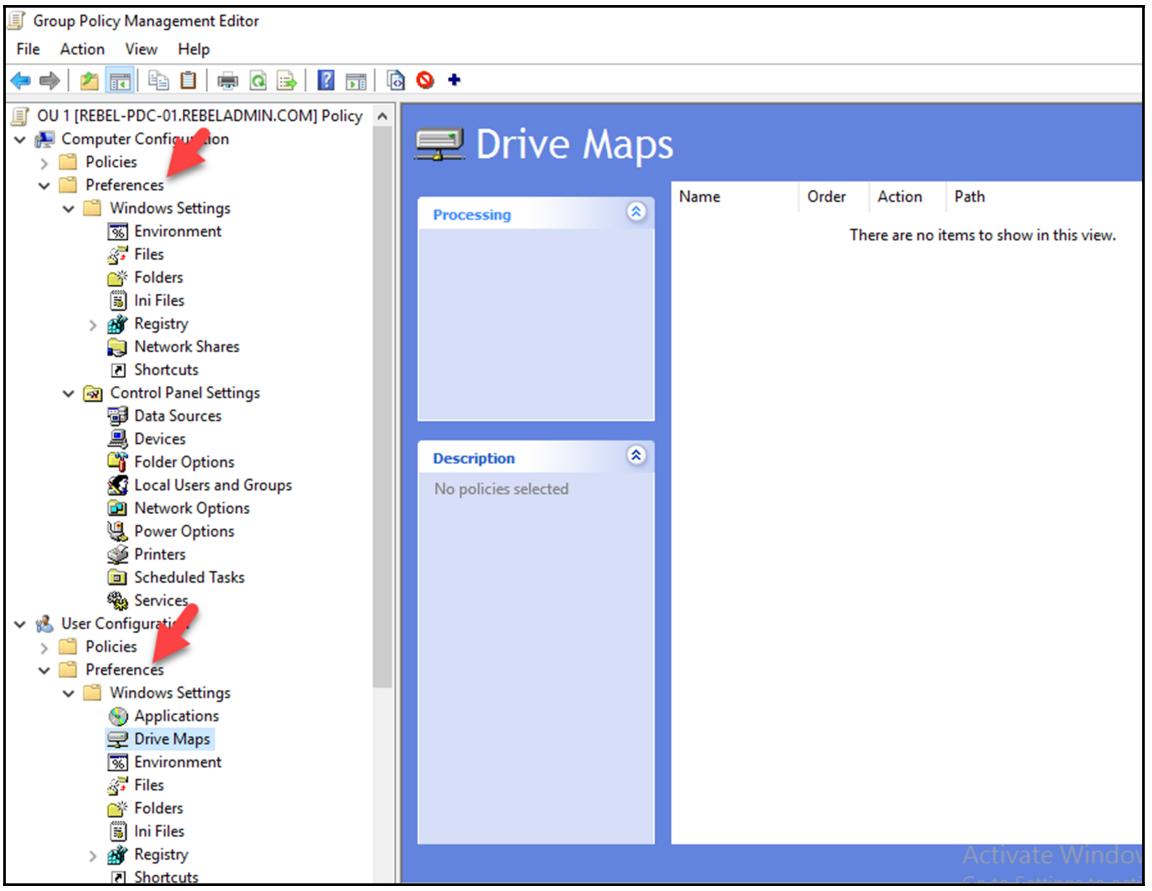

Test Users Security Settings
Security
Group or user names:
Domain Admins (REBELADMIN\Domain Admins)
Enterprise Admins (REBELADMIN\Enterprise Admin
ENTERPRISE DOMAIN CONTROLLERS
Technical Department (REBELADMIN\Technical Departm
Add...
Remove
Permissions for Technical Department
Allow
Deny
Read
Write
Create all child objects
Delete all child objects
Apply group policy
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

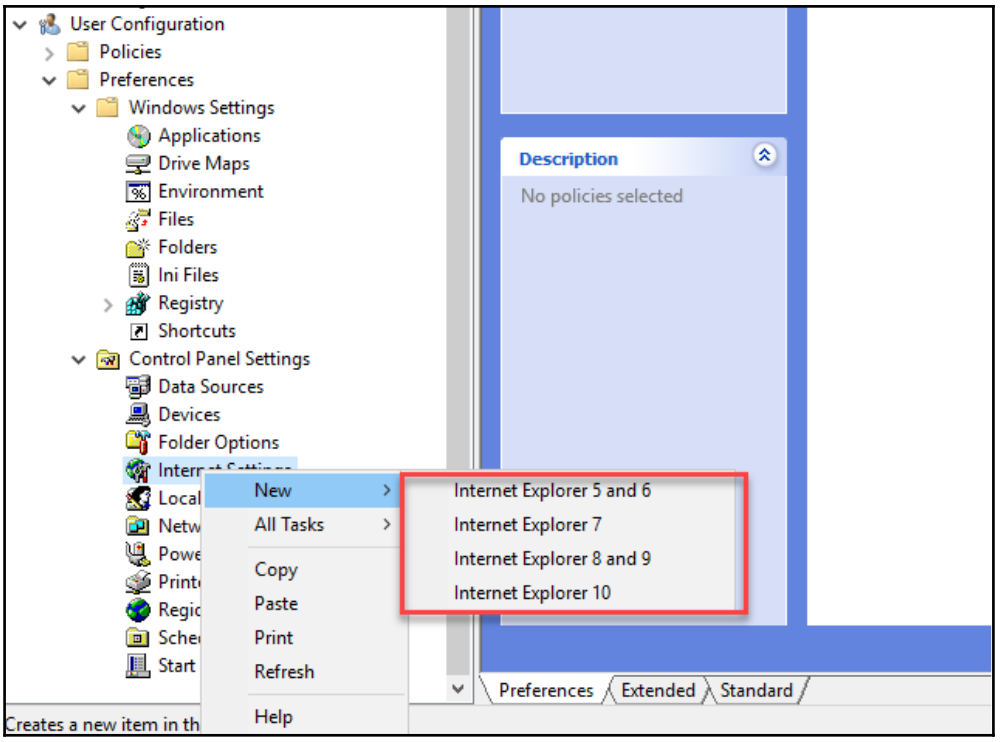

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: rebeladmin.com
Domains
rebeladmin.com
Default Domain Policy
Root 1
Root 2
Site 1
Asia
Domain Controllers
Europe
OU 1
Computers
Users
Sites
WMI Filters in rebeladmin.com
Contents
Delegation
Name
Description
1
2
New...
Import...
View
New Window from Here
Refresh
Help

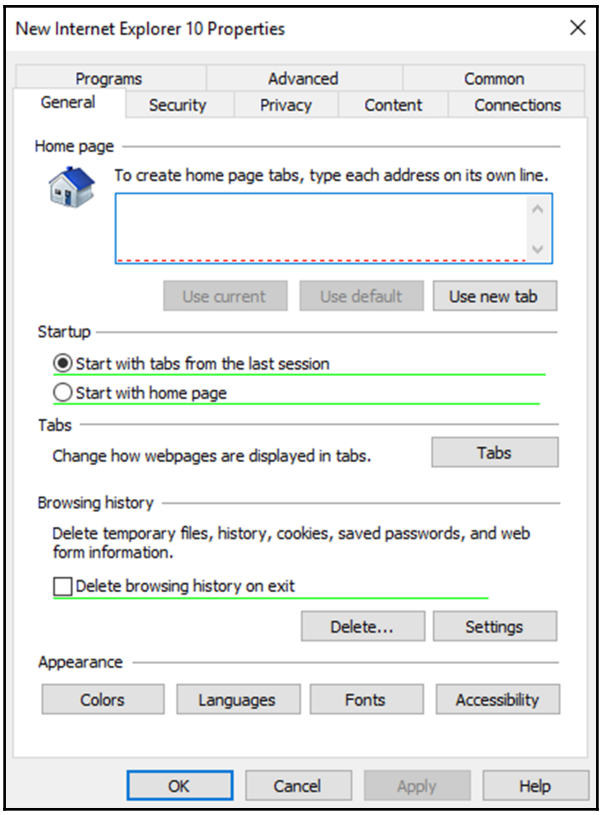

Only 32 Bit OS - Windows 10
Name:
Only 32 Bit OS - Windows 10
Description:
Apply Policy to OS with 32 bit Computers
Queries:
Namespace
Query
root\CIMv2
select * from Win32_OperatingSystem WHERE Version like "10.%" AND ProductType="1" AND NOT OSArchitecture = "64-bit"
Add
Remove
Edit
Save
Cancel

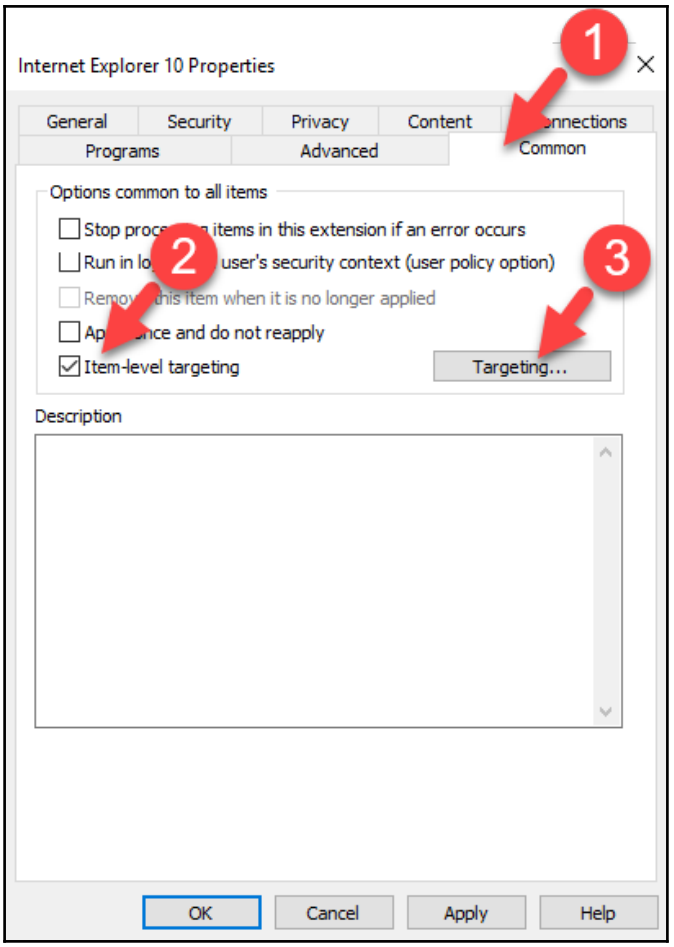

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: rebeladmin.com
Domains
rebeladmin.com
Default Domain Policy
Root 1
Root 2
Site 1
Asia
Europe
Computers
Users
Test User 2
Test User 3
Test User 4
Test Users
Group Policy Objects
WMI Filters
Only 32 Bit OS
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
1
2
3
Scope
Details
Settings
Delegation
Links
Display links in this location:
rebeladmin.com
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Europe
No
Yes
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties
WMI Filtering
<none>
Open
<none>
Only 32 Bit OS

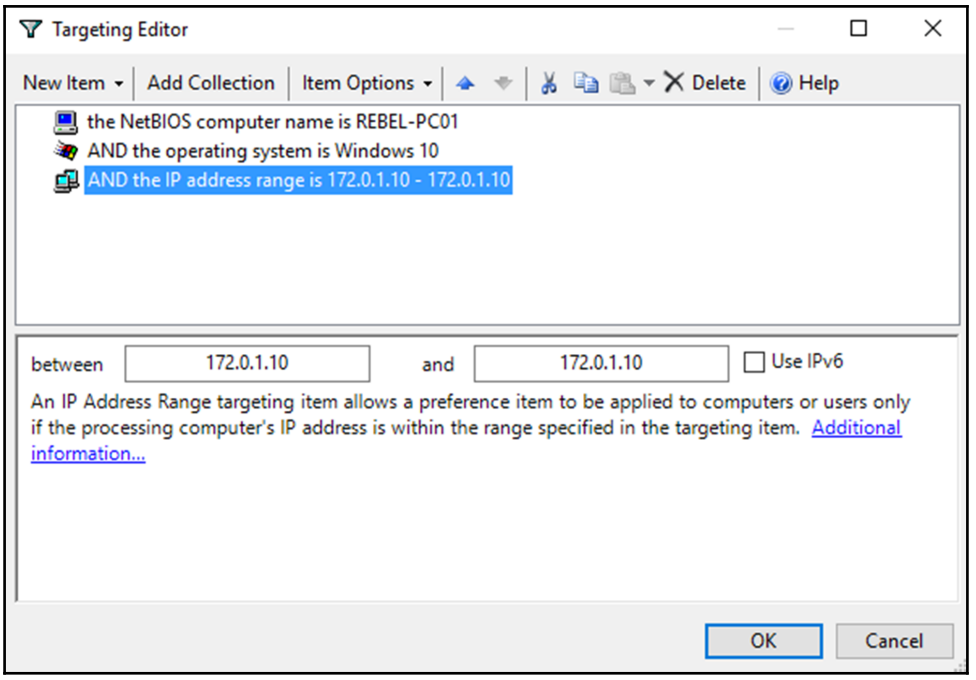

Administrator: Windows PowerShell
Site Name: Default-First-Site-Name
Roaming Profile: N/A
Local Profile: C:\Users\administrator
Connected over a slow link?: No
COMPUTER SETTINGS
CN=REBEL-PC01,OU=Europe,DC=rebeladmin,DC=com
Last time Group Policy was applied: 02/03/2017 at 23:52:28
Group Policy was applied from: REBEL-PDC-01.rebeladmin.com
Group Policy slow link threshold: 500 kbps
Domain Name: REBELADMIN
Domain Type: Windows 2008 or later
Applied Group Policy Objects
Default Domain Policy
The following GPOs were not applied because they were filtered out
OU 1
Filtering: Denied (WMI Filter)
WMI Filter: Only 32 Bit OS - Windows 10
Local Group Policy
Filtering: Not Applied (Empty)
The computer is a part of the following security groups
BUILTIN\Administrators
Everyone
BUILTIN\Users
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
This Organization
REBEL-PC01$
Domain Computers
Authentication authority asserted identity
System Mandatory Level

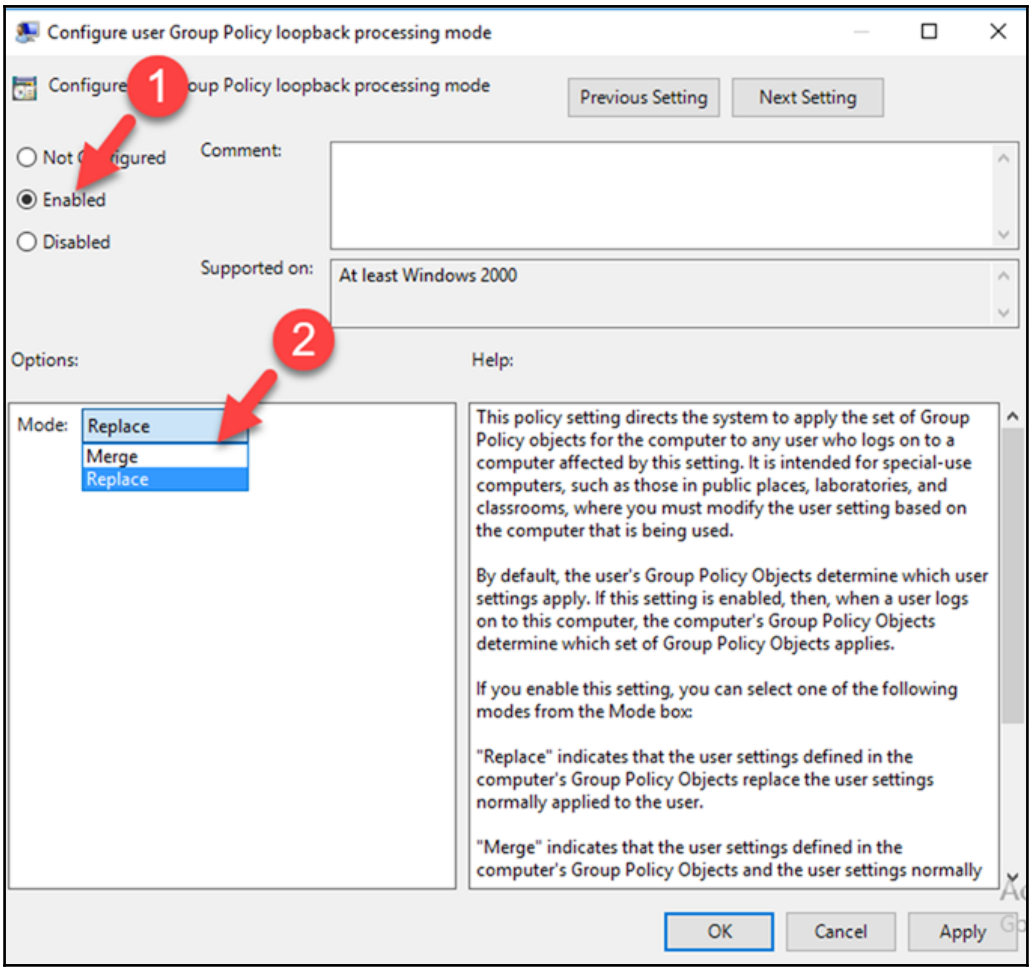

Group Policy Management Editor
File Action View Help
OU 1 [REBEL-PDC-01.REBELADMIN.COM] Policy
Computer Configuration
Policies
Preferences
Windows Settings
Environment
Files
Folders
Ini Files
Registry
Network Shares
Shortcuts
Control Panel Settings
Data Sources
Devices
Folder Options
Local Users and Groups
Network Options
Power Options
Printers
Scheduled Tasks
Services
User Configuration
Policies
Preferences
Windows Settings
Applications
Drive Maps
Environment
Files
Folders
Ini Files
Registry
Shortcuts
Drive Maps
Processing
Description
No policies selected
Name
Order
Action
Path
There are no items to show in this view.

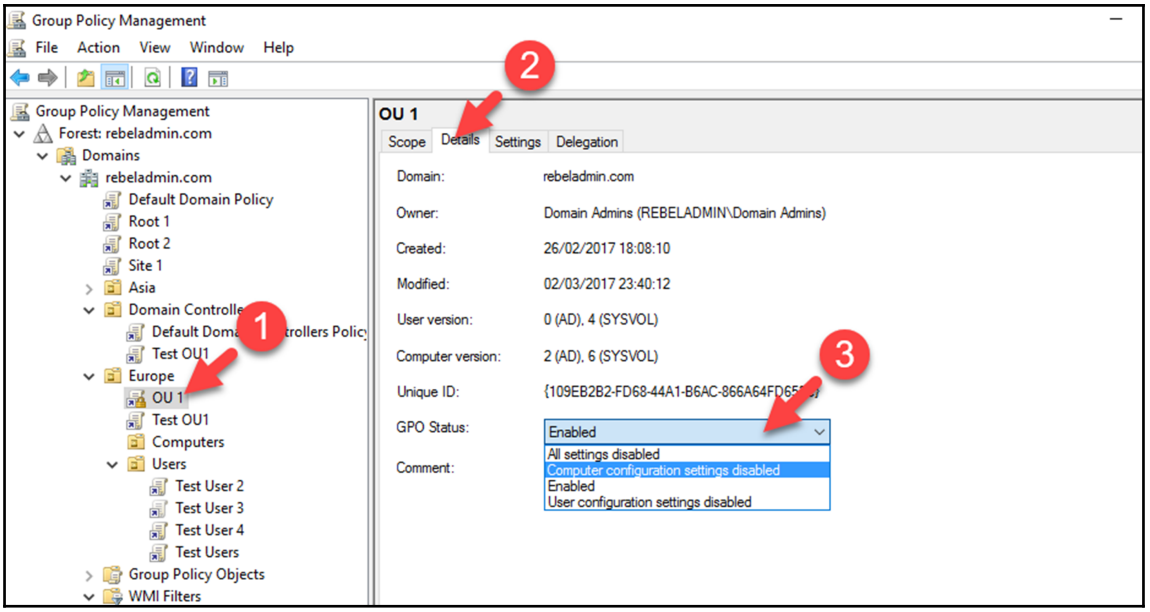

User Configuration
Policies
Preferences
Windows Settings
Applications
Drive Maps
Environment
Files
Folders
Ini Files
Registry
Shortcuts
Control Panel Settings
Data Sources
Devices
Folder Options
New
All Tasks
Copy
Paste
Print
Refresh
Help
Internet Explorer 5 and 6
Internet Explorer 7
Internet Explorer 8 and 9
Internet Explorer 10
Description
No policies selected
Preferences
Extended
Standard
Creates a new item in th


New Internet Explorer 10 Properties
Programs
Advanced
Common
General
Security
Privacy
Content
Connections
Home page
To create home page tabs, type each address on its own line.
Use current
Use default
Use new tab
Startup
Start with tabs from the last session
Start with home page
Tabs
Change how webpages are displayed in tabs.
Tabs
Browsing history
Delete temporary files, history, cookies, saved passwords, and web form information.
Delete browsing history on exit
Delete...
Settings
Appearance
Colors
Languages
Fonts
Accessibility
OK
Cancel
Apply
Help

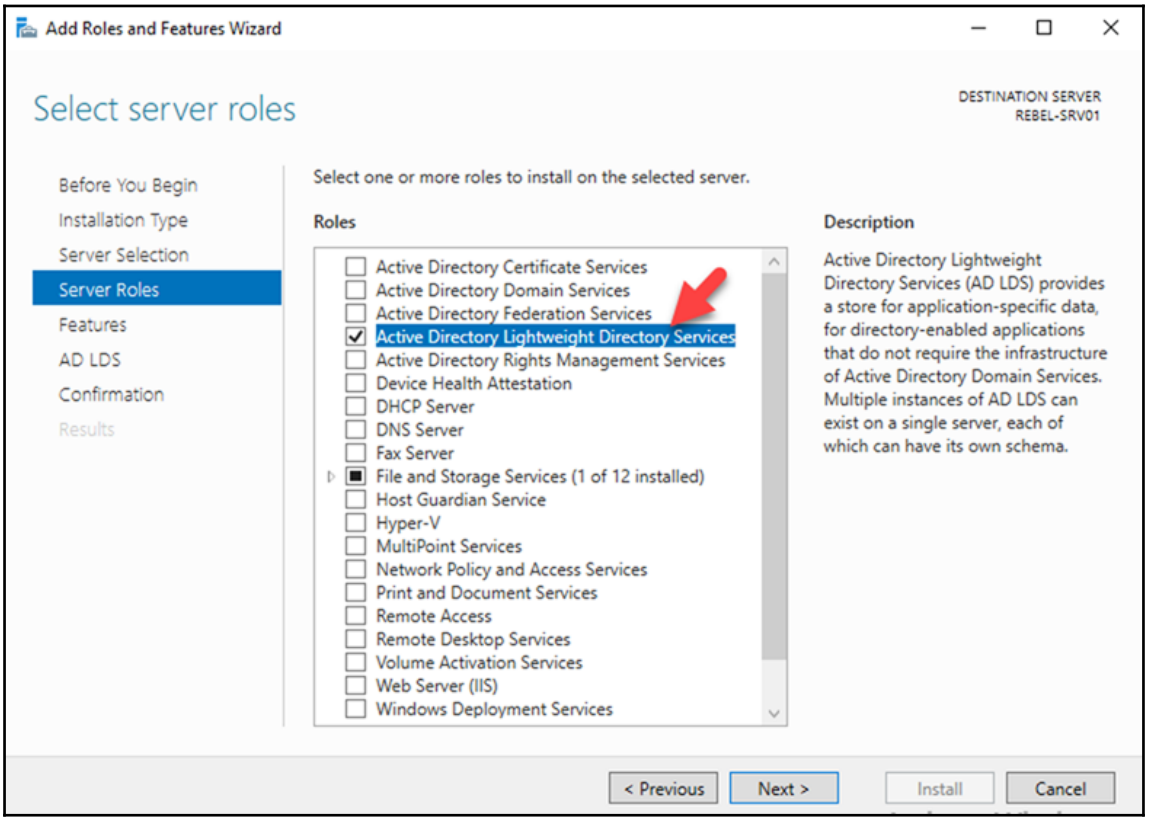

Internet Explorer 10 Properties
1
General
Security
Privacy
Content
Programs
Advanced
Common
Options common to all items
2
3
Item-level targeting
Targeting...
Description
OK
Cancel
Apply
Help

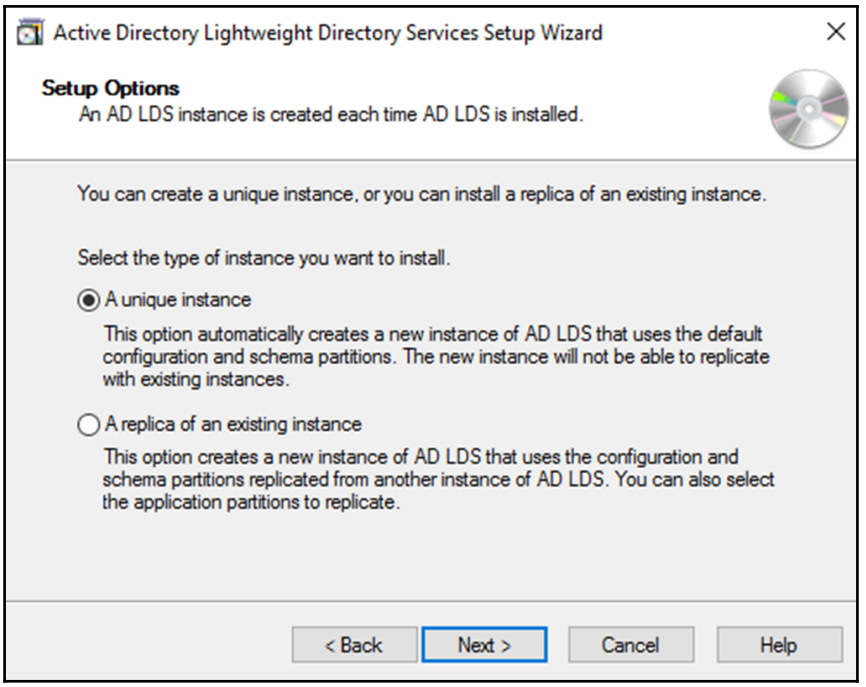

Targeting Editor
New Item
Add Collection
Item Options
Delete
Help
the NetBIOS computer name is REBEL-PC01
AND the operating system is Windows 10
AND the IP address range is 172.0.1.10 - 172.0.1.10
between
172.0.1.10
and
172.0.1.10
Use IPv6
An IP Address Range targeting item allows a preference item to be applied to computers or users only if the processing computer's IP address is within the range specified in the targeting item. Additional information...
OK
Cancel

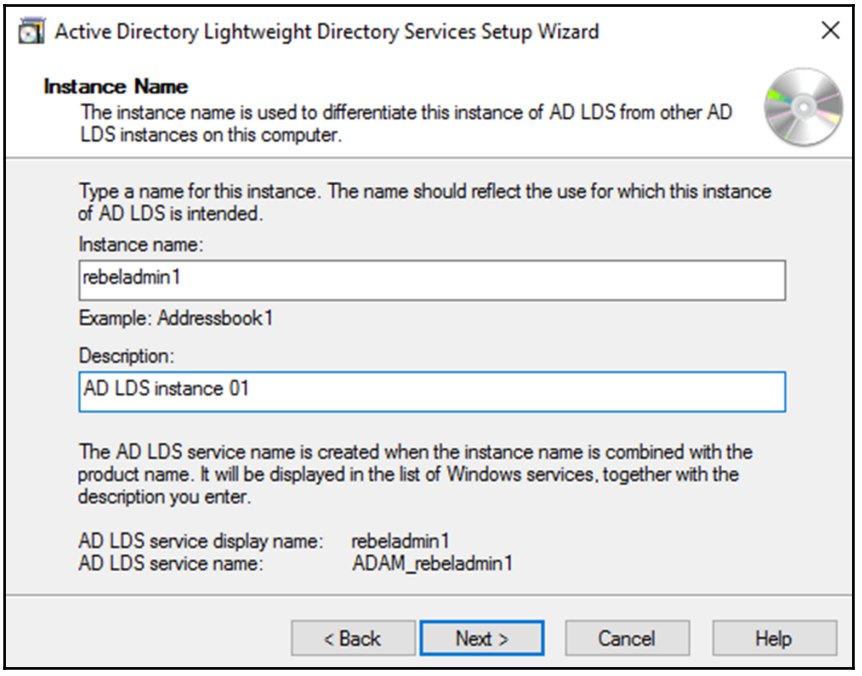

Configure user Group Policy loopback processing mode
Configure oup Policy loopback processing mode
Previous Setting
Next Setting
1
Not C igured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000
2
Options:
Help:
Mode:
Replace
Merge
Replace
This policy setting directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this setting. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user setting based on the computer that is being used.
By default, the user's Group Policy Objects determine which user settings apply. If this setting is enabled, then, when a user logs on to this computer, the computer's Group Policy Objects determine which set of Group Policy Objects applies.
If you enable this setting, you can select one of the following modes from the Mode box:
"Replace" indicates that the user settings defined in the computer's Group Policy Objects replace the user settings normally applied to the user.
"Merge" indicates that the user settings defined in the computer's Group Policy Objects and the user settings normally
OK
Cancel
Apply

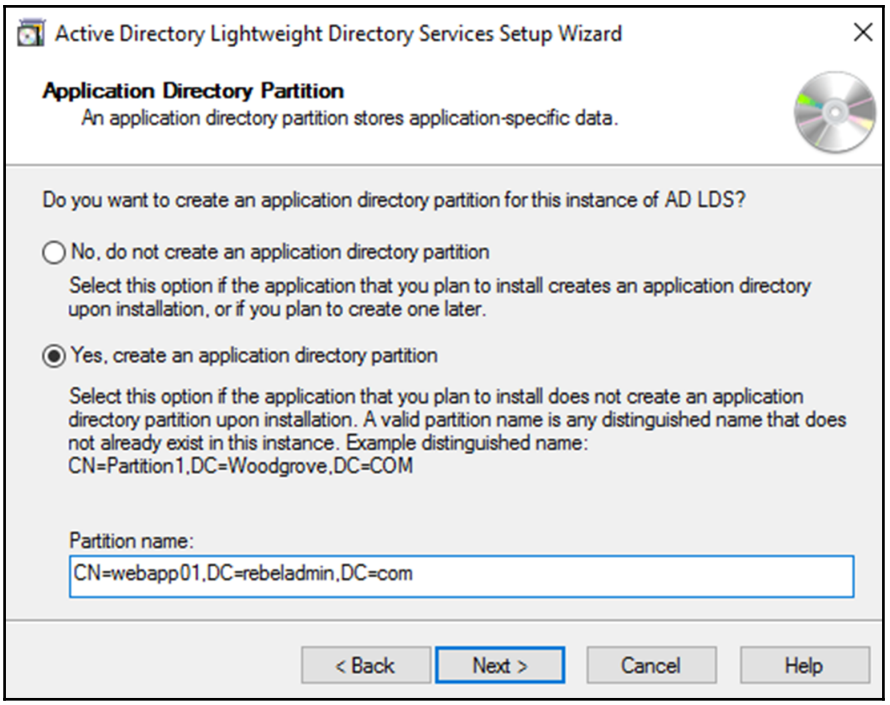

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: rebeladmin.com
Domains
rebeladmin.com
Default Domain Policy
Root 1
Root 2
Site 1
Asia
Domain Controlle
Default Dom trollers Policy
Test OU1
Europe
OU 1
Test OU1
Computers
Users
Test User 2
Test User 3
Test User 4
Test Users
Group Policy Objects
WMI Filters
1
2
3
OU 1
Scope Details Settings Delegation
Domain: rebeladmin.com
Owner: Domain Admins (REBELADMIN\Domain Admins)
Created: 26/02/2017 18:08:10
Modified: 02/03/2017 23:40:12
User version: 0 (AD), 4 (SYSVOL)
Computer version: 2 (AD), 6 (SYSVOL)
Unique ID:
GPO Status: Enabled
Comment:
All settings disabled
Computer configuration settings disabled
Enabled
User configuration settings disabled

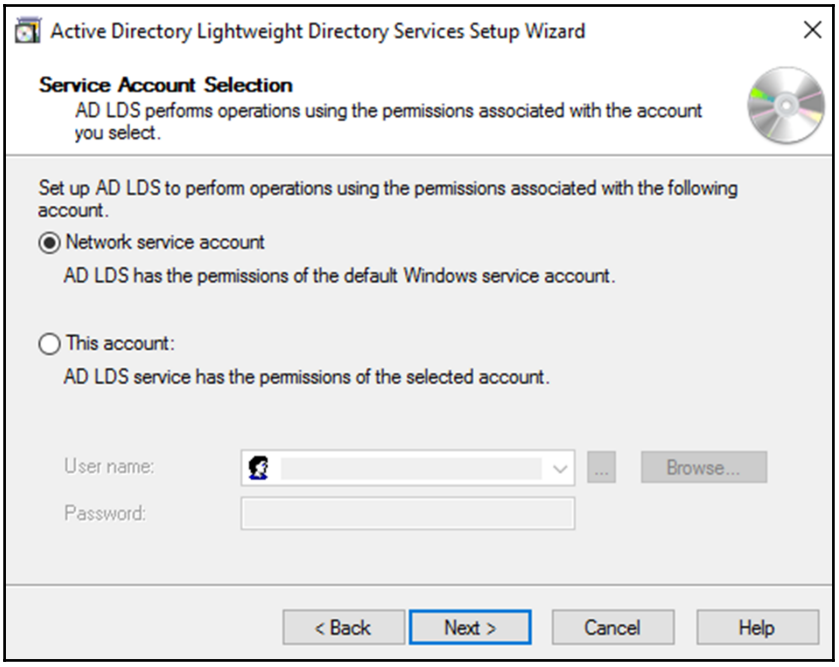
Chapter 11: Active Directory Services

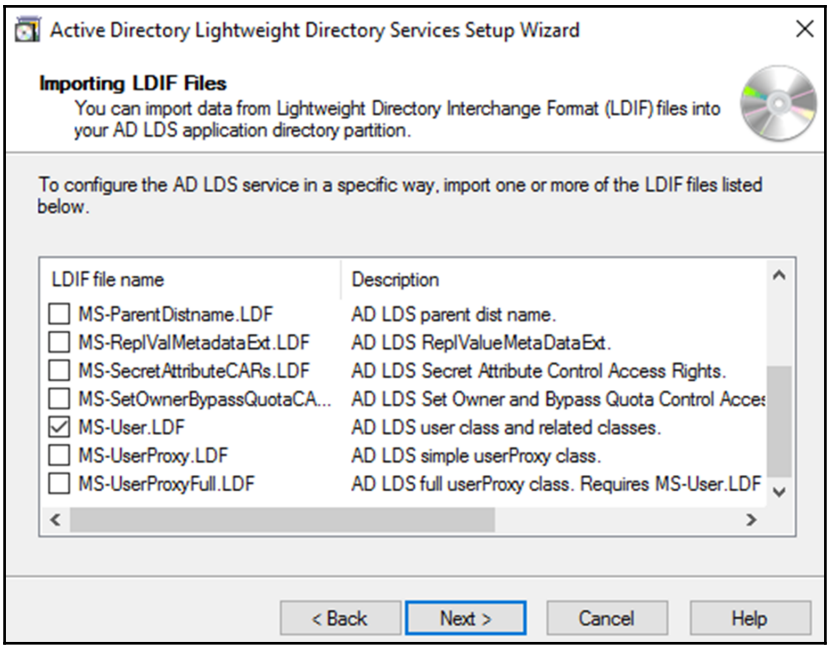


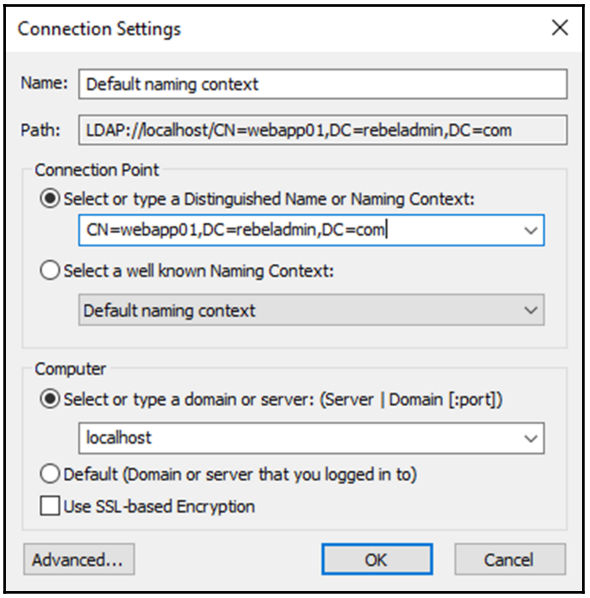

Active Directory Lightweight Directory Services Setup Wizard
Setup Options
An AD LDS instance is created each time AD LDS is installed.
You can create a unique instance, or you can install a replica of an existing instance.
Select the type of instance you want to install.
A unique instance
This option automatically creates a new instance of AD LDS that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.
A replica of an existing instance
This option creates a new instance of AD LDS that uses the configuration and schema partitions replicated from another instance of AD LDS. You can also select the application partitions to replicate.
< Back
Next >
Cancel
Help


Active Directory Lightweight Directory Services Setup Wizard
Instance Name
The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.
Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.
Instance name:
rebeladmin1
Example: Addressbook1
Description:
AD LDS instance 01
The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter.
AD LDS service display name: rebeladmin1
AD LDS service name: ADAM_rebeladmin1
< Back
Next >
Cancel
Help

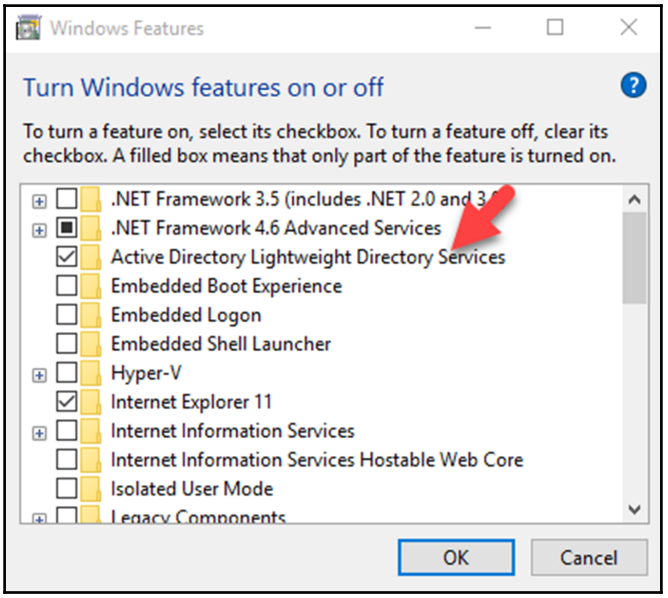

Active Directory Lightweight Directory Services Setup Wizard
Application Directory Partition
An application directory partition stores application-specific data.
Do you want to create an application directory partition for this instance of AD LDS?
No, do not create an application directory partition
Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.
Yes, create an application directory partition
Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name: CN=Partition1,DC=Woodgrove,DC=COM
Partition name:
CN=webapp01,DC=rebeladmin,DC=com
< Back
Next >
Cancel
Help

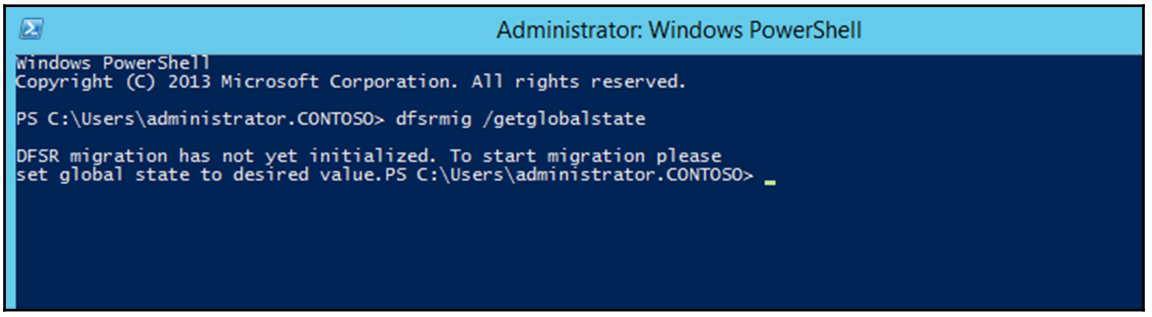

Active Directory Lightweight Directory Services Setup Wizard
Service Account Selection
AD LDS performs operations using the permissions associated with the account you select.
Set up AD LDS to perform operations using the permissions associated with the following account.
Network service account
AD LDS has the permissions of the default Windows service account.
This account:
AD LDS service has the permissions of the selected account.
User name:
Password:
Browse...
< Back
Next >
Cancel
Help

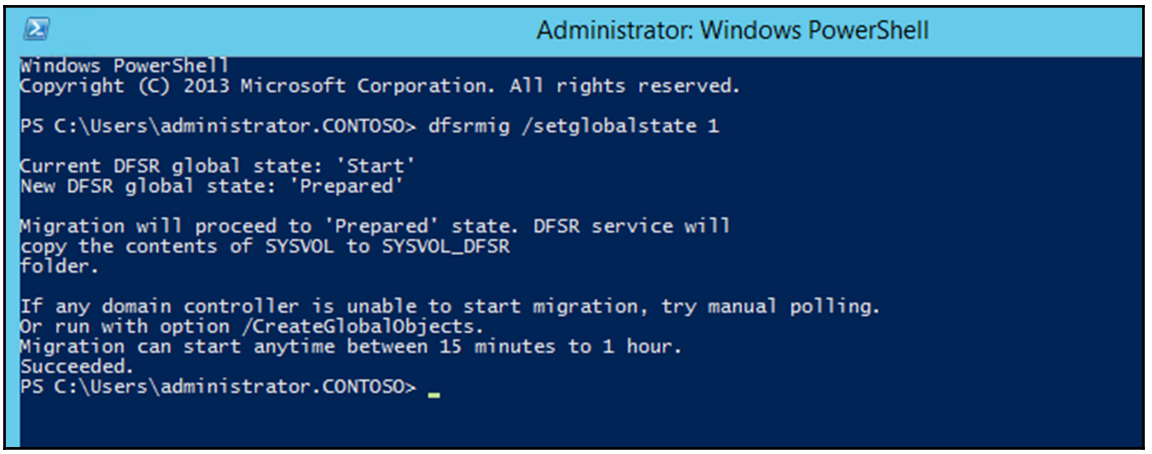

Active Directory Lightweight Directory Services Setup Wizard
Importing LDIF Files
You can import data from Lightweight Directory Interchange Format (LDIF) files into your AD LDS application directory partition.
To configure the AD LDS service in a specific way, import one or more of the LDIF files listed below.
LDIF file name
Description
MS-ParentDistname.LDF
AD LDS parent dist name.
MS-ReplValMetadataExt.LDF
AD LDS ReplValueMetaDataExt.
MS-SecretAttributeCARs.LDF
AD LDS Secret Attribute Control Access Rights.
MS-SetOwnerBypassQuotaCA...
AD LDS Set Owner and Bypass Quota Control Acces
MS-User.LDF
AD LDS user class and related classes.
MS-UserProxy.LDF
AD LDS simple userProxy class.
MS-UserProxyFull.LDF
AD LDS full userProxy class. Requires MS-User.LDF
< Back
Next >
Cancel
Help

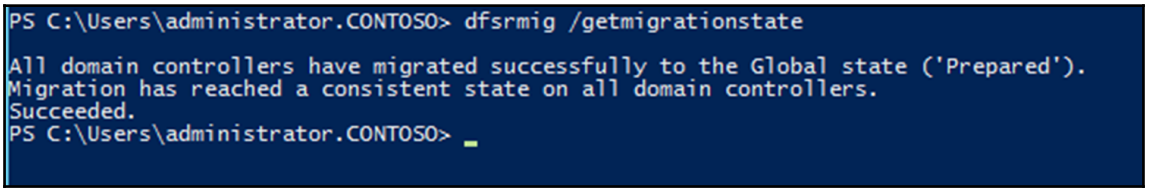

Connection Settings
Name:
Default naming context
Path:
LDAP://localhost/CN=webapp01,DC=rebeladmin,DC=com
Connection Point
Select or type a Distinguished Name or Naming Context:
CN=webapp01,DC=rebeladmin,DC=com
Select a well known Naming Context:
Default naming context
Computer
Select or type a domain or server: (Server | Domain [:port])
localhost
Default (Domain or server that you logged in to)
Use SSL-based Encryption
Advanced...
OK
Cancel

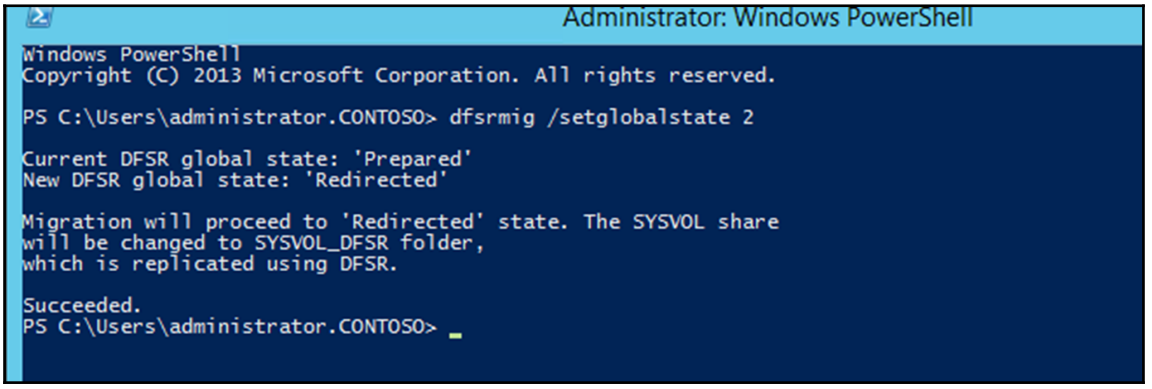
```
PS C:\Users\Administrator> Get-ADUser -Filter * -SearchBase "CN=webapp01,DC=rebeladmin,DC=com" -server 'localhost:389'


DistinguishedName : CN=tidris,CN=webapp01,DC=rebeladmin,DC=com
Enabled           : False
GivenName         :
Name              : tidris
ObjectClass       : user
ObjectGUID        : bfb4aa5e-3af6-4cfa-8934-c5b468a07326
SID               : S-1-378946516-2781328988-2354691366-1218222115-2413536430-3425642021
Surname           :
UserPrincipalName :
```

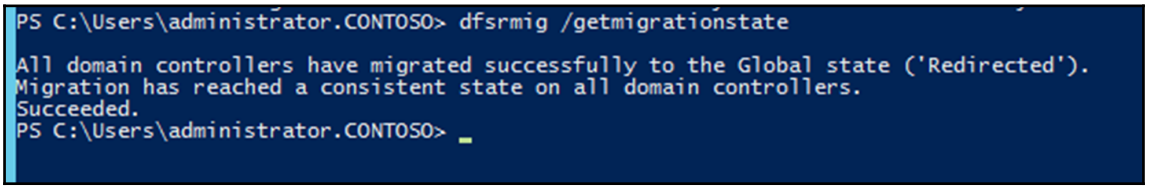


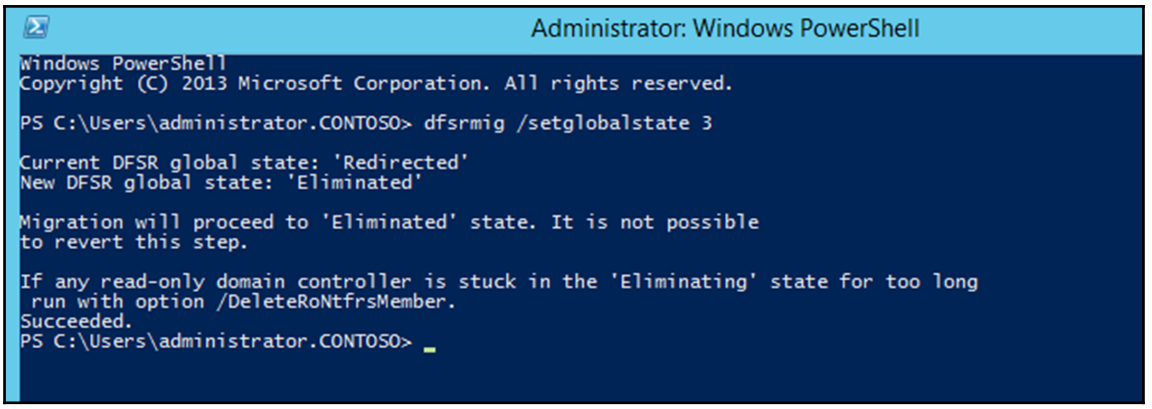


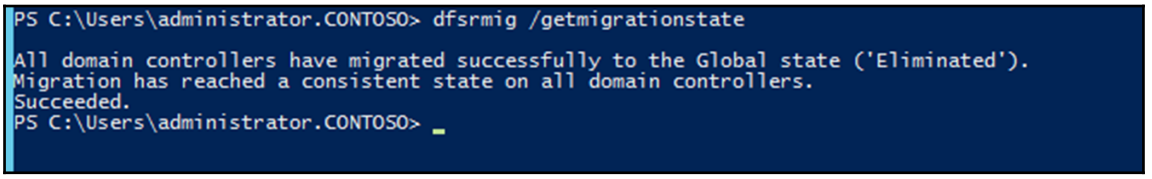

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\Users\administrator.CONTOSO> dfsrmig /setglobalstate 1
Current DFSR global state: 'Start'
New DFSR global state: 'Prepared'
Migration will proceed to 'Prepared' state. DFSR service will
copy the contents of SYSVOL to SYSVOL_DFSR
folder.
If any domain controller is unable to start migration, try manual polling.
Or run with option /CreateGlobalObjects.
Migration can start anytime between 15 minutes to 1 hour.
Succeeded.
PS C:\Users\administrator.CONTOSO>

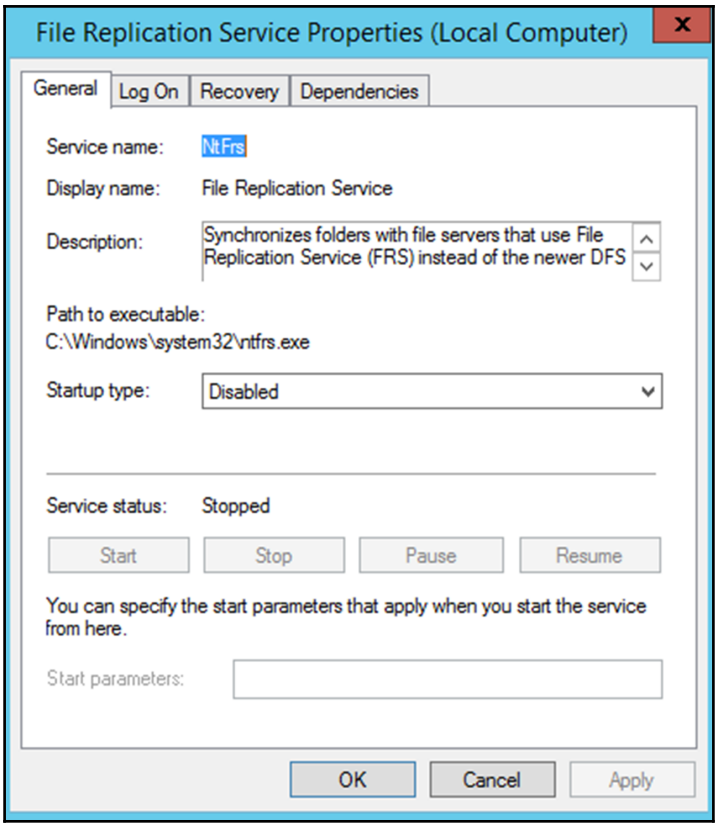

PS C:\Users\administrator.CONTOSO> dfsrmig /getmigrationstate
All domain controllers have migrated successfully to the Global state ('Prepared').
Migration has reached a consistent state on all domain controllers.
Succeeded.
PS C:\Users\administrator.CONTOSO>

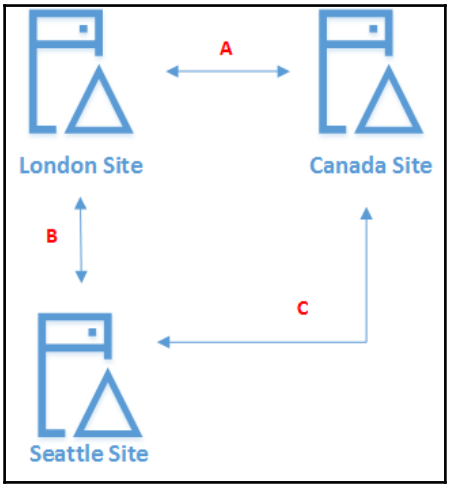

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\Users\administrator.CONTOSO> dfsrmig /setglobalstate 2
Current DFSR global state: 'Prepared'
New DFSR global state: 'Redirected'
Migration will proceed to 'Redirected' state. The SYSVOL share
will be changed to SYSVOL_DFSR folder,
which is replicated using DFSR.
Succeeded.
PS C:\Users\administrator.CONTOSO>


PS C:\Users\administrator.CONTOSO> dfsrmig /getmigrationstate
All domain controllers have migrated successfully to the Global state ('Redirected').
Migration has reached a consistent state on all domain controllers.
Succeeded.
PS C:\Users\administrator.CONTOSO>

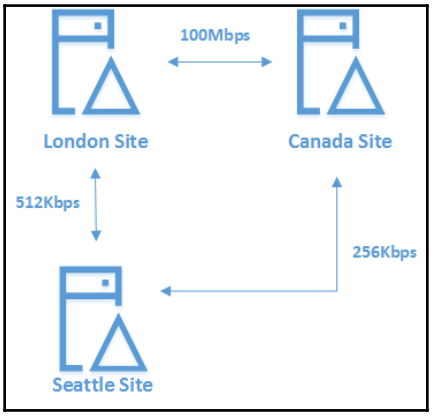

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\Users\administrator.CONTOSO> dfsrmig /setglobalstate 3
Current DFSR global state: 'Redirected'
New DFSR global state: 'Eliminated'
Migration will proceed to 'Eliminated' state. It is not possible
to revert this step.
If any read-only domain controller is stuck in the 'Eliminating' state for too long
run with option /DeleteRoNtfrsMember.
Succeeded.
PS C:\Users\administrator.CONTOSO>

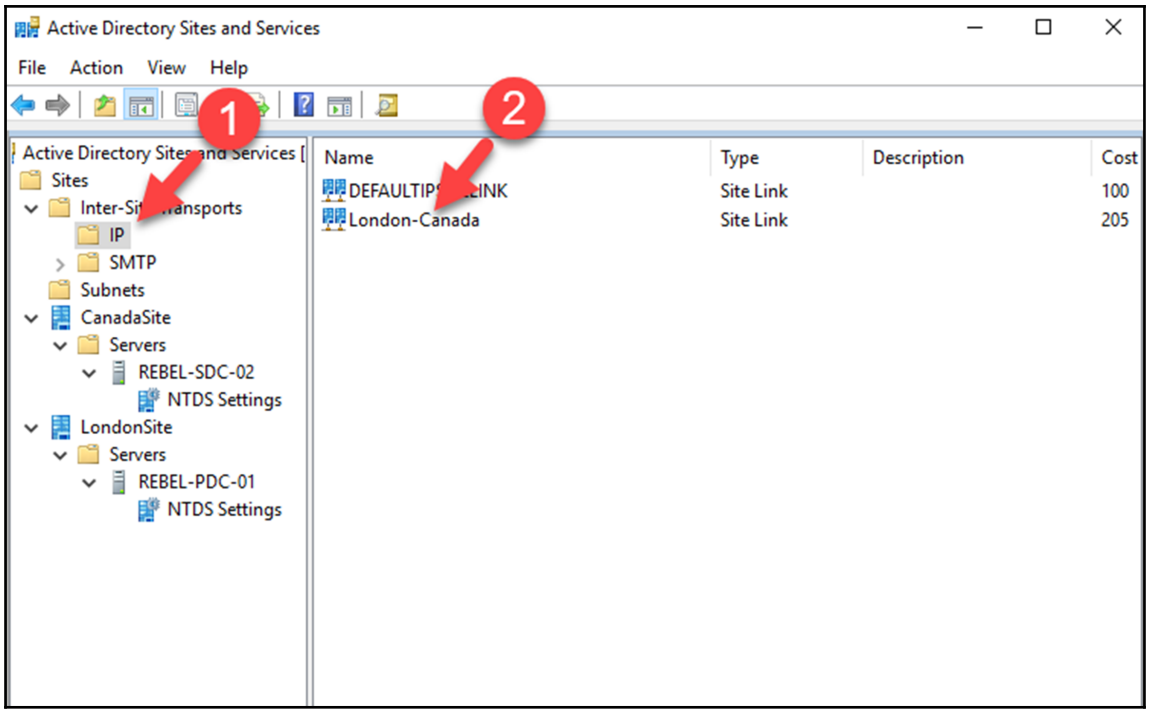

PS C:\Users\administrator.CONTOSO> dfsrmig /getmigrationstate
All domain controllers have migrated successfully to the Global state ('Eliminated').
Migration has reached a consistent state on all domain controllers.
Succeeded.
PS C:\Users\administrator.CONTOSO>

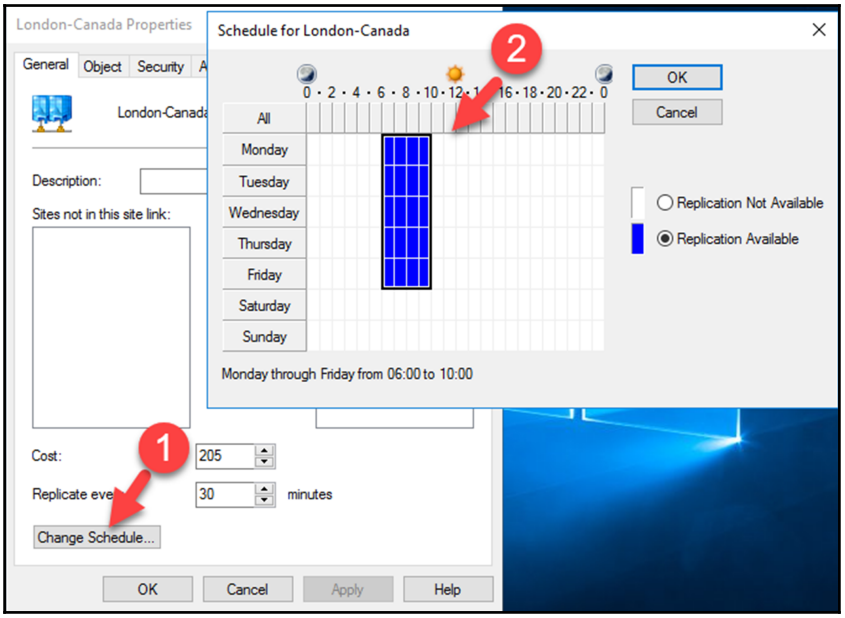

File Replication Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
NtFrs
Display name:
File Replication Service
Description:
Synchronizes folders with file servers that use File Replication Service (FRS) instead of the newer DFS
Path to executable:
C:\Windows\system32\ntfrs.exe
Startup type:
Disabled
Service status:
Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply

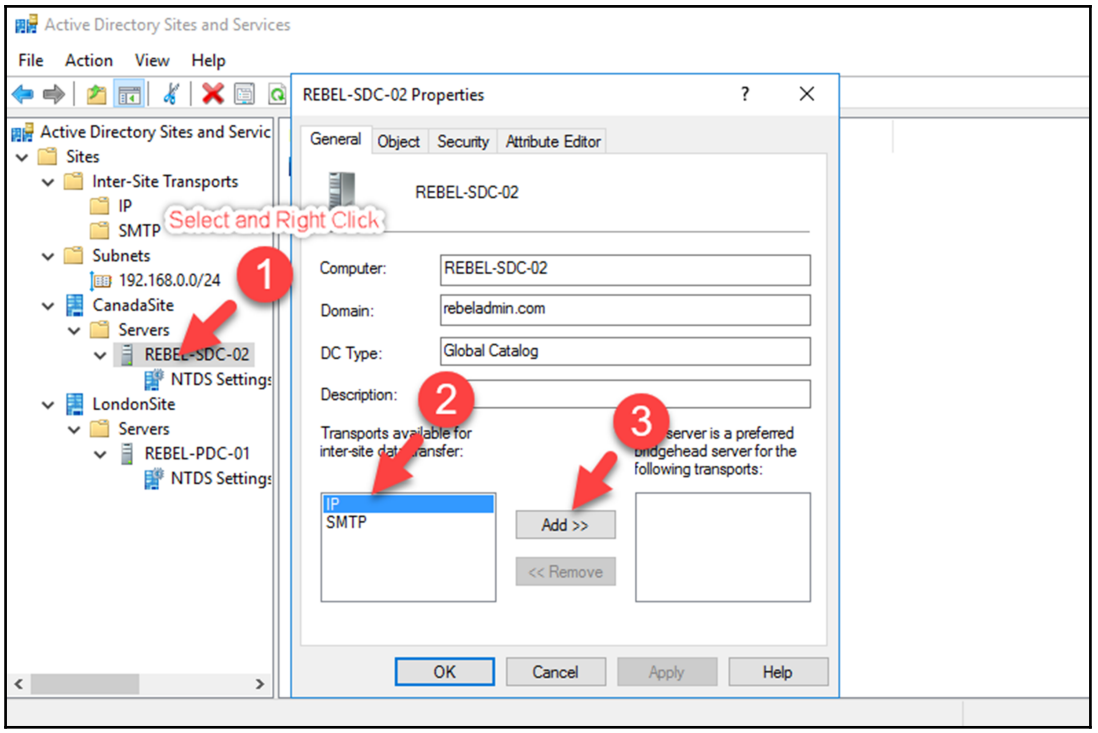

A
London Site
Canada Site
B
C
Seattle Site

```
PS C:\Users\Administrator> Get-ADReplicationSite -Filter *


Description                     : UK AD Site
DistinguishedName               : CN=LondonSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
InterSiteTopologyGenerator      : CN=NTDS Settings,CN=REBEL-SDC-02,CN=Servers,CN=LondonSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
ManagedBy                       :
Name                            : LondonSite
ObjectClass                     : site
ObjectGUID                      : fbef3a2c-2de8-44d2-bde9-c37403c9f3a9
ReplicationSchedule             : System.DirectoryServices.ActiveDirectory.ActiveDirectorySchedule
UniversalGroupCachingRefreshSite :

Description                     : Canada AD Site
DistinguishedName               : CN=CanadaSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
InterSiteTopologyGenerator      :
ManagedBy                       :
Name                            : CanadaSite
ObjectClass                     : site
ObjectGUID                      : 1bc04b4a-0f69-4ef5-8083-98d9bb0e88ca
ReplicationSchedule             :
UniversalGroupCachingRefreshSite :
```

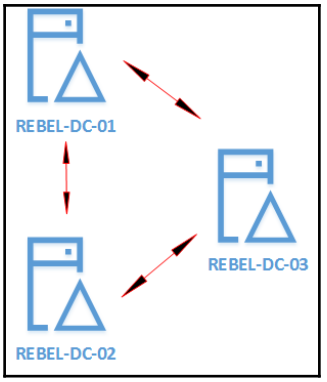


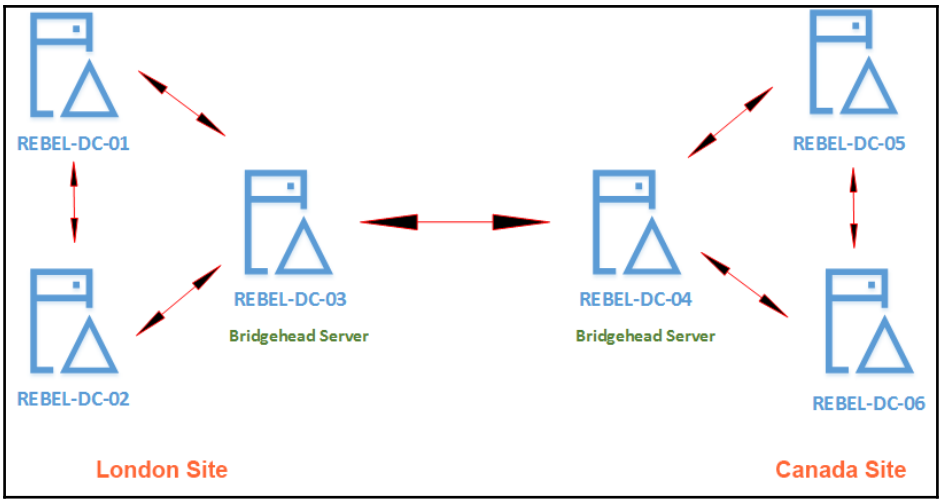

Active Directory Sites and Services
File
Action
View
Help
1
2
Active Directory Sites and Services [
Sites
Inter-Site Transports
IP
SMTP
Subnets
CanadaSite
Servers
REBEL-SDC-02
NTDS Settings
LondonSite
Servers
REBEL-PDC-01
NTDS Settings
Name
Type
Description
Cost
DEFAULTIPSITELINK
Site Link
100
London-Canada
Site Link
205

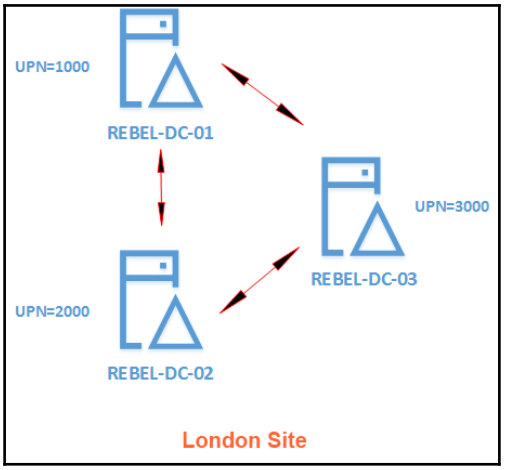

London-Canada Properties
General
Object
Security
Description:
Sites not in this site link:
Cost:
205
Replicate every:
30
minutes
Change Schedule...
OK
Cancel
Apply
Help
1
Schedule for London-Canada
2
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0
All
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Monday through Friday from 06:00 to 10:00
OK
Cancel
Replication Not Available
Replication Available




```
PS C:\Users\Administrator> Get-ADReplicationSubnet -Filter {Site -Eq "CanadaSite"}


DistinguishedName : CN=192.168.0.0/24,CN=Subnets,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
Location          :
Name              : 192.168.0.0/24
ObjectClass       : subnet
ObjectGUID        : 1e84b584-7bcf-4c08-b29b-ac96aaab4eb7
Site              : CN=CanadaSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
```





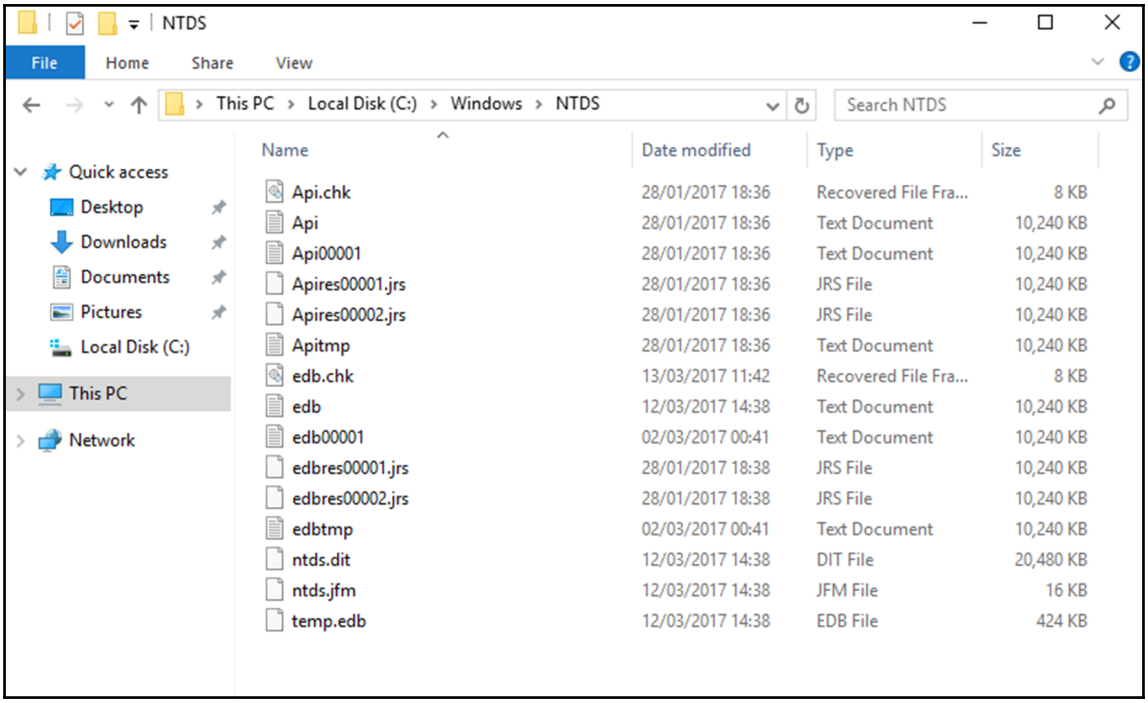



```
PS C:\Users\Administrator> Add-ADDSReadOnlyDomainControllerAccount -DomainControllerAccountName REBEL-RODC-01 -DomainNa
e rebeladmin.com -DelegatedAdministratorAccountName "rebeladmin\dfrancis" -SiteName LondonSite
WARNING: Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography
algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).

WARNING: Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography
algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).


Message                      Context          RebootRequired  Status
-------                      -------          --------------  ------
Operation completed successfully DCPromo.General.1          False Success
```

```
ComputerObjectDN           : CN=REBEL-RODC-01,OU=Domain Controllers,DC=rebeladmin,DC=com
DefaultPartition           : DC=rebeladmin,DC=com
Domain                     : rebeladmin.com
Enabled                    : False
Forest                     : rebeladmin.com
HostName                   : REBEL-RODC-01.rebeladmin.com
InvocationId               : 00000000-0000-0000-0000-000000000000
IPv4Address                :
IPv6Address                :
IsGlobalCatalog            : True
IsReadOnly                 : True
LdapPort                   : 389
Name                       : REBEL-RODC-01
NTDSSettingsObjectDN       : CN=NTDS Settings,CN=REBEL-RODC-01,CN=Servers,CN=LondonSite,CN=Sites,CN=Configuration,DC=re
                             beladmin,DC=com
OperatingSystem            :
OperatingSystemHotfix      :
OperatingSystemServicePack :
OperatingSystemVersion     :
OperationMasterRoles       : {}
Partitions                 : {CN=Schema,CN=Configuration,DC=rebeladmin,DC=com, CN=Configuration,DC=rebeladmin,DC=com,
                             DC=rebeladmin,DC=com}
ServerObjectDN             : CN=REBEL-RODC-01,CN=Servers,CN=LondonSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
ServerObjectGuid           : 2fc5dc79-dbc8-4ffb-a708-656b8c2c9875
Site                       : LondonSite
SslPort                    : 636
```

```
PS C:\Users\Administrator> Get-ADDomainControllerPasswordReplicationPolicy -Identity REBEL-RODC-01 -Allowed


DistinguishedName : CN=user1,OU=Users,OU=Europe,DC=rebeladmin,DC=com
Name              : user1
ObjectClass       : user
ObjectGUID        : edd1f313-f14d-48cc-bd27-e6f8e57a5fc4
SamAccountName    : user1
SID               : S-1-5-21-4041220333-1835452706-552999228-1104

DistinguishedName : CN=Allowed RODC Password Replication Group,CN=Users,DC=rebeladmin,DC=com
Name              : Allowed RODC Password Replication Group
ObjectClass       : group
ObjectGUID        : 89f5a011-391f-49d2-9238-8bebdb80c1ce
SamAccountName    : Allowed RODC Password Replication Group
SID               : S-1-5-21-4041220333-1835452706-552999228-571
```

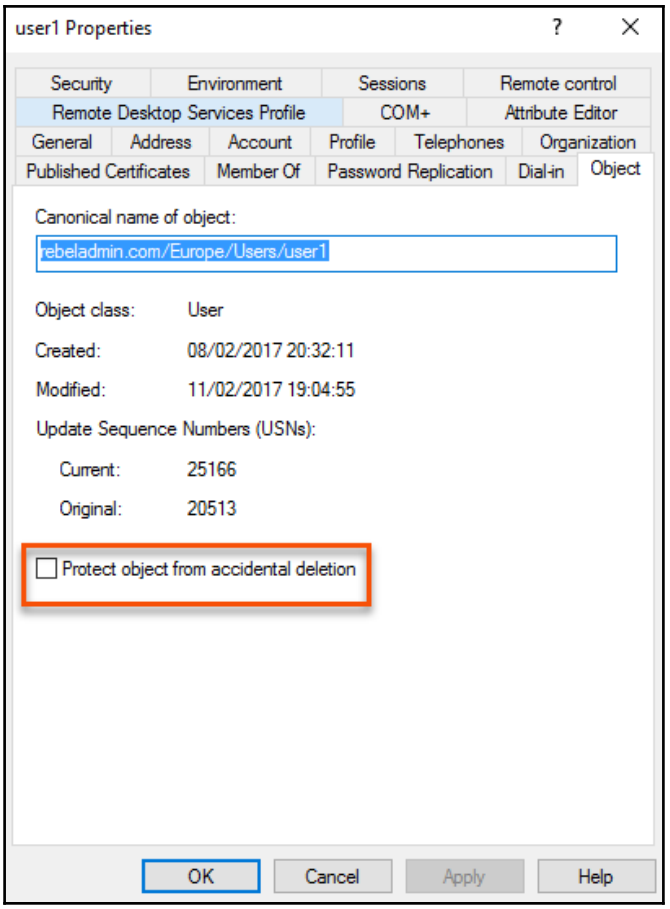
```
PS C:\Users\Administrator> Add-ADDomainControllerPasswordReplicationPolicy -Identity REBEL-RODC-01 -DeniedList "user2"
PS C:\Users\Administrator> Get-ADDomainControllerPasswordReplicationPolicy -Identity REBEL-RODC-01 -Denied


DistinguishedName : CN=user2,OU=Users,OU=Europe,DC=rebeladmin,DC=com
Name              : user2
ObjectClass       : user
ObjectGUID        : 679ec55b-fb62-427f-b828-bd0ec31d7e30
SamAccountName    : user2
SID               : S-1-5-21-4041220333-1835452706-552999228-1105
```

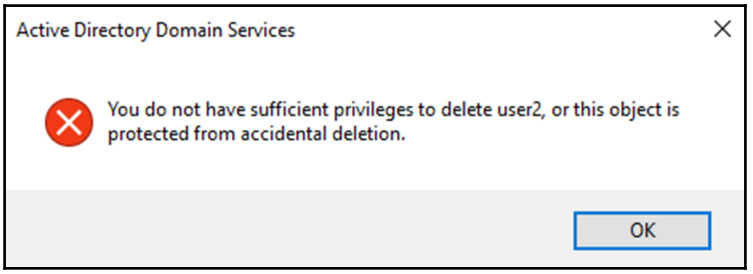

NTDS
File
Home
Share
View
This PC › Local Disk (C:) › Windows › NTDS
Search NTDS
Quick access
Desktop
Downloads
Documents
Pictures
Local Disk (C:)
This PC
Network
Name
Date modified
Type
Size
Api.chk 28/01/2017 18:36 Recovered File Fra... 8 KB
Api 28/01/2017 18:36 Text Document 10,240 KB
Api00001 28/01/2017 18:36 Text Document 10,240 KB
Apires00001.jrs 28/01/2017 18:36 JRS File 10,240 KB
Apires00002.jrs 28/01/2017 18:36 JRS File 10,240 KB
Apitmp 28/01/2017 18:36 Text Document 10,240 KB
edb.chk 13/03/2017 11:42 Recovered File Fra... 8 KB
edb 12/03/2017 14:38 Text Document 10,240 KB
edb00001 02/03/2017 00:41 Text Document 10,240 KB
edbres00001.jrs 28/01/2017 18:38 JRS File 10,240 KB
edbres00002.jrs 28/01/2017 18:38 JRS File 10,240 KB
edbtmp 02/03/2017 00:41 Text Document 10,240 KB
ntds.dit 12/03/2017 14:38 DIT File 20,480 KB
ntds.jfm 12/03/2017 14:38 JFM File 16 KB
temp.edb 12/03/2017 14:38 EDB File 424 KB

```
PS E:\> ntdsutil
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: files
file maintenance: move db to E:\ADDB

Successfully updated the backup exclusion key.
Copying NTFS security from C:\Windows\NTDS to E:\ADDB...
The previous NTDS database location C:\Windows\NTDS\dsadata.bak is unavailable. The default NTFS security will be applie
d to NTDS folders.
Default NTFS security on NTDS folders will be set on reboot.
Copying NTFS security from C:\Windows\NTDS to E:\ADDB...

Drive Information:

        C:\ NTFS (Fixed Drive  ) free(28.8 Gb) total(39.4 Gb)
        E:\ NTFS (Fixed Drive  ) free(1.9 Gb) total(1.9 Gb)

DS Path Information:

        Database   : E:\ADDB\ntds.dit - 20.0 Mb
        Backup dir : E:\ADDB\DSADATA.BAK
        Working dir: E:\ADDB
        Log dir    : C:\Windows\NTDS - 50.0 Mb total
                     edbtmp.log - 10.0 Mb
                     edbres00002.jrs - 10.0 Mb
                     edbres00001.jrs - 10.0 Mb
                     edb00001.log - 10.0 Mb
                     edb.log - 10.0 Mb

Move database is successful.
Please make a backup immediately else restore will not retain the new file
location.
file maintenance: move logs to E:\ADDB
Successfully updated the backup exclusion key.

Copying NTFS security from C:\Windows\NTDS to E:\ADDB...

Drive Information:

        C:\ NTFS (Fixed Drive  ) free(28.9 Gb) total(39.4 Gb)
        E:\ NTFS (Fixed Drive  ) free(1.8 Gb) total(1.9 Gb)

DS Path Information:

        Database   : E:\ADDB\ntds.dit - 20.0 Mb
        Backup dir : E:\ADDB\DSADATA.BAK
        Working dir: E:\ADDB
        Log dir    : E:\ADDB - 50.0 Mb total
                     edbtmp.log - 10.0 Mb
                     edbres00002.jrs - 10.0 Mb
                     edbres00001.jrs - 10.0 Mb
                     edb00001.log - 10.0 Mb
                     edb.log - 10.0 Mb

If move log files was successful,
 please make a backup immediately else restore
 will not retain the new file location.
```



```
PS E:\> ntdsutil
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: files
file maintenance: compact to E:\CompactDB
Initiating DEFRAGMENTATION mode...
     Source Database: E:\ADDB\ntds.dit
     Target Database: E:\CompactDB\ntds.dit

                Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

It is recommended that you immediately perform a full backup
of this database. If you restore a backup made before the
defragmentation, the database will be rolled back to the state
it was in at the time of that backup.

Compaction is successful. You need to:
   copy "E:\CompactDB\ntds.dit" "E:\ADDB\ntds.dit"
and delete the old log files:
   del E:\ADDB\*.log


file maintenance: quit
C:\Windows\system32\ntdsutil.exe: quit
PS E:\>
```


user1 Properties
Security
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
Attribute Editor
General
Address
Account
Profile
Telephones
Organization
Published Certificates
Member Of
Password Replication
Dial-in
Object
Canonical name of object:
rebeladmin.com/Europe/Users/user1
Object class: User
Created: 08/02/2017 20:32:11
Modified: 11/02/2017 19:04:55
Update Sequence Numbers (USNs):
Current: 25166
Original: 20513
Protect object from accidental deletion
OK
Cancel
Apply
Help


Active Directory Domain Services
You do not have sufficient privileges to delete user2, or this object is protected from accidental deletion.
OK

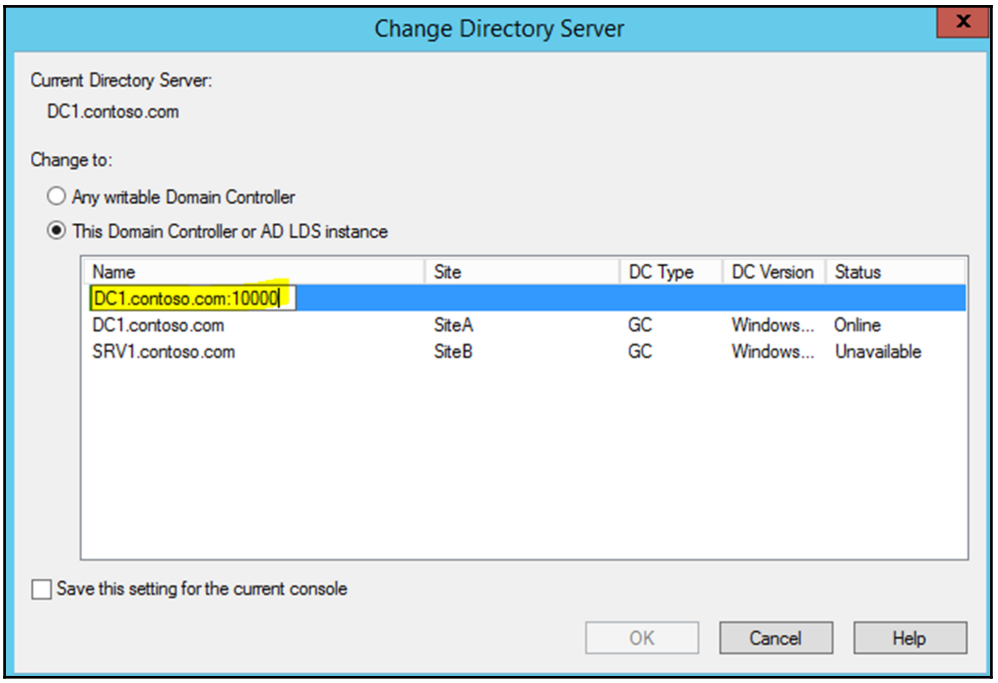
```
PS C:\Users\Administrator> Get-ADObject -IncludeDeletedObjects -Filter {samAccountName -eq 'user01'}

Deleted           : True
DistinguishedName : CN=user01\0ADEL:2ac6350b-e44f-465e-a264-54c271e8ebfc,CN=Deleted Objects,DC=rebeladmin,DC=com
Name              : user01
                    DEL:2ac6350b-e44f-465e-a264-54c271e8ebfc
ObjectClass       : user
ObjectGUID        : 2ac6350b-e44f-465e-a264-54c271e8ebfc
```

```
PS C:\Users\Administrator> Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target rebeladmin.com
WARNING: Enabling 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=rebeladmin,DC=com' is an irreversible action! You will not be
able to disable 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=rebeladmin,DC=com' if you proceed.

Confirm
Are you sure you want to perform this action?
Performing the operation "Enable" on target "Recycle Bin Feature".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
PS C:\Users\Administrator>
```

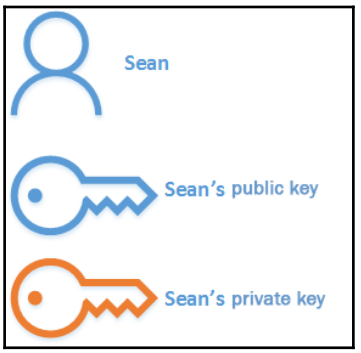
```
PS C:\Users\Administrator> Get-ADObject -Filter 'samaccountname -eq "dfrancis"' -IncludeDeletedObjects | Restore-ADObject
PS C:\Users\Administrator> Get-ADUser -Identity dfrancis


DistinguishedName : CN=Dishan Francis,OU=Users,OU=Europe,DC=rebeladmin,DC=com
Enabled           : True
GivenName         : Dishan
Name              : Dishan Francis
ObjectClass       : user
ObjectGUID        : 276f06a4-b457-4daf-a503-6092300cae70
SamAccountName    : dfrancis
SID               : S-1-5-21-4041220333-1835452706-552999228-1186
Surname           : Francis
UserPrincipalName : dfrancis@rebeladmin.com
```

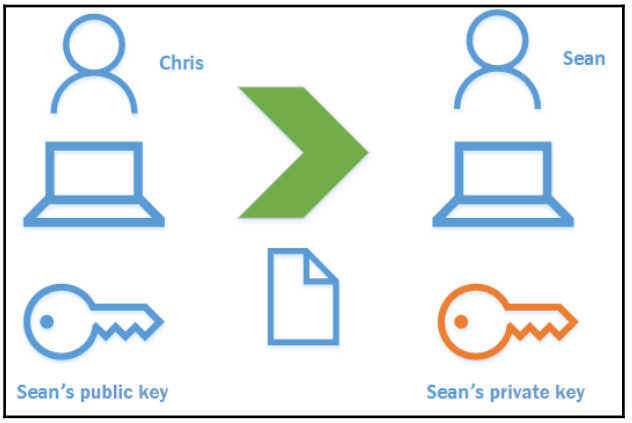
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ntdsutil
C:\Windows\system32\ntdsutil.exe: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: create
Creating snapshot...
Snapshot set {cd41cb4c-89c0-4c3e-8c08-989d8da69e03} generated successfully.
snapshot: quit
C:\Windows\system32\ntdsutil.exe: quit
PS C:\Users\Administrator>
```

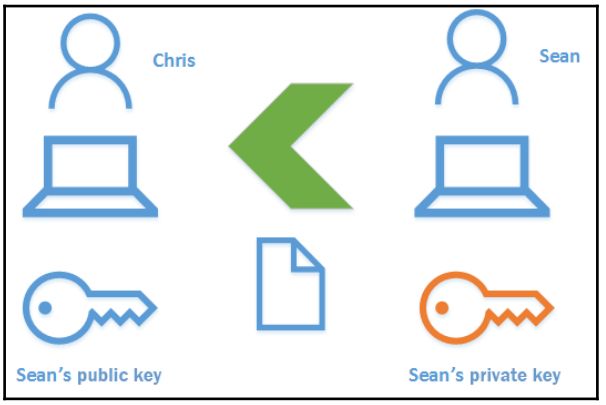
```
PS C:\Users\Administrator> ntdsutil
C:\Windows\system32\ntdsutil.exe: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: list all
 1: 2017/03/15:23:33 {cd41cb4c-89c0-4c3e-8c08-989d8da69e03}
 2:   C: {c7986714-032c-40ec-9ab3-b061562e1831}
 3:   E: {1e6f873e-f9a1-4f2f-99af-f7cc936a863a}

snapshot: mount 1
Snapshot {c7986714-032c-40ec-9ab3-b061562e1831} mounted as C:\$SNAP_201703152333_VOLUMEC$\
Snapshot {1e6f873e-f9a1-4f2f-99af-f7cc936a863a} mounted as C:\$SNAP_201703152333_VOLUMEE$\
snapshot: quit
```

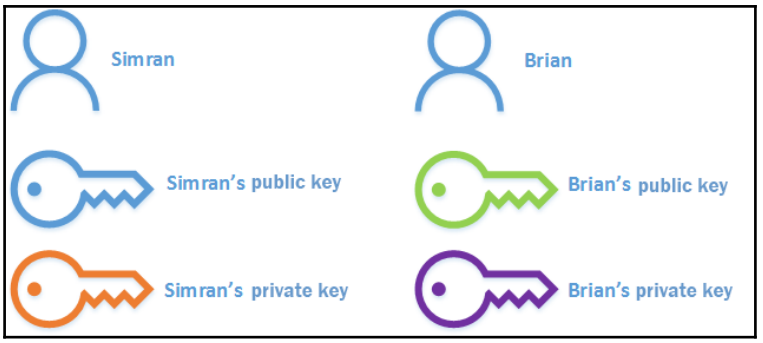

Change Directory Server
Current Directory Server:
DC1.contoso.com
Change to:
Any writable Domain Controller
This Domain Controller or AD LDS instance
Name
Site
DC Type
DC Version
Status
DC1.contoso.com:10000
DC1.contoso.com
SiteA
GC
Windows...
Online
SRV1.contoso.com
SiteB
GC
Windows...
Unavailable
Save this setting for the current console
OK
Cancel
Help

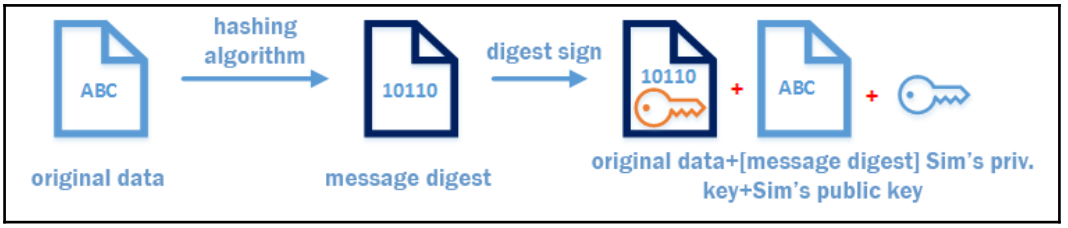
Chapter 12: Active Directory Certificate Services

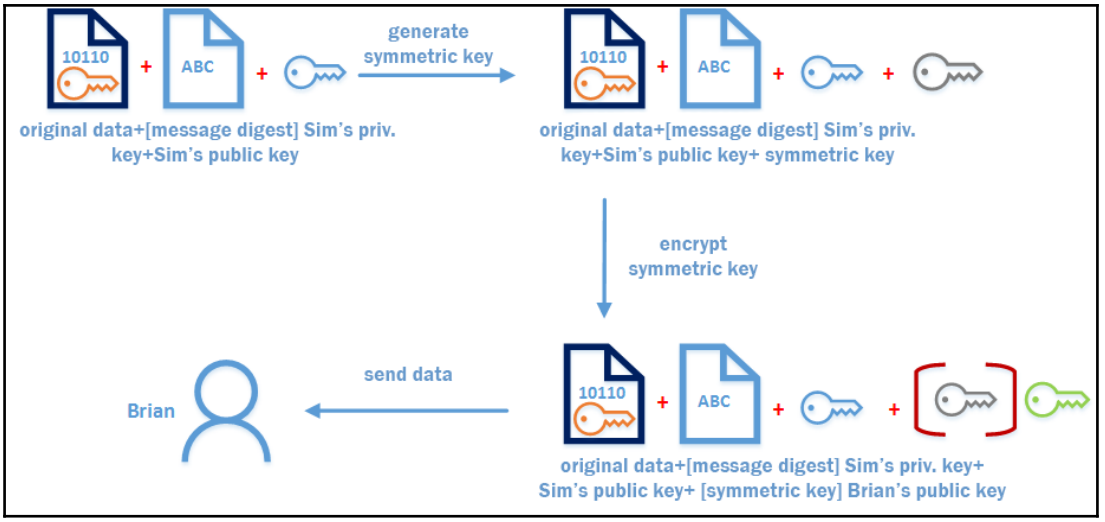


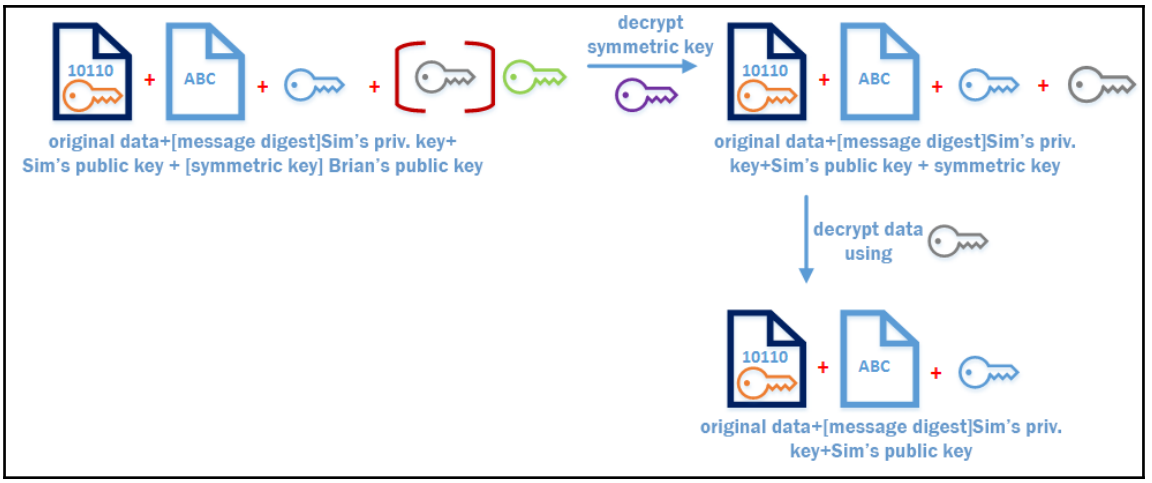


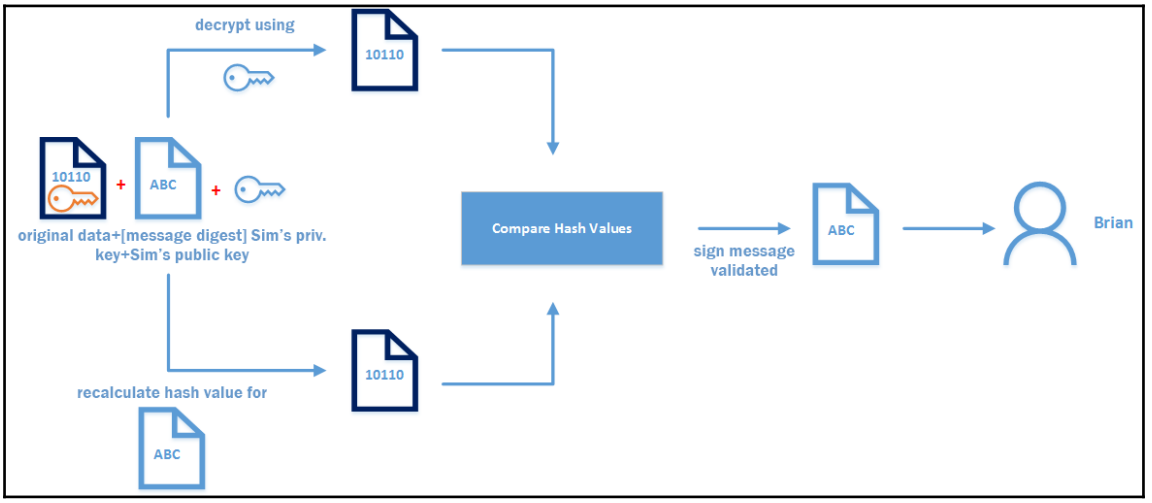


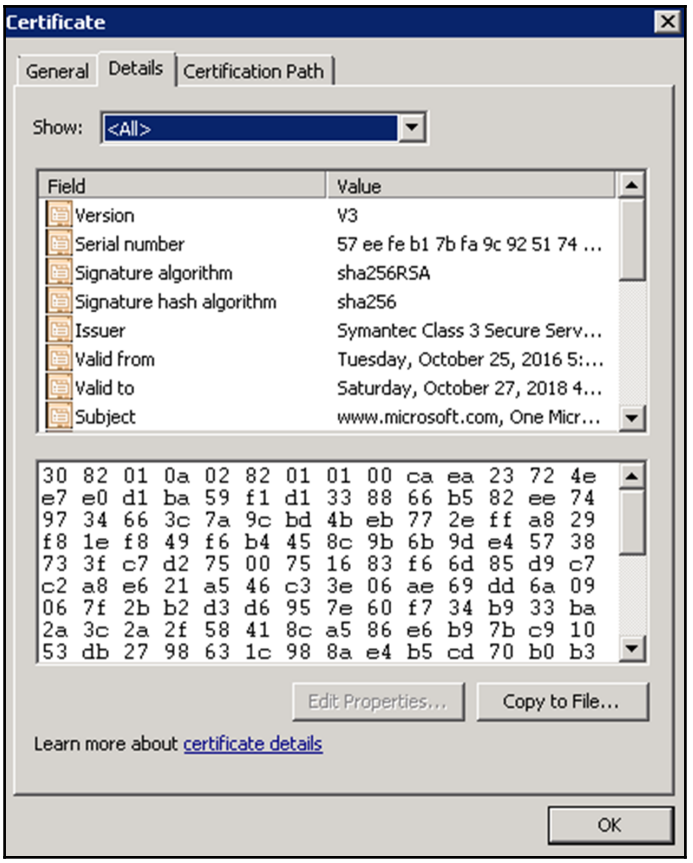

Simran
Brian
Simran's public key
Brian's public key
Simran's private key
Brian's private key

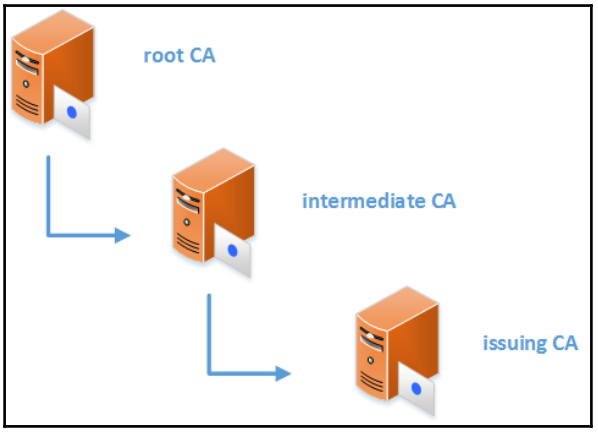

ABC
hashing algorithm
10110
digest sign
10110
ABC
original data
message digest
original data+[message digest] Sim's priv. key+Sim's public key


10110
ABC
generate symmetric key
original data+[message digest] Sim's priv. key+Sim's public key
original data+[message digest] Sim's priv. key+Sim's public key+ symmetric key
encrypt symmetric key
Brian
send data
original data+[message digest] Sim's priv. key+ Sim's public key+ [symmetric key] Brian's public key

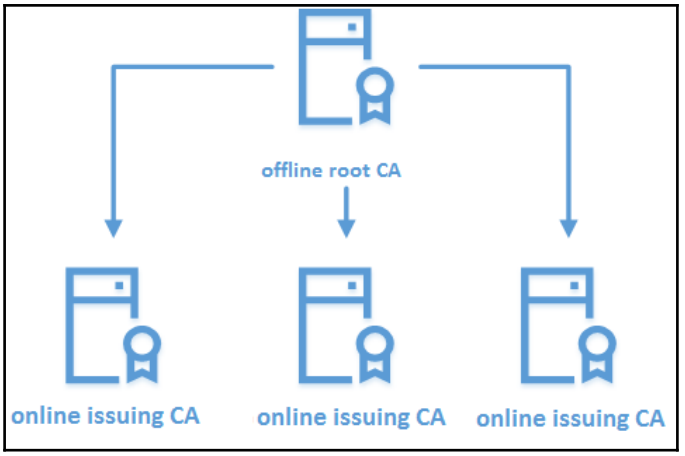

10110
ABC
original data+[message digest]Sim's priv. key+
Sim's public key + [symmetric key] Brian's public key
decrypt
symmetric key
10110
ABC
original data+[message digest]Sim's priv.
key+Sim's public key + symmetric key
decrypt data
using
10110
ABC
original data+[message digest]Sim's priv.
key+Sim's public key

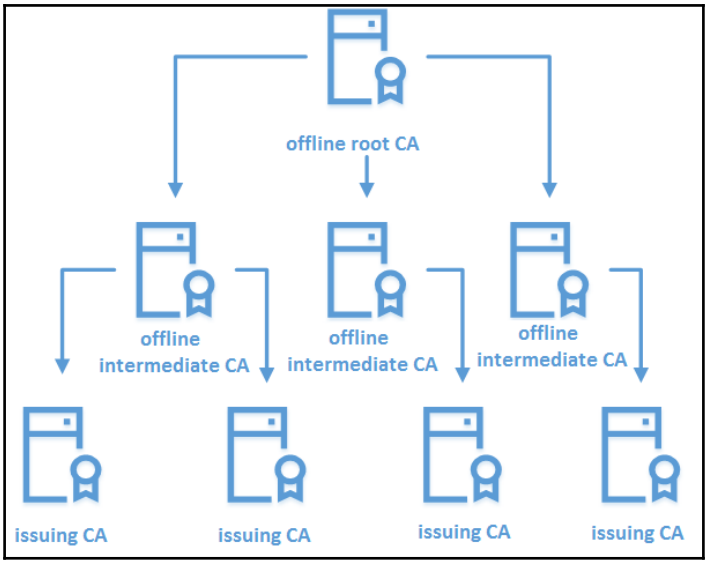

decrypt using
10110
10110
ABC
original data+[message digest] Sim's priv.
key+Sim's public key
Compare Hash Values
sign message
validated
ABC
Brian
recalculate hash value for
10110
ABC

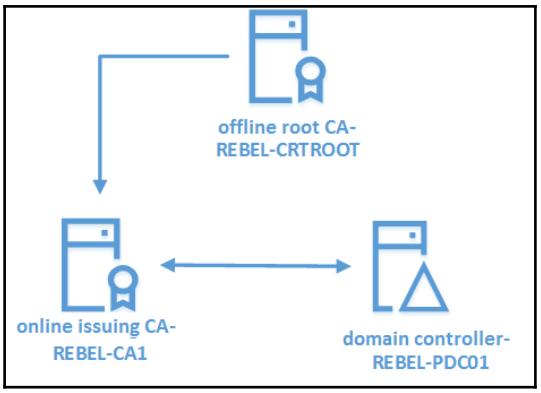

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
57 ee fe b1 7b fa 9c 92 51 74 ...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Symantec Class 3 Secure Serv...
Valid from
Tuesday, October 25, 2016 5:...
Valid to
Saturday, October 27, 2018 4...
Subject
www.microsoft.com, One Micr...
30 82 01 0a 02 82 01 01 00 ca ea 23 72 4e
e7 e0 d1 ba 59 f1 d1 33 88 66 b5 82 ee 74
97 34 66 3c 7a 9c bd 4b eb 77 2e ff a8 29
f8 1e f8 49 f6 b4 45 8c 9b 6b 9d e4 57 38
73 3f c7 d2 75 00 75 16 83 f6 6d 85 d9 c7
c2 a8 e6 21 a5 46 c3 3e 06 ae 69 dd 6a 09
06 7f 2b b2 d3 d6 95 7e 60 f7 34 b9 33 ba
2a 3c 2a 2f 58 41 8c a5 86 e6 b9 7b c9 10
53 db 27 98 63 1c 98 8a e4 b5 cd 70 b0 b3
Edit Properties...
Copy to File...
Learn more about certificate details
OK

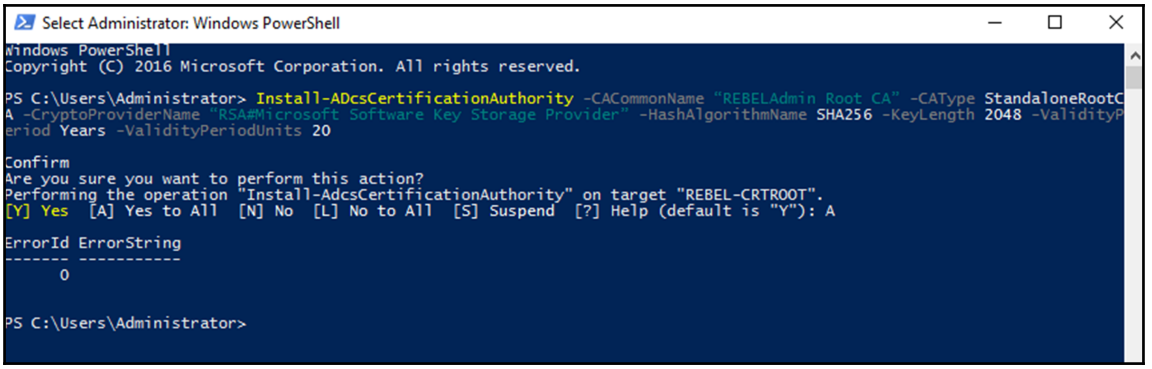

root CA
intermediate CA
issuing CA

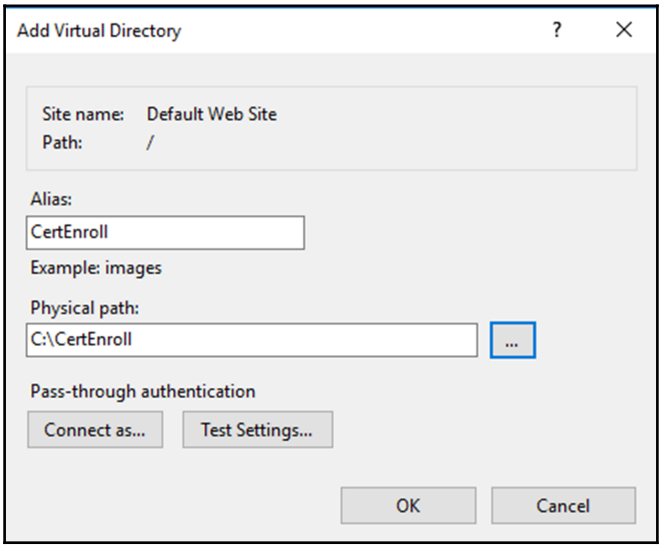

root and issuing CA


offline root CA
online issuing CA
online issuing CA
online issuing CA


offline root CA
offline
intermediate CA
offline
intermediate CA
offline
intermediate CA
issuing CA
issuing CA
issuing CA
issuing CA

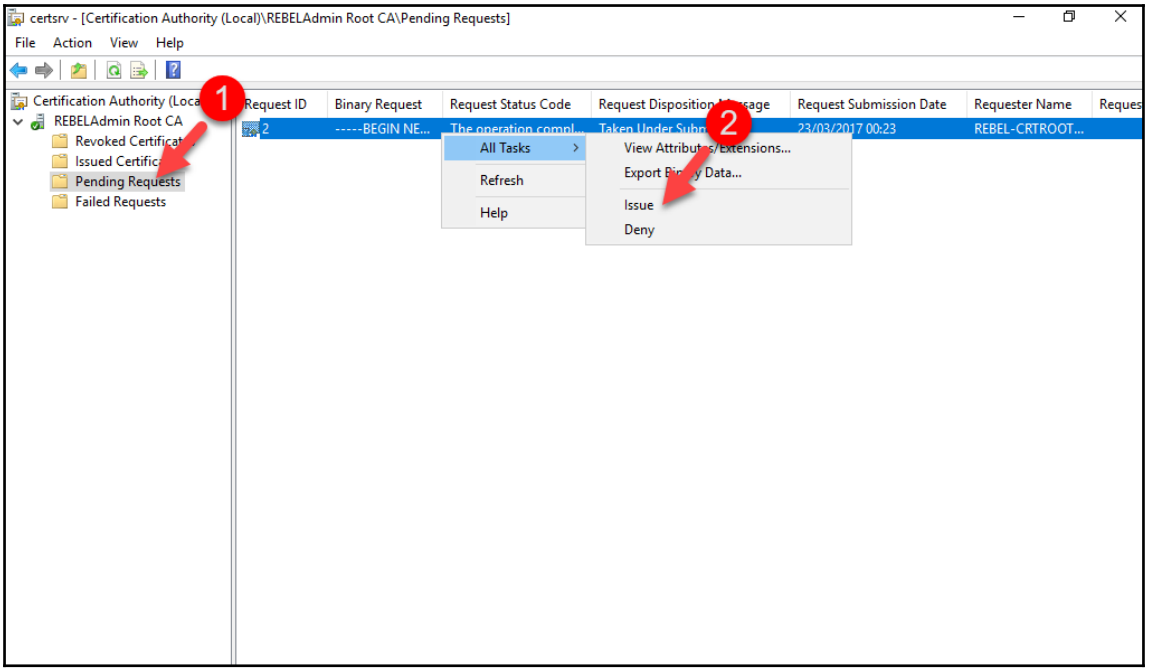

offline root CA-
REBEL-CRTROOT
online issuing CA-
REBEL-CA1
domain controller-
REBEL-PDC01

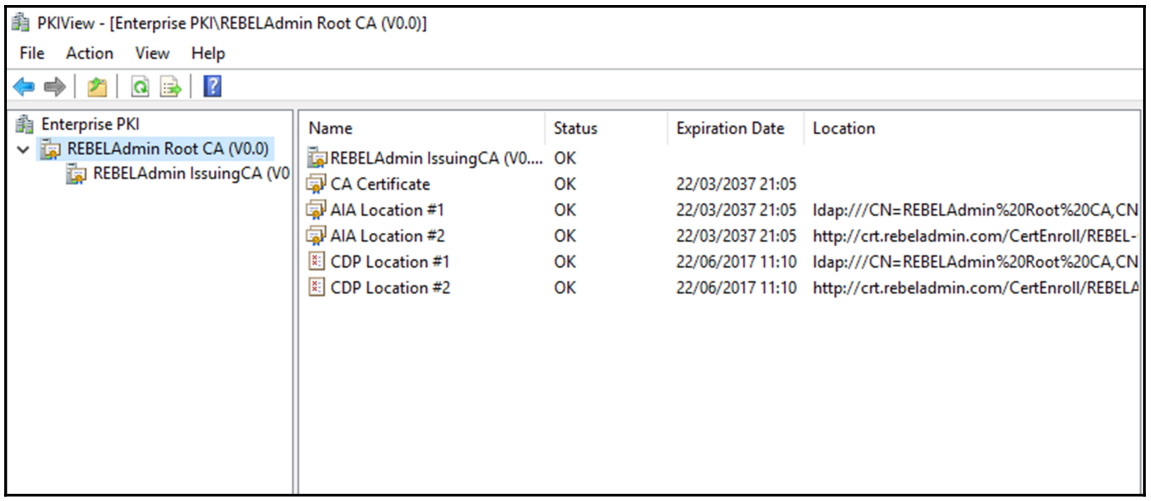

Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> Install-ADcsCertificationAuthority -CACommonName "REBELAdmin Root CA" -CAType StandaloneRootC
A -CryptoProviderName "RSA#Microsoft Software Key Storage Provider" -HashAlgorithmName SHA256 -KeyLength 2048 -ValidityP
eriod Years -ValidityPeriodUnits 20
Confirm
Are you sure you want to perform this action?
Performing the operation "Install-AdcsCertificationAuthority" on target "REBEL-CRTROOT".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A
ErrorId ErrorString
0
PS C:\Users\Administrator>

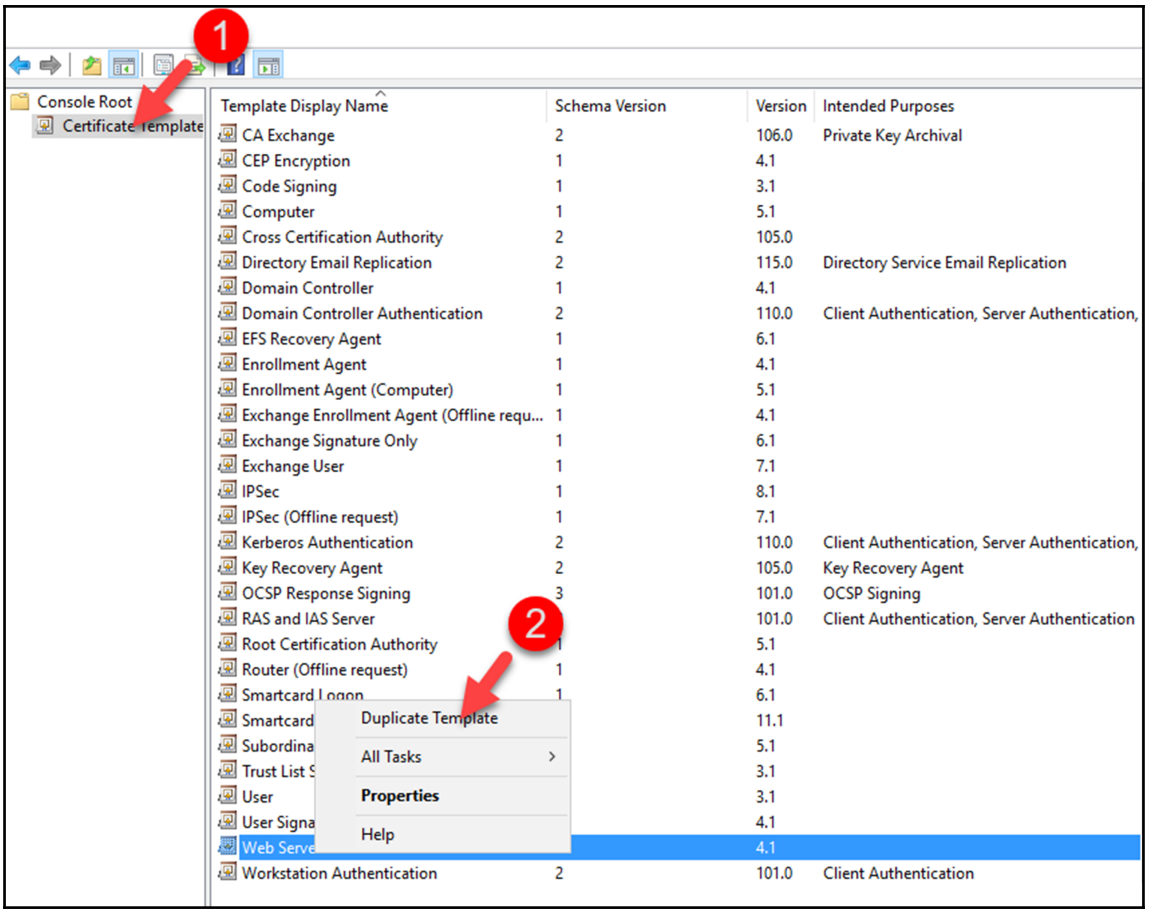

Add Virtual Directory
Site name: Default Web Site
Path: /
Alias:
CertEnroll
Example: images
Physical path:
C:\CertEnroll
...
Pass-through authentication
Connect as...
Test Settings...
OK
Cancel

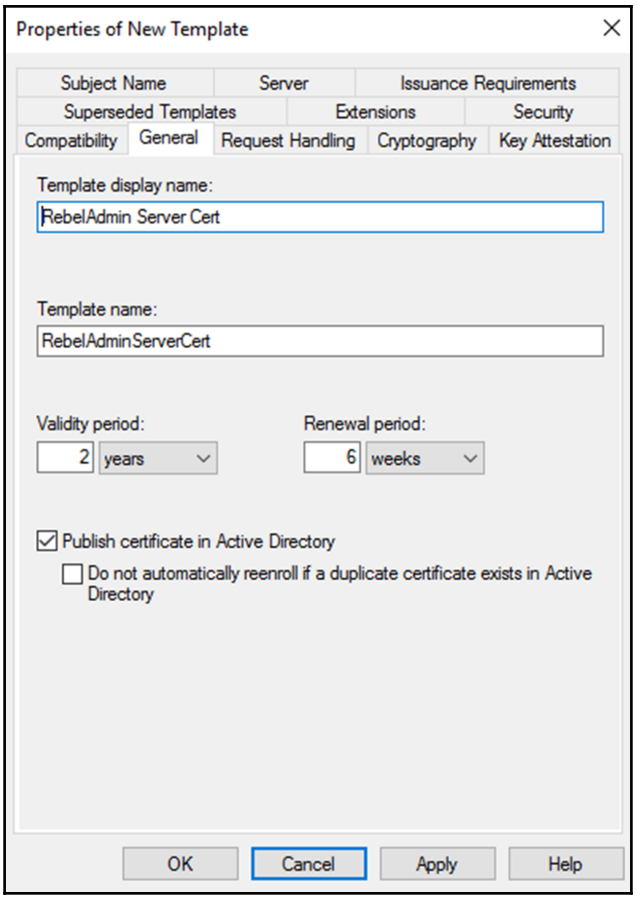
```
PS C:\Users\Administrator> cd C:\Windows\System32\CertSrv\CertEnroll
PS C:\Windows\System32\CertSrv\CertEnroll> dir


    Directory: C:\Windows\System32\CertSrv\CertEnroll


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        22/03/2017     21:05            793 REBEL-CRTROOT_REBELAdmin Root CA.crt
-a----        22/03/2017     23:00            694 REBELAdmin Root CA.crl


PS C:\Windows\System32\CertSrv\CertEnroll>
```

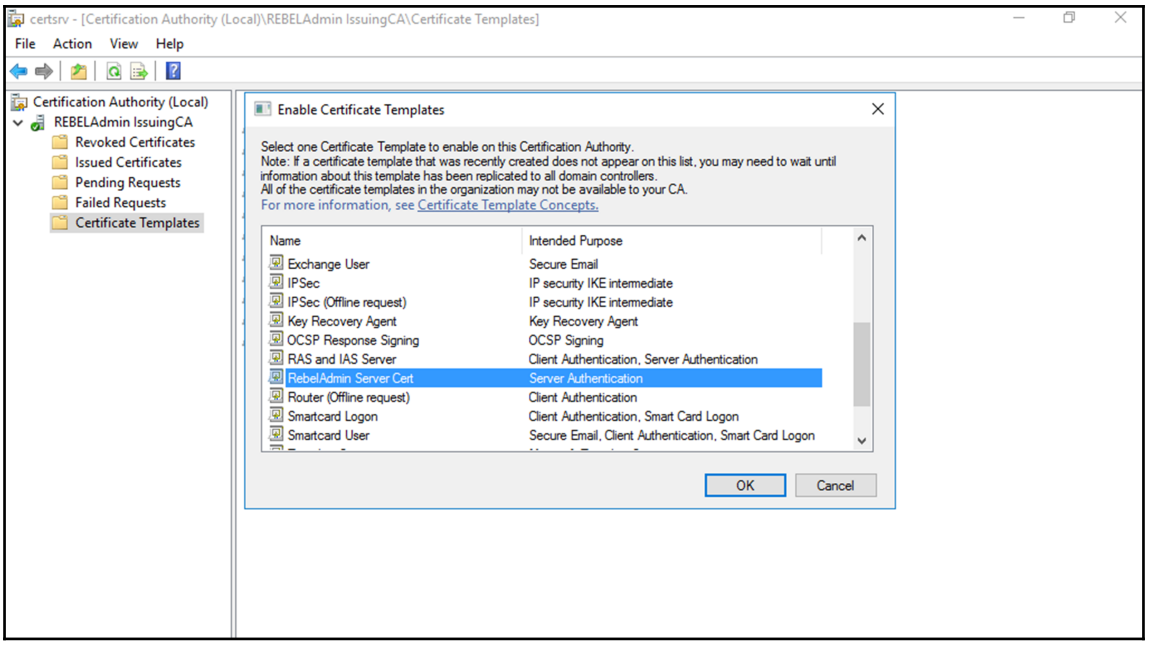
```
PS C:\Users\administrator.REBELADMIN> Install-ADcsCertificationAuthority -CACommonName "REBELAdmin IssuingCA" -CAType En
terpriseSubordinateCA -CryptoProviderName "RSA#Microsoft Software Key Storage Provider" -HashAlgorithmName SHA256 -KeyLe
ngth 2048

Confirm
Are you sure you want to perform this action?
Performing the operation "Install-AdcsCertificationAuthority" on target "REBEL-CA1".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
WARNING: The Active Directory Certificate Services installation is incomplete. To complete the installation, use the
request file "C:\REBEL-CA1.rebeladmin.com_REBELAdmin IssuingCA.req" to obtain a certificate from the parent CA. Then,
use the Certification Authority snap-in to install the certificate. To complete this procedure, right-click the node
with the name of the CA, and then click Install CA Certificate. The operation completed successfully. 0x0 (WIN32: 0)

ErrorId ErrorString
------- -----------
    398 The Active Directory Certificate Services installation is incomplete. To complete the installation, use the ...
```

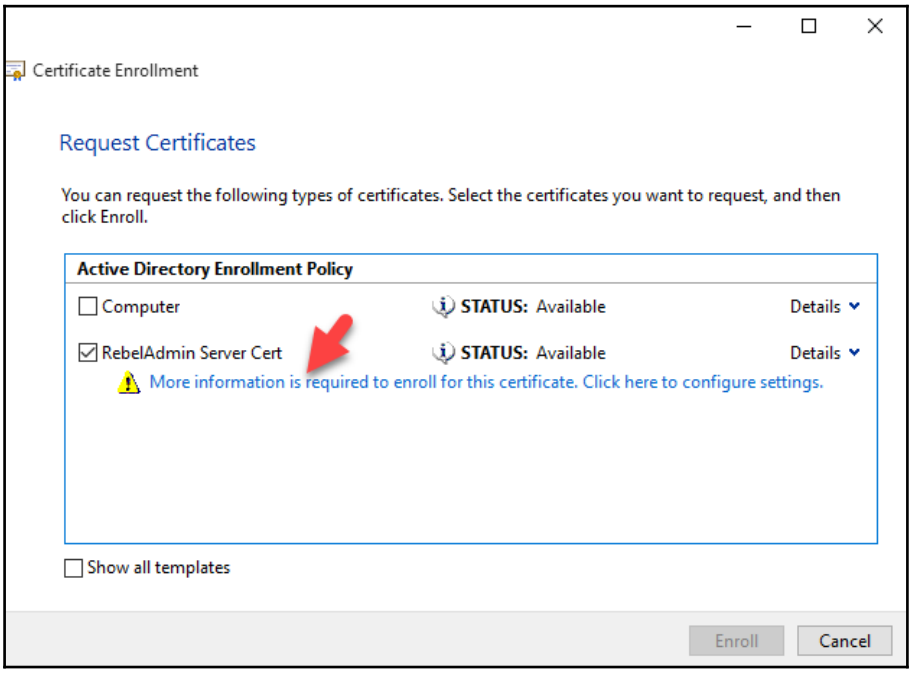


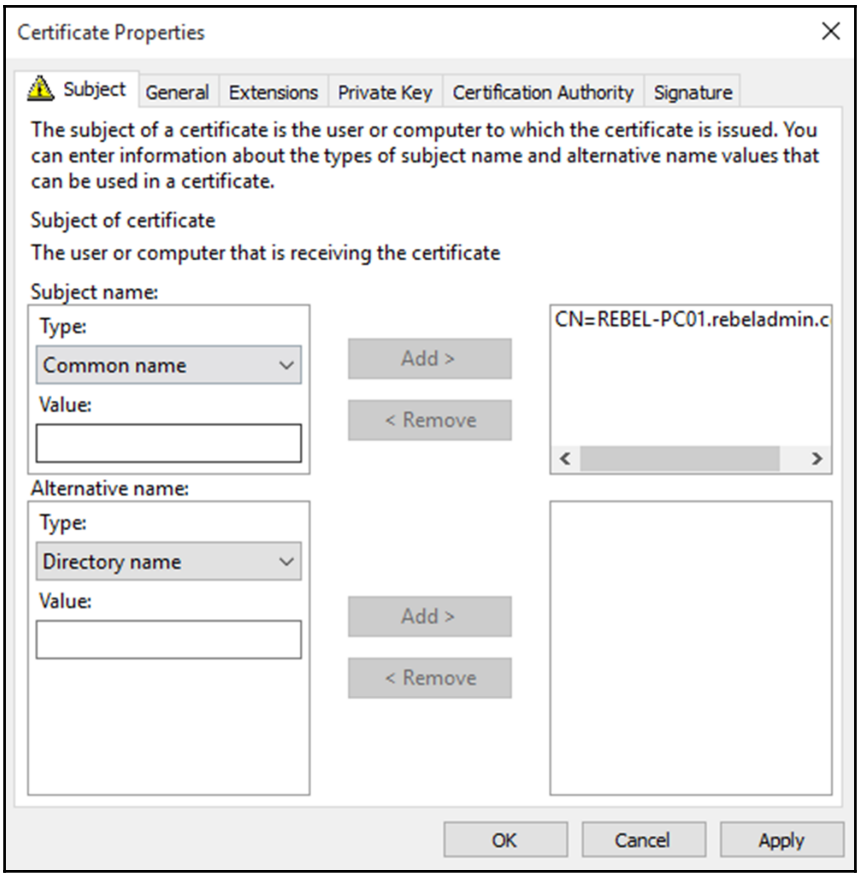

PKIView - [Enterprise PKI\REBELAdmin Root CA (V0.0)]
File Action View Help
Enterprise PKI
REBELAdmin Root CA (V0.0)
REBELAdmin IssuingCA (V0
Name
Status
Expiration Date
Location
REBELAdmin IssuingCA (V0....
OK
CA Certificate
OK
22/03/2037 21:05
AIA Location #1
OK
22/03/2037 21:05
ldap:///CN=REBELAdmin%20Root%20CA,CN
AIA Location #2
OK
22/03/2037 21:05
http://crt.rebeladmin.com/CertEnroll/REBEL-
CDP Location #1
OK
22/06/2017 11:10
ldap:///CN=REBELAdmin%20Root%20CA,CN
CDP Location #2
OK
22/06/2017 11:10
http://crt.rebeladmin.com/CertEnroll/REBELA

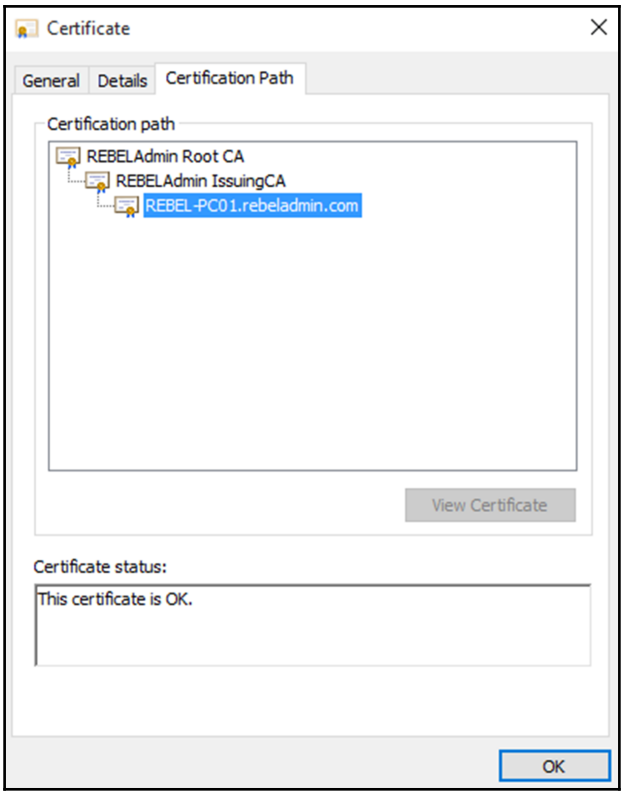

1
Console Root
Certificate Templates
Template Display Name
Schema Version
Version
Intended Purposes
CA Exchange 2 106.0 Private Key Archival
CEP Encryption 1 4.1
Code Signing 1 3.1
Computer 1 5.1
Cross Certification Authority 2 105.0
Directory Email Replication 2 115.0 Directory Service Email Replication
Domain Controller 1 4.1
Domain Controller Authentication 2 110.0 Client Authentication, Server Authentication,
EFS Recovery Agent 1 6.1
Enrollment Agent 1 4.1
Enrollment Agent (Computer) 1 5.1
Exchange Enrollment Agent (Offline requ... 1 4.1
Exchange Signature Only 1 6.1
Exchange User 1 7.1
IPSec 1 8.1
IPSec (Offline request) 1 7.1
Kerberos Authentication 2 110.0 Client Authentication, Server Authentication,
Key Recovery Agent 2 105.0 Key Recovery Agent
OCSP Response Signing 3 101.0 OCSP Signing
RAS and IAS Server 101.0 Client Authentication, Server Authentication
Root Certification Authority 5.1
Router (Offline request) 1 4.1
Smartcard Logon 6.1
Smartcard 11.1
Subordina 5.1
Trust List S 3.1
User 3.1
User Signa 4.1
Web Serve 4.1
Workstation Authentication 2 101.0 Client Authentication
2
Duplicate Template
All Tasks
Properties
Help


Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Template display name:
RebelAdmin Server Cert
Template name:
RebelAdminServerCert
Validity period:
2
years
Renewal period:
6
weeks
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory
OK
Cancel
Apply
Help

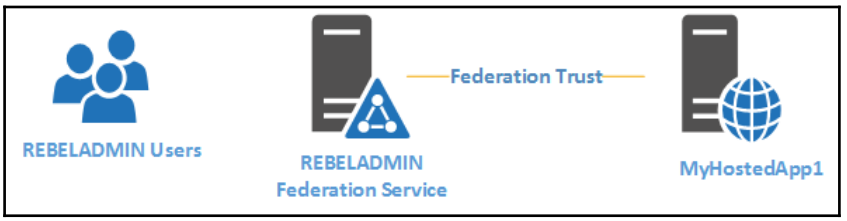

certsrv - [Certification Authority (Local)\REBELAdmin IssuingCA\Certificate Templates]
File Action View Help
Certification Authority (Local)
REBELAdmin IssuingCA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Enable Certificate Templates
Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until
information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.
Name
Intended Purpose
Exchange User
Secure Email
IPSec
IP security IKE intermediate
IPSec (Offline request)
IP security IKE intermediate
Key Recovery Agent
Key Recovery Agent
OCSP Response Signing
OCSP Signing
RAS and IAS Server
Client Authentication, Server Authentication
RebelAdmin Server Cert
Server Authentication
Router (Offline request)
Client Authentication
Smartcard Logon
Client Authentication, Smart Card Logon
Smartcard User
Secure Email, Client Authentication, Smart Card Logon
OK
Cancel

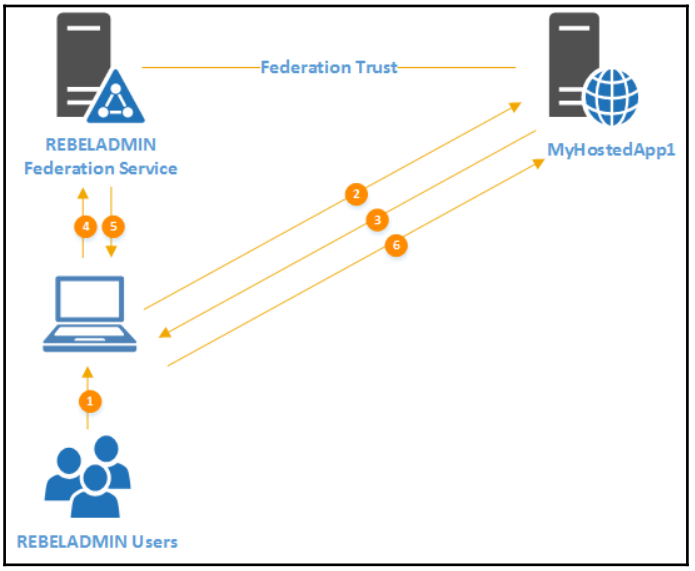

Certificate Enrollment
Request Certificates
You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.
Active Directory Enrollment Policy
Computer
STATUS: Available
Details
RebelAdmin Server Cert
STATUS: Available
Details
More information is required to enroll for this certificate. Click here to configure settings.
Show all templates
Enroll
Cancel

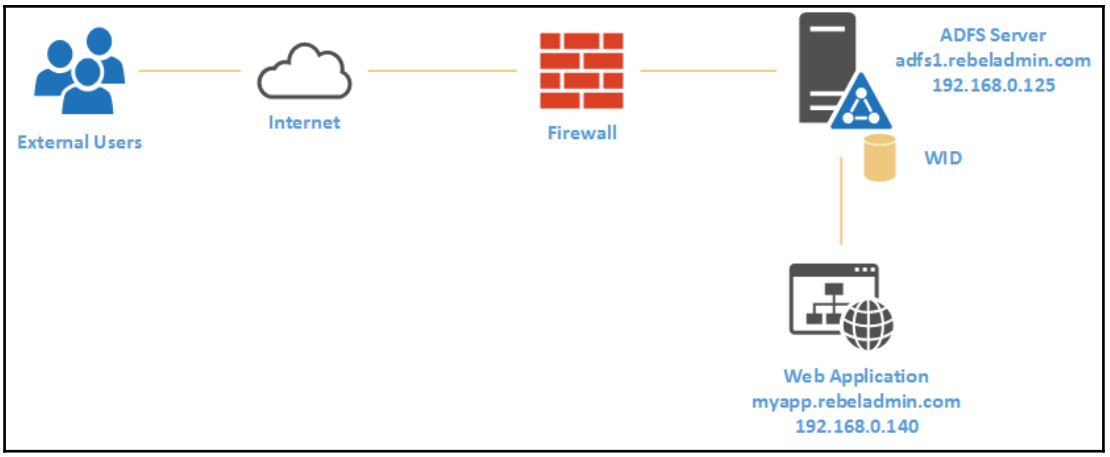

Certificate Properties
Subject
General
Extensions
Private Key
Certification Authority
Signature
The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.
Subject of certificate
The user or computer that is receiving the certificate
Subject name:
Type:
Common name
Value:
Add >
< Remove
CN=REBEL-PC01.rebeladmin.c
Alternative name:
Type:
Directory name
Value:
Add >
< Remove
OK
Cancel
Apply

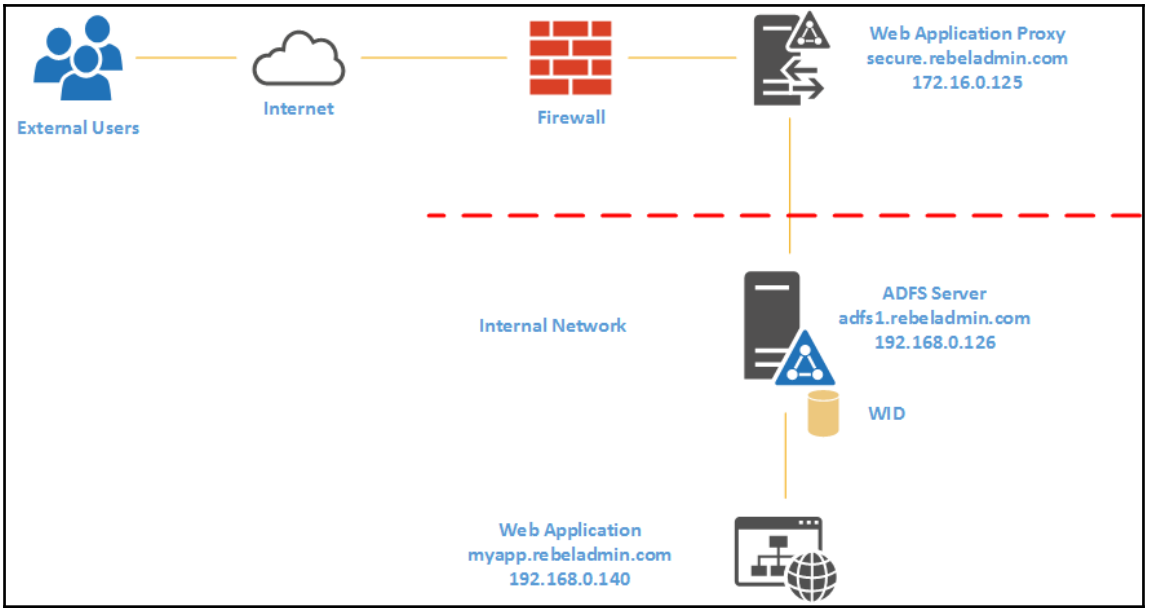

Certificate
General
Details
Certification Path
Certification path
REBELAdmin Root CA
REBELAdmin IssuingCA
REBEL-PC01.rebeladmin.com
View Certificate
Certificate status:
This certificate is OK.
OK

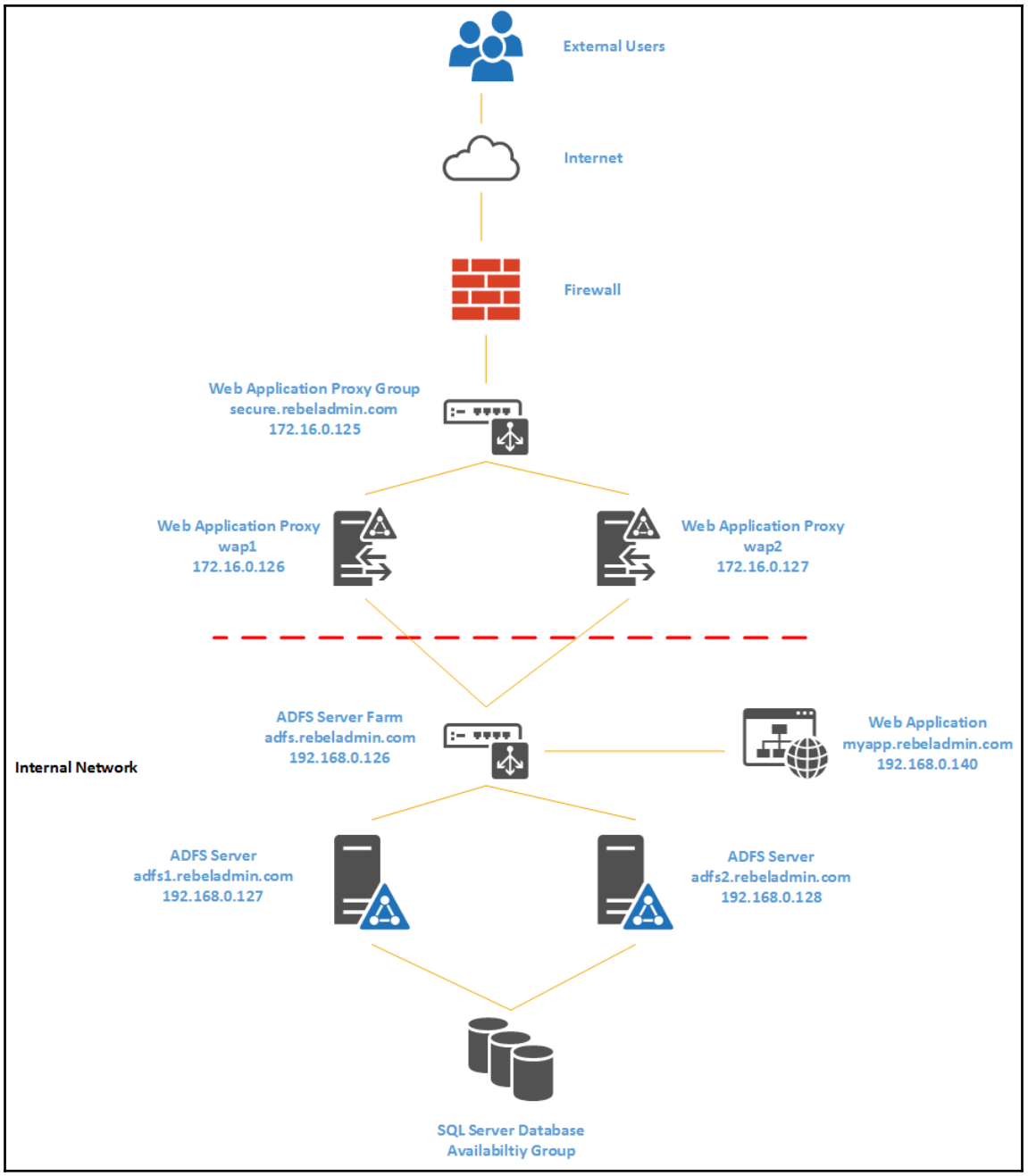
Chapter 13: Active Directory Federation Services

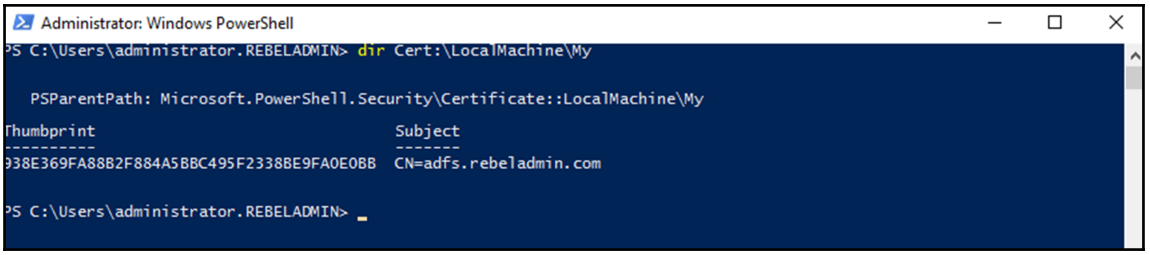


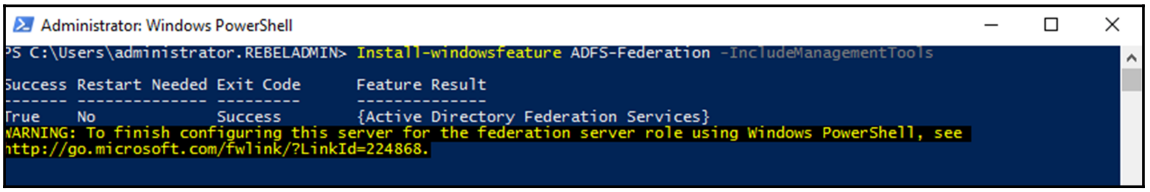


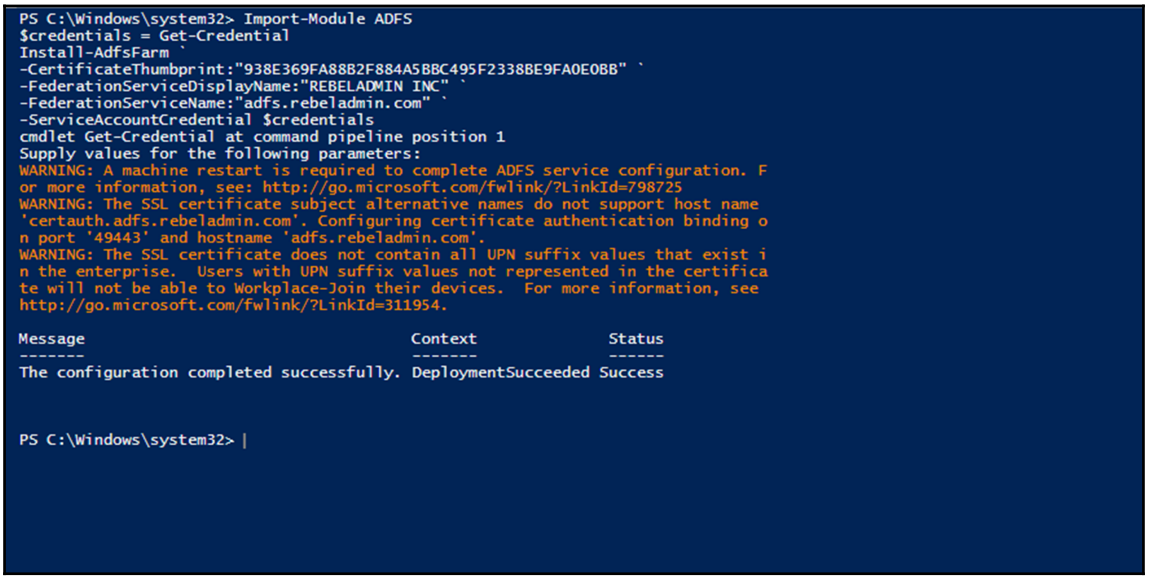

External Users
Internet
Firewall
ADFS Server
adfs1.rebeladmin.com
192.168.0.125
WID
Web Application
myapp.rebeladmin.com
192.168.0.140

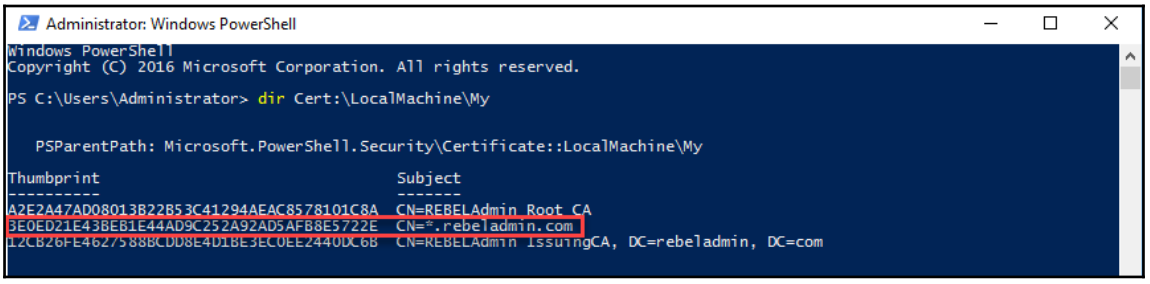

External Users
Internet
Firewall
Web Application Proxy
secure.rebeladmin.com
172.16.0.125
Internal Network
ADFS Server
adfs1.rebeladmin.com
192.168.0.126
WID
Web Application
myapp.rebeladmin.com
192.168.0.140


External Users
Internet
Firewall
Web Application Proxy Group
secure.rebeladmin.com
172.16.0.125
Web Application Proxy
wap1
172.16.0.126
Web Application Proxy
wap2
172.16.0.127
ADFS Server Farm
adfs.rebeladmin.com
192.168.0.126
Web Application
myapp.rebeladmin.com
192.168.0.140
Internal Network
ADFS Server
adfs1.rebeladmin.com
192.168.0.127
ADFS Server
adfs2.rebeladmin.com
192.168.0.128
SQL Server Database
Availabiltiy Group


Administrator: Windows PowerShell
PS C:\Users\administrator.REBELADMIN> dir Cert:\LocalMachine\My
PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint Subject
938E369FA88B2F884A5BBC495F2338BE9FA0E0BB CN=adfs.rebeladmin.com
PS C:\Users\administrator.REBELADMIN>


Administrator: Windows PowerShell
PS C:\Users\administrator.REBELADMIN> Install-windowsfeature ADFS-Federation -IncludeManagementTools
Success Restart Needed Exit Code Feature Result
True No Success {Active Directory Federation Services}
WARNING: To finish configuring this server for the federation server role using Windows PowerShell, see
http://go.microsoft.com/fwlink/?LinkId=224868.

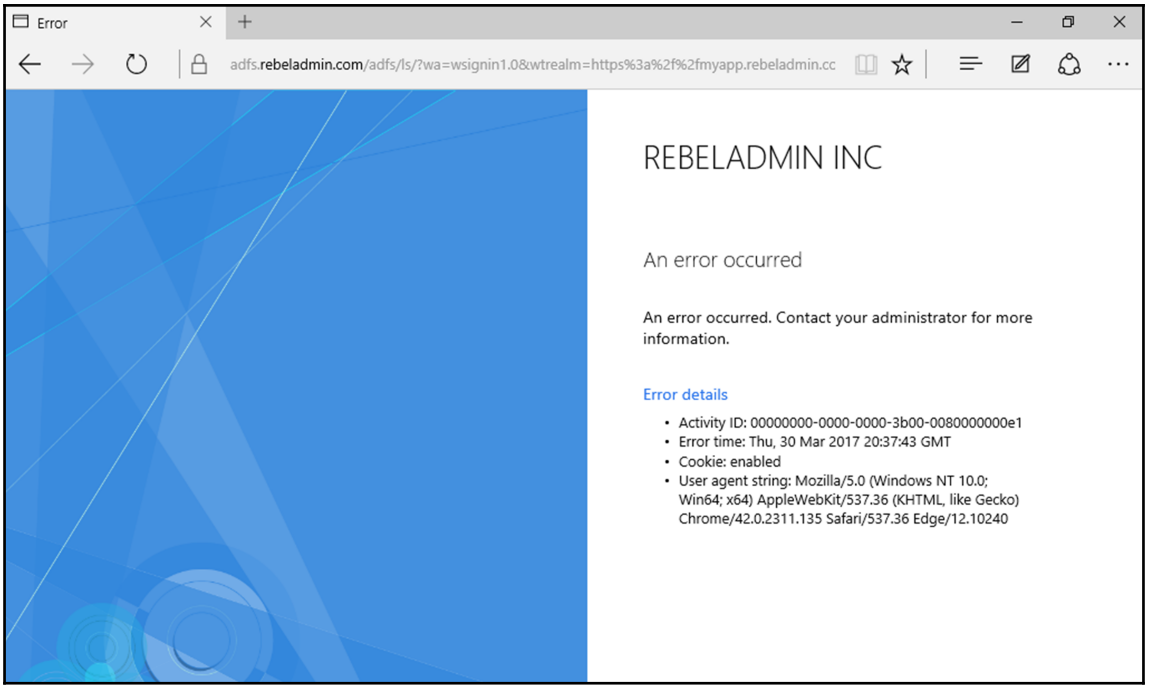

PS C:\Windows\system32> Import-Module ADFS
$credentials = Get-Credential
Install-AdfsFarm `
-CertificateThumbprint:"938E369FA88B2F884A5BBC495F2338BE9FA0E0BB" `
-FederationServiceDisplayName:"REBELADMIN INC" `
-FederationServiceName:"adfs.rebeladmin.com" `
-ServiceAccountCredential $credentials
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
WARNING: A machine restart is required to complete ADFS service configuration. F
or more information, see: http://go.microsoft.com/fwlink/?LinkId=798725
WARNING: The SSL certificate subject alternative names do not support host name
'certauth.adfs.rebeladmin.com'. Configuring certificate authentication binding o
n port '49443' and hostname 'adfs.rebeladmin.com'.
WARNING: The SSL certificate does not contain all UPN suffix values that exist i
n the enterprise. Users with UPN suffix values not represented in the certifica
te will not be able to Workplace-Join their devices. For more information, see
http://go.microsoft.com/fwlink/?LinkId=311954.
Message Context Status
The configuration completed successfully. DeploymentSucceeded Success
PS C:\Windows\system32>

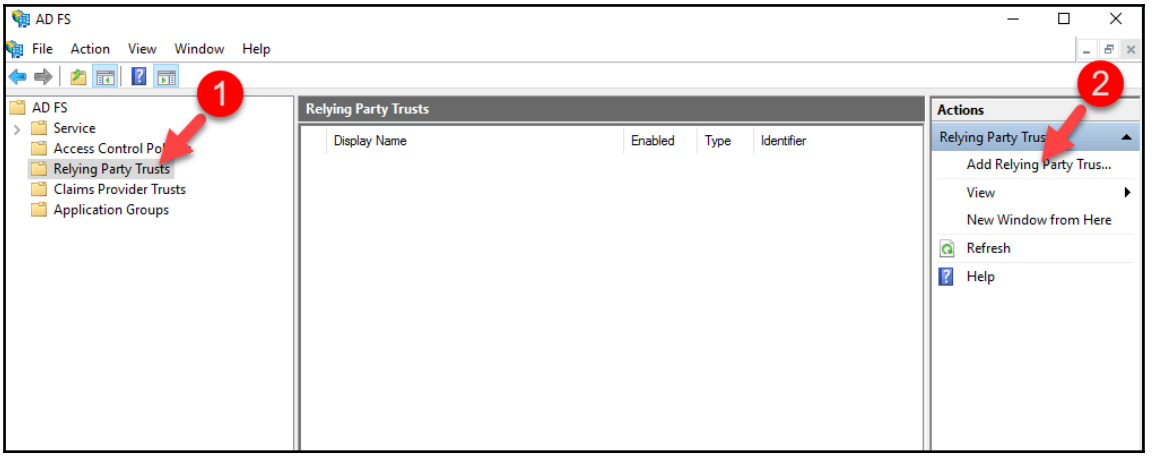

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> dir Cert:\LocalMachine\My
PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint Subject
A2E2A47AD08013B22B53C41294AEAC8578101C8A CN=REBELAdmin Root CA
3E0ED21E43BEB1E44AD9C252A92AD5AFB8E5722E CN=*.rebeladmin.com
12CB26FE4627588BCDD8E4D1BE3EC0EE2440DC6B CN=REBELAdmin IssuingCA, DC=rebeladmin, DC=com

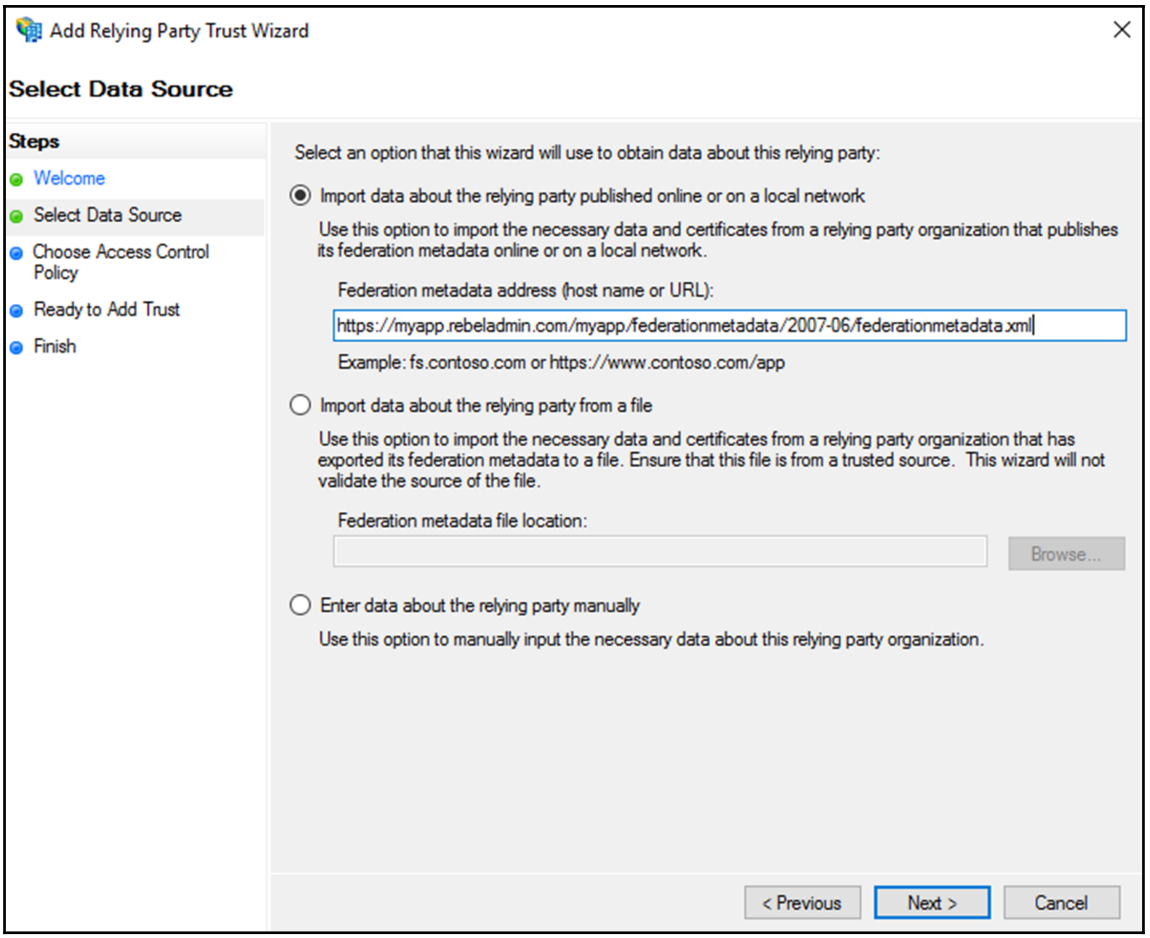
```
PS C:\Users\Administrator> Install-WindowsFeature Web-Application-Proxy -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {RAS Connection Manager Administration Kit...
WARNING: To finish configuring this server for the Web Application Proxy role service using Windows PowerShell, see
http://go.microsoft.com/fwlink/?LinkId=294322.
```

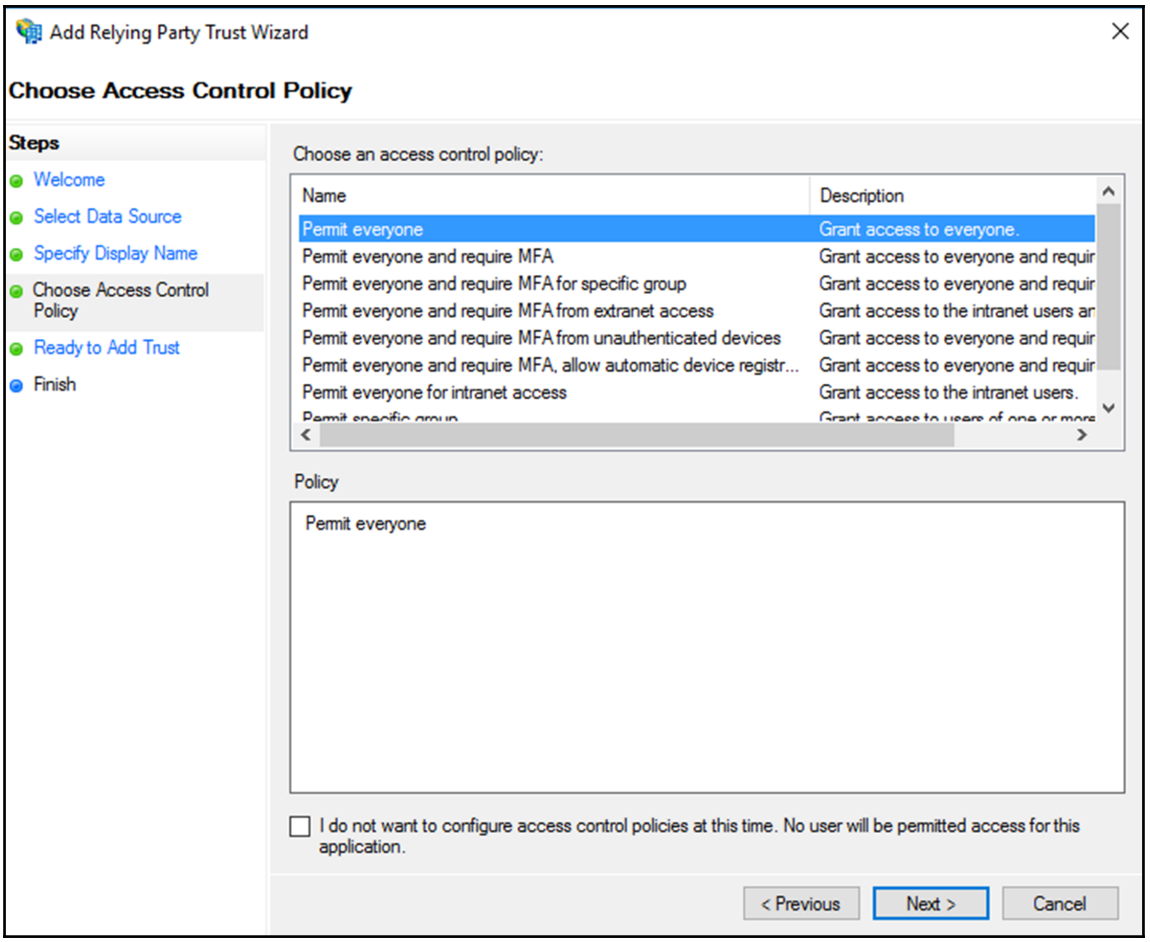
```
PS C:\Windows\system32> $credentials = Get-Credential
Install-WebApplicationProxy -FederationServiceName "adfs.rebeladmin.com" -FederationServiceTrustCredential $credentials -CertificateThum
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
WARNING: Given SSL certificate does not match the STS certificate. Requests doin
g NTLM authentication over the proxy will fail.
WARNING: A machine restart is required to complete ADFS service configuration. F
or more information, see: http://go.microsoft.com/fwlink/?LinkId=798725

Message                                 Context            Status
-------                                 -------            ------
The configuration completed successfully. DeploymentSucceeded Success
```

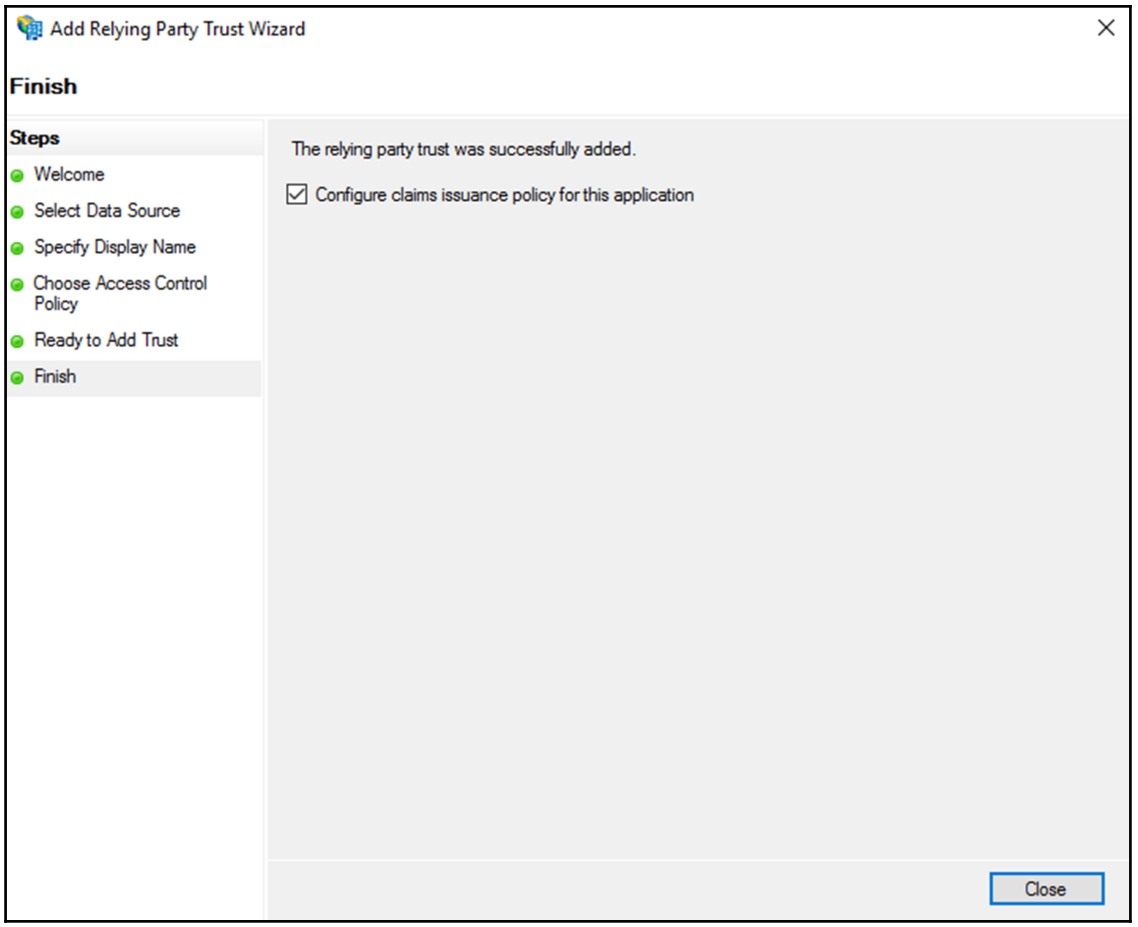
```
PS C:\Users\administrator.REBELADMIN> Get-WinEvent "AD FS/Admin" | Where-Object {$_.ID -eq "396"} | fl


TimeCreated  : 30/03/2017 00:37:38
ProviderName : AD FS
Id           : 396
Message      : The trust between the federation server proxy and the Federation Service was renewed successfully.

               Proxy trust certificate subject: CN=ADFS ProxyTrust - REBEL-CRTROOT.
               Proxy trust certificate old thumbprint: 0A191B3E42B8B9B826F8ED1AE6BEC2C142B0CABA.
               Proxy trust certificate new thumbprint: D0CA59939D1427A95FA1EEE09DAD2B950040E4A0.

TimeCreated  : 30/03/2017 00:36:37
ProviderName : AD FS
Id           : 396
Message      : The trust between the federation server proxy and the Federation Service was renewed successfully.

               Proxy trust certificate subject: CN=ADFS ProxyTrust - REBEL-CRTROOT.
               Proxy trust certificate old thumbprint: 0A191B3E42B8B9B826F8ED1AE6BEC2C142B0CABA.
               Proxy trust certificate new thumbprint: D465695A3D4BE6137903645177E2569ADB8411BE.

TimeCreated  : 30/03/2017 00:27:56
ProviderName : AD FS
Id           : 396
Message      : The trust between the federation server proxy and the Federation Service was renewed successfully.

               Proxy trust certificate subject: CN=ADFS ProxyTrust - REBEL-CRTROOT.
               Proxy trust certificate old thumbprint: 0A191B3E42B8B9B826F8ED1AE6BEC2C142B0CABA.
               Proxy trust certificate new thumbprint: F4C1680F09C36C278B2FB981BFD5FC2415C8E06E.

TimeCreated  : 30/03/2017 00:26:55
ProviderName : AD FS
Id           : 396
Message      : The trust between the federation server proxy and the Federation Service was renewed successfully.

               Proxy trust certificate subject: CN=ADFS ProxyTrust - REBEL-CRTROOT.
               Proxy trust certificate old thumbprint: 0A191B3E42B8B9B826F8ED1AE6BEC2C142B0CABA.
               Proxy trust certificate new thumbprint: FA394B73302BD662407A374FCADC18306964B3B2.
```

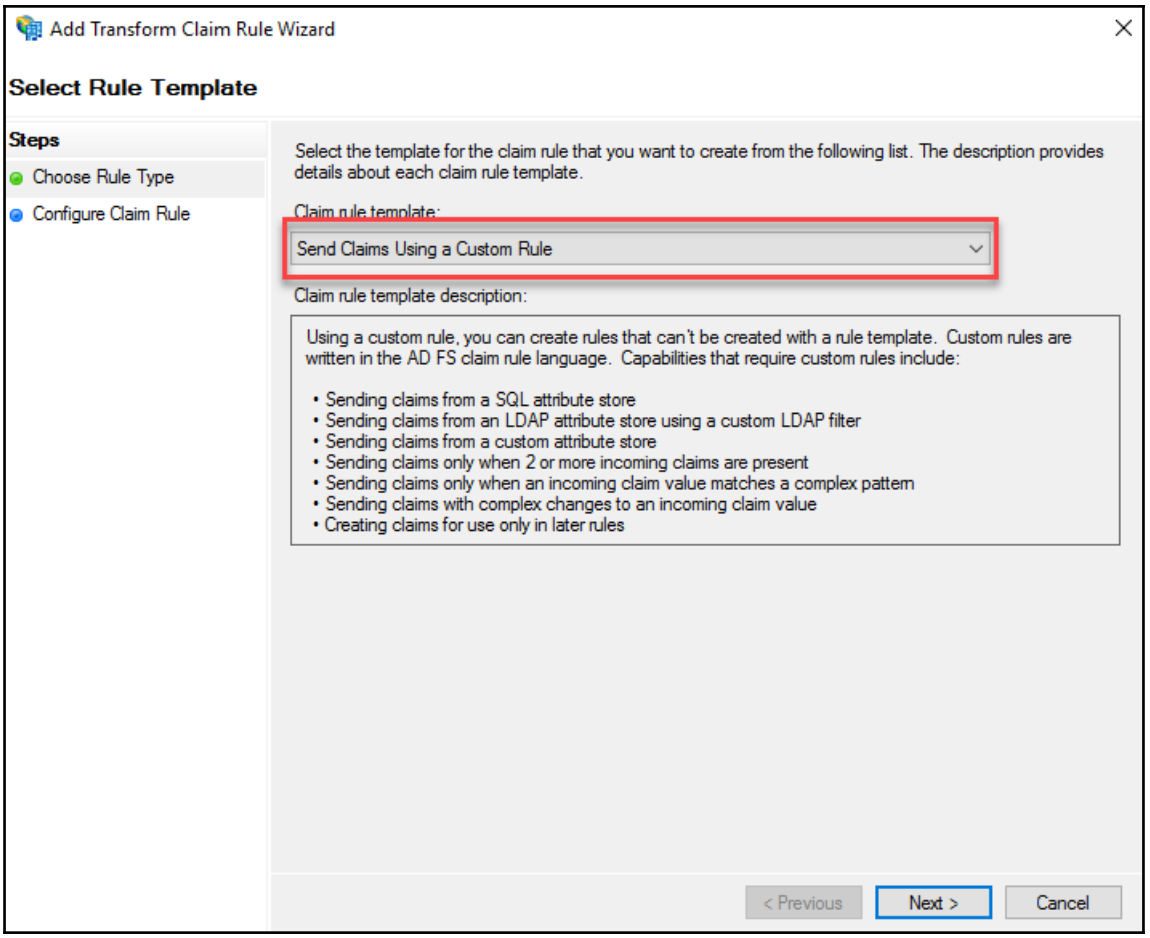

Error
adfs.rebeladmin.com/adfs/ls/?wa=wsignin1.0&wtrealm=https%3a%2f%2fmyapp.rebeladmin.cc
REBELADMIN INC
An error occurred
An error occurred. Contact your administrator for more information.
Error details
Activity ID: 00000000-0000-0000-3b00-0080000000e1
Error time: Thu, 30 Mar 2017 20:37:43 GMT
Cookie: enabled
User agent string: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.10240

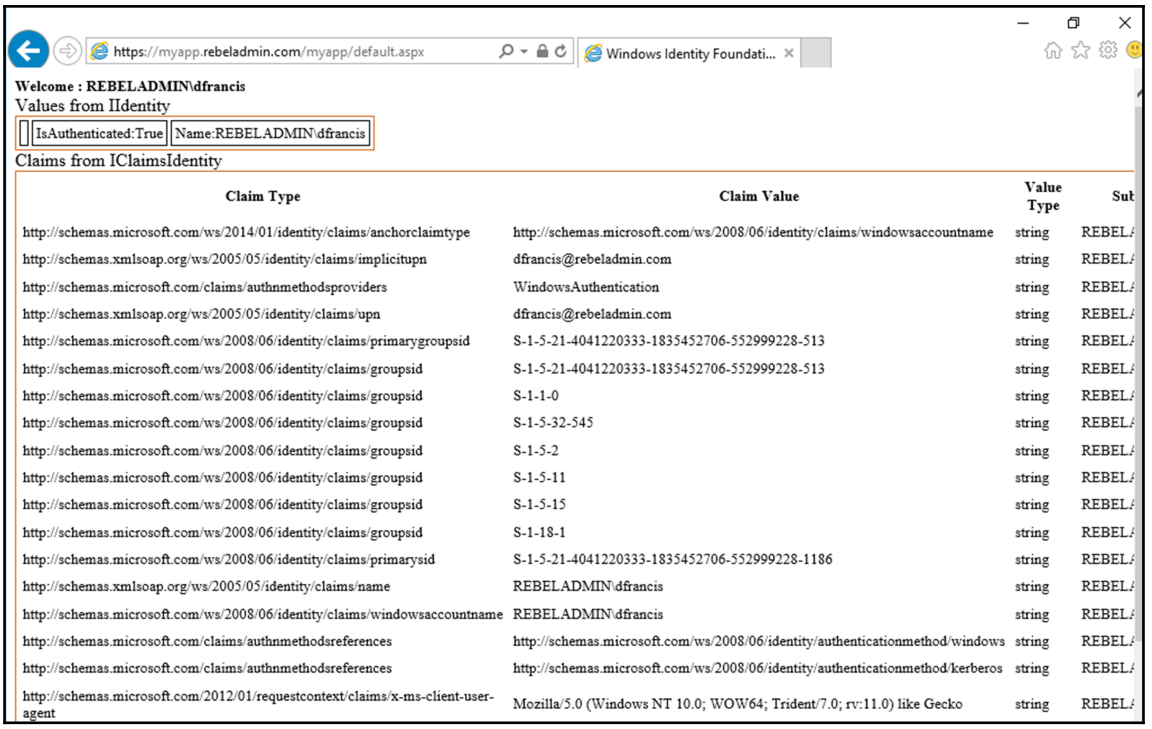

AD FS
File Action View Window Help
1
2
AD FS
Service
Access Control Po
Relying Party Trusts
Claims Provider Trusts
Application Groups
Relying Party Trusts
Display Name
Enabled
Type
Identifier
Actions
Relying Party Trus
Add Relying Party Trus...
View
New Window from Here
Refresh
Help


Add Relying Party Trust Wizard
Select Data Source
Steps
Welcome
Select Data Source
Choose Access Control Policy
Ready to Add Trust
Finish
Select an option that this wizard will use to obtain data about this relying party:
Import data about the relying party published online or on a local network
Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.
Federation metadata address (host name or URL):
https://myapp.rebeladmin.com/myapp/federationmetadata/2007-06/federationmetadata.xml
Example: fs.contoso.com or https://www.contoso.com/app
Import data about the relying party from a file
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.
Federation metadata file location:
Browse...
Enter data about the relying party manually
Use this option to manually input the necessary data about this relying party organization.
< Previous
Next >
Cancel

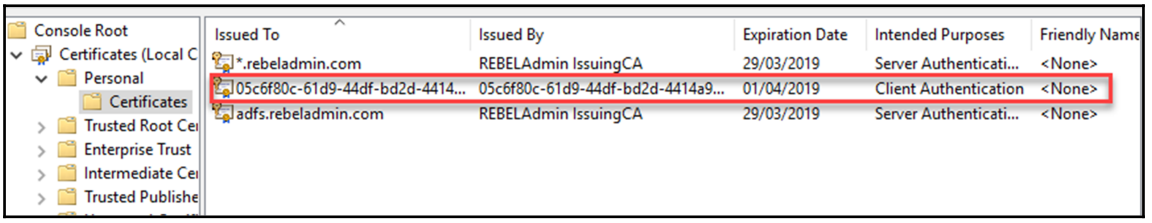

Add Relying Party Trust Wizard
Choose Access Control Policy
Steps
Welcome
Select Data Source
Specify Display Name
Choose Access Control Policy
Ready to Add Trust
Finish
Choose an access control policy:
Name
Description
Permit everyone
Grant access to everyone.
Permit everyone and require MFA
Grant access to everyone and requir
Permit everyone and require MFA for specific group
Grant access to everyone and requir
Permit everyone and require MFA from extranet access
Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices
Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...
Grant access to everyone and requir
Permit everyone for intranet access
Grant access to the intranet users.
Policy
Permit everyone
I do not want to configure access control policies at this time. No user will be permitted access for this application.
< Previous
Next >
Cancel


Add Relying Party Trust Wizard
Finish
Steps
Welcome
Select Data Source
Specify Display Name
Choose Access Control Policy
Ready to Add Trust
Finish
The relying party trust was successfully added.
Configure claims issuance policy for this application
Close

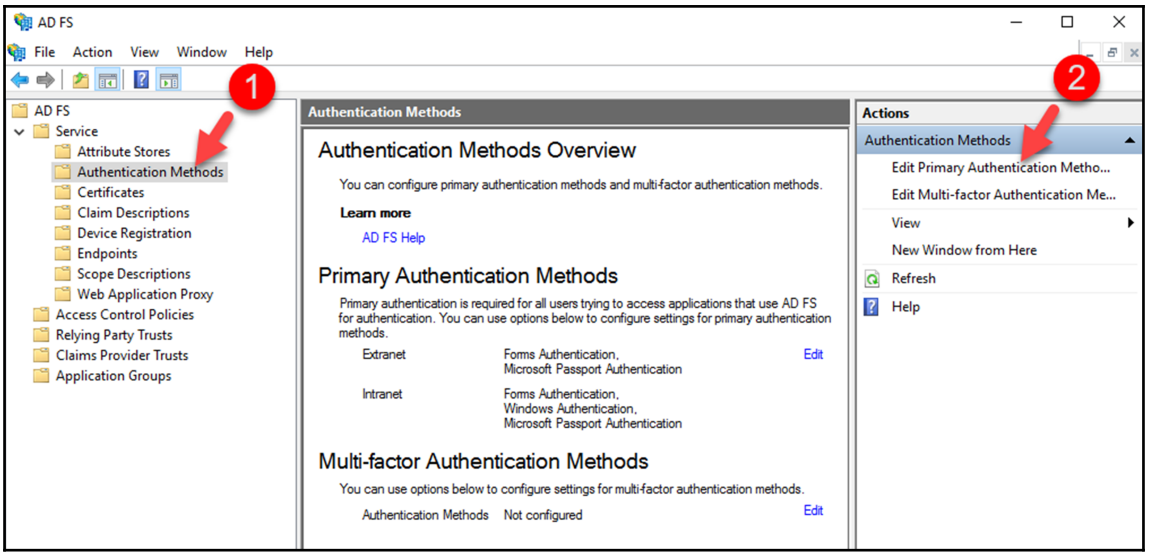

Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Claim rule template:
Send Claims Using a Custom Rule
Claim rule template description:
Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:
• Sending claims from a SQL attribute store
• Sending claims from an LDAP attribute store using a custom LDAP filter
• Sending claims from a custom attribute store
• Sending claims only when 2 or more incoming claims are present
• Sending claims only when an incoming claim value matches a complex pattern
• Sending claims with complex changes to an incoming claim value
• Creating claims for use only in later rules
< Previous
Next >
Cancel

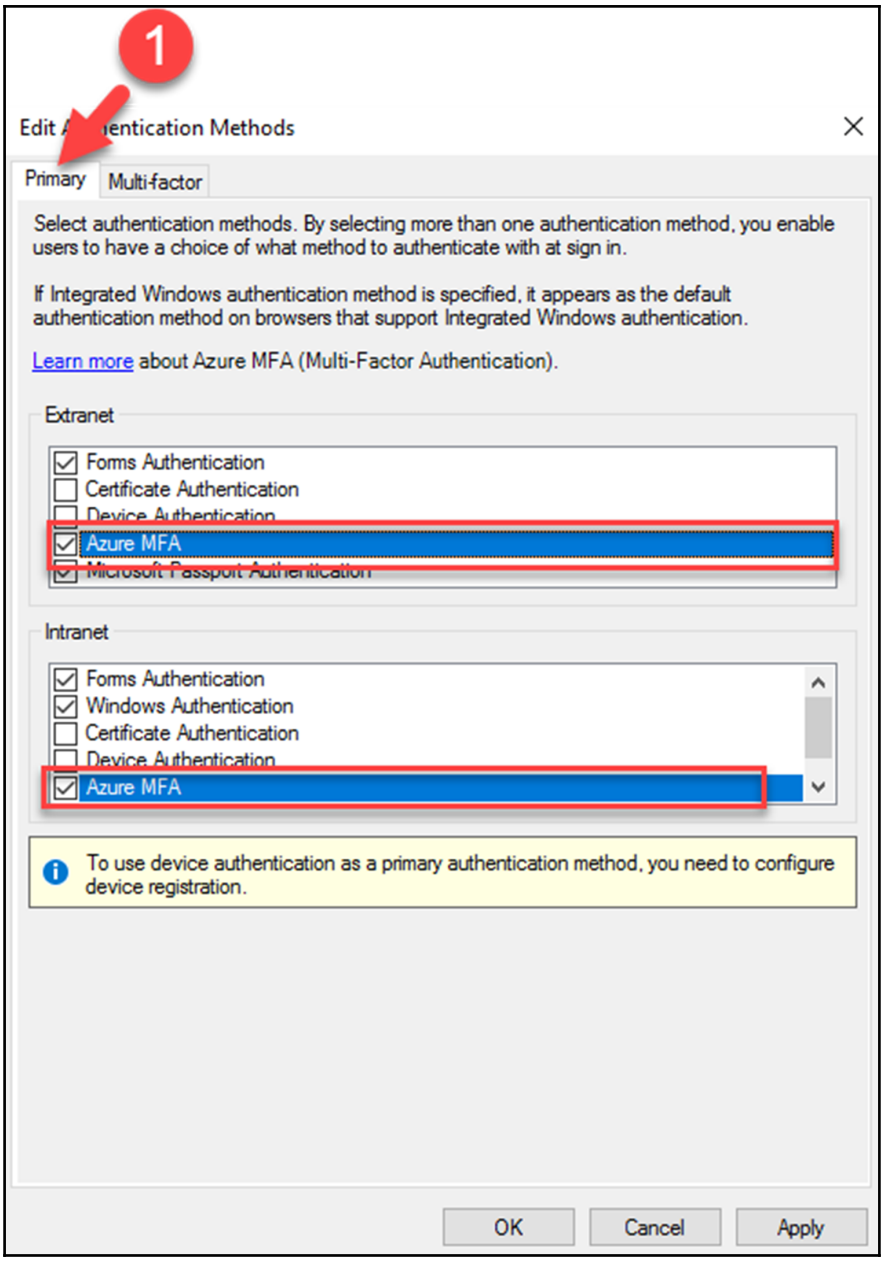


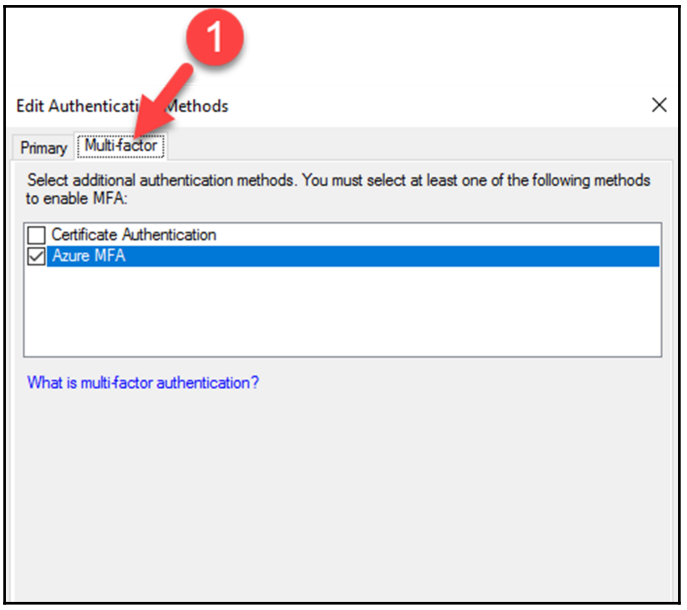

```
Environment           : AzureCloud
Account               : dcadmin@REBELADMIN.onmicrosoft.com
TenantId              : 05c6f80c-61d9-44df-bd2d-4414a983c1d4
SubscriptionId        :
SubscriptionName      :
CurrentStorageAccount :
```



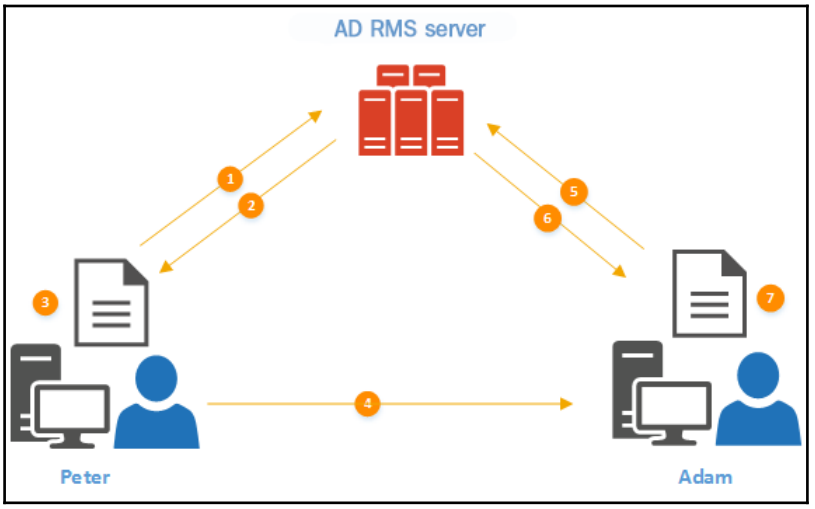

```
PS C:\Users\administrator.REBELADMIN\Desktop> Set-AdfsAzureMfaTenant -TenantId 05c6f80c-61d9-44df-bd2d-4414a983c1d4 -Cli
entId 981f26a1-7f43-403b-a875-f8b09b8cd720
WARNING: PS0177: The authentication provider configuration data was successfully updated.  Before your changes take
effect, you must restart the AD FS Windows Service on each server in the farm.
PS C:\Users\administrator.REBELADMIN\Desktop>
```


AD FS
File Action View Window Help
1
2
AD FS
Service
Attribute Stores
Authentication Methods
Certificates
Claim Descriptions
Device Registration
Endpoints
Scope Descriptions
Web Application Proxy
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Authentication Methods
Authentication Methods Overview
You can configure primary authentication methods and multi-factor authentication methods.
Learn more
AD FS Help
Primary Authentication Methods
Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure settings for primary authentication methods.
Extranet
Forms Authentication, Microsoft Passport Authentication
Edit
Intranet
Forms Authentication, Windows Authentication, Microsoft Passport Authentication
Multi-factor Authentication Methods
You can use options below to configure settings for multi-factor authentication methods.
Authentication Methods
Not configured
Edit
Actions
Authentication Methods
Edit Primary Authentication Metho...
Edit Multi-factor Authentication Me...
View
New Window from Here
Refresh
Help

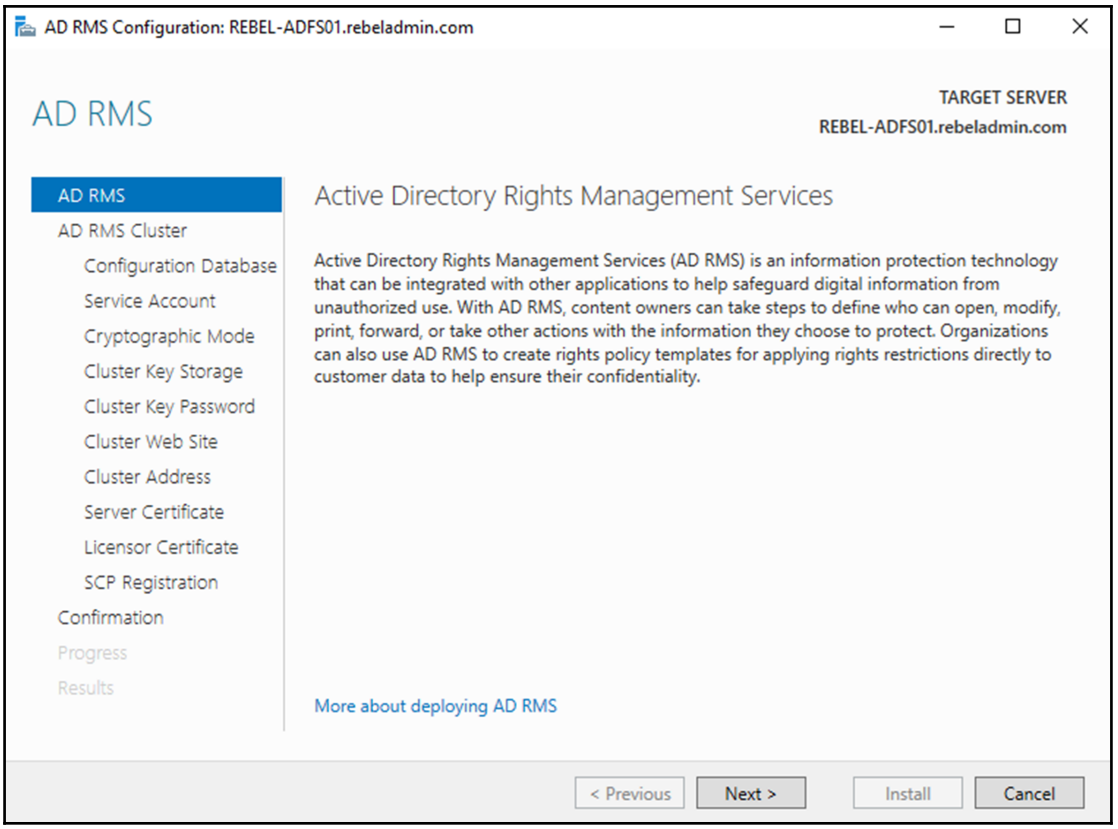

1
Edit A entication Methods
Primary
Multi-factor
Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in.
If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.
Learn more about Azure MFA (Multi-Factor Authentication).
Extranet
Forms Authentication
Certificate Authentication
Azure MFA
Intranet
Forms Authentication
Windows Authentication
Certificate Authentication
Azure MFA
To use device authentication as a primary authentication method, you need to configure device registration.
OK
Cancel
Apply

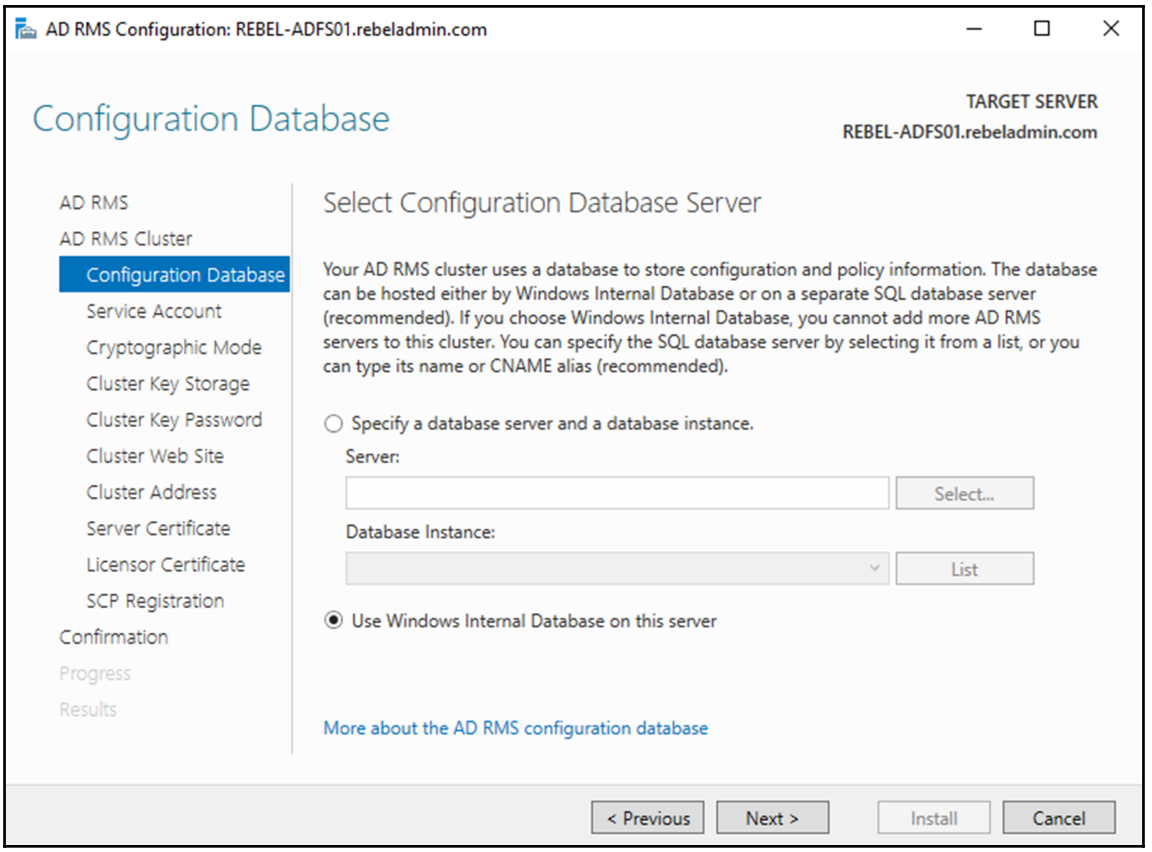

1
Edit Authenticati Methods
Primary
Multi-factor
Select additional authentication methods. You must select at least one of the following methods to enable MFA:
Certificate Authentication
Azure MFA
What is multi-factor authentication?

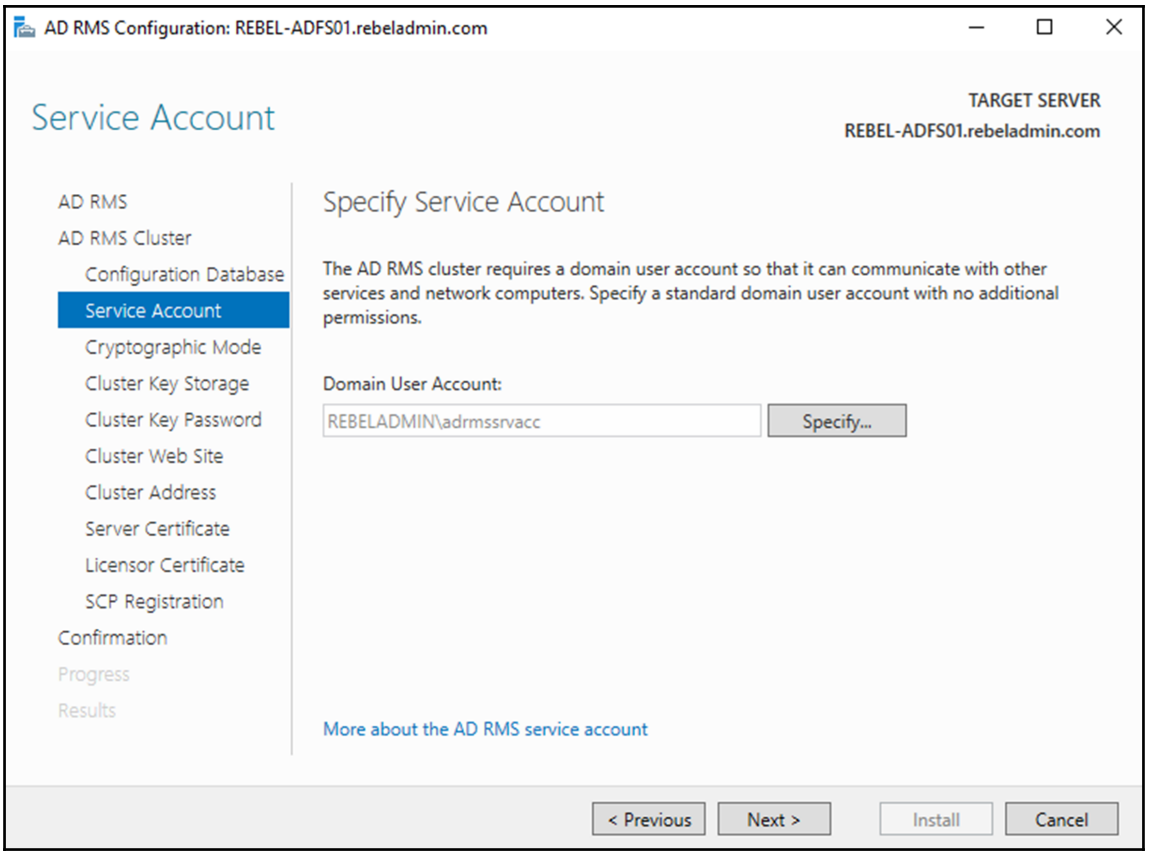
Chapter 14: Active Directory Rights Management Services

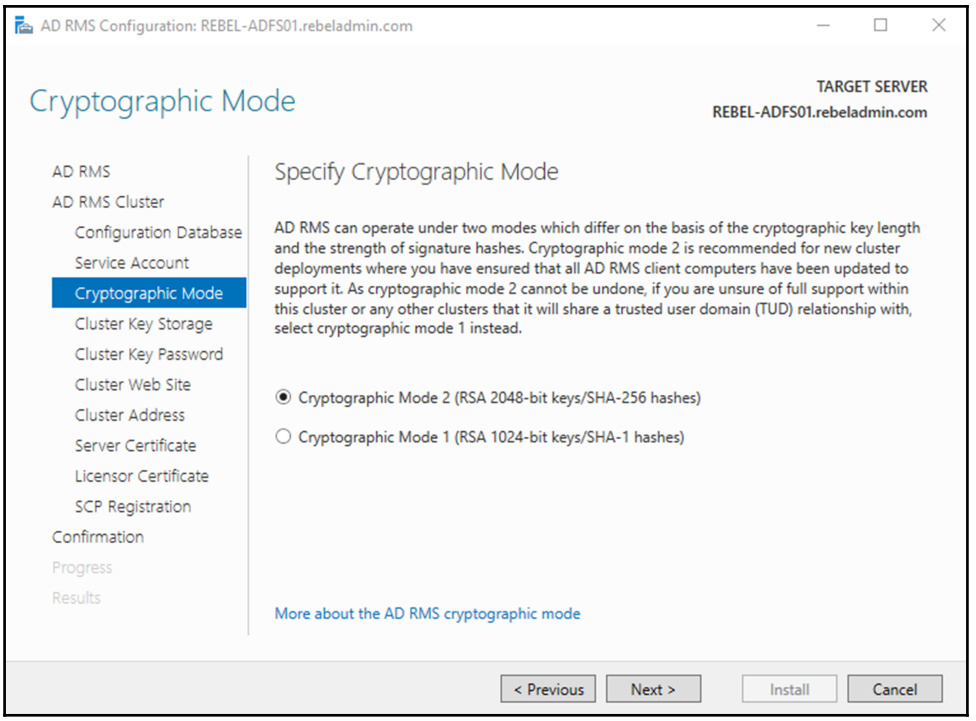


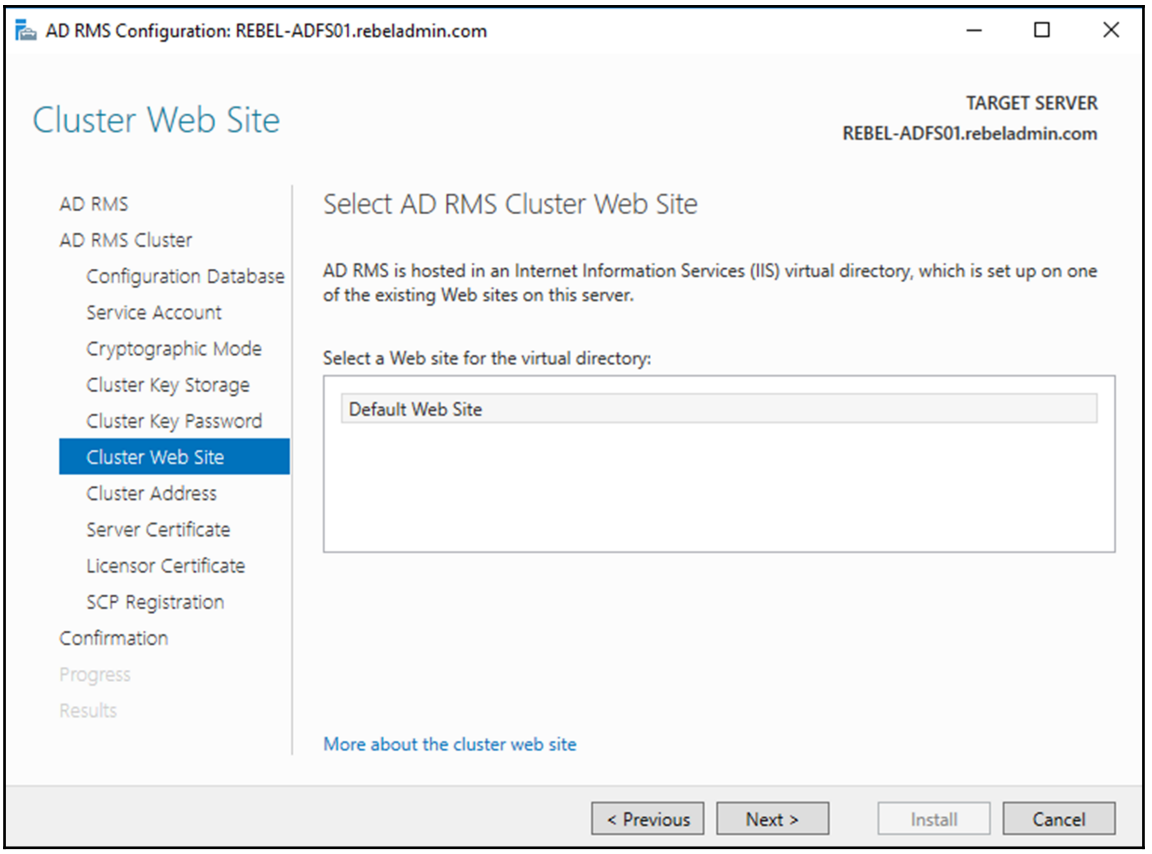

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.REBELADMIN> Install-WindowsFeature ADRMS -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Rights Management Servic...

PS C:\Users\administrator.REBELADMIN>
```

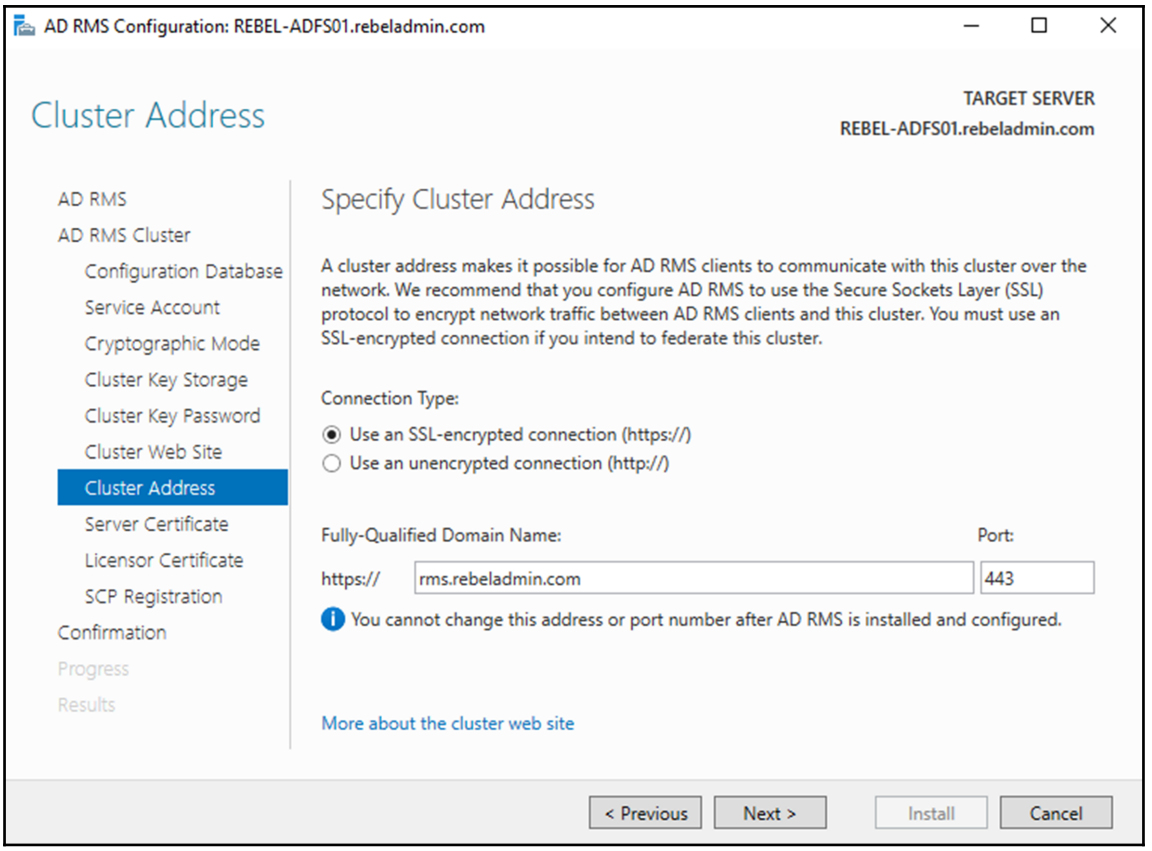

AD RMS Configuration: REBEL-ADFS01.rebeladmin.com
AD RMS
TARGET SERVER
REBEL-ADFS01.rebeladmin.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Active Directory Rights Management Services
Active Directory Rights Management Services (AD RMS) is an information protection technology that can be integrated with other applications to help safeguard digital information from unauthorized use. With AD RMS, content owners can take steps to define who can open, modify, print, forward, or take other actions with the information they choose to protect. Organizations can also use AD RMS to create rights policy templates for applying rights restrictions directly to customer data to help ensure their confidentiality.
More about deploying AD RMS
< Previous
Next >
Install
Cancel

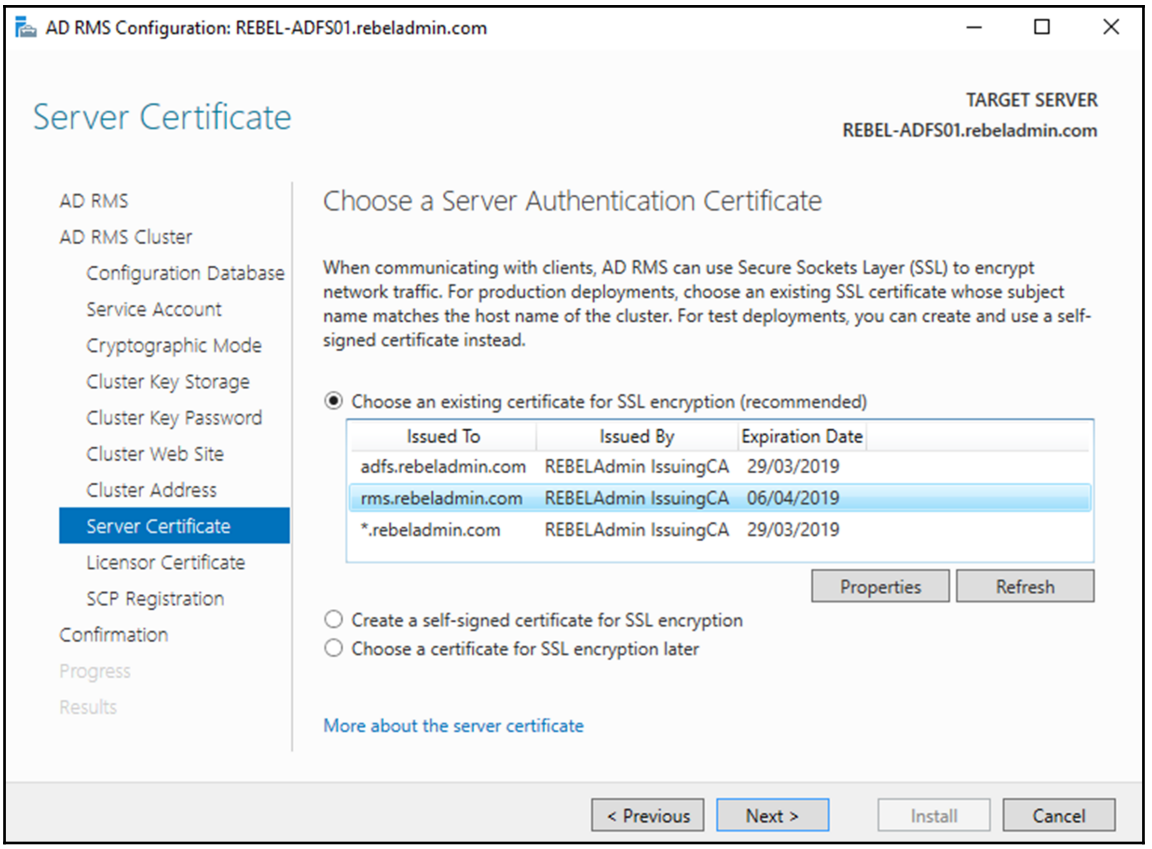

AD RMS Configuration: REBEL-ADFS01.rebeladmin.com
Configuration Database
TARGET SERVER
REBEL-ADFS01.rebeladmin.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Select Configuration Database Server
Your AD RMS cluster uses a database to store configuration and policy information. The database can be hosted either by Windows Internal Database or on a separate SQL database server (recommended). If you choose Windows Internal Database, you cannot add more AD RMS servers to this cluster. You can specify the SQL database server by selecting it from a list, or you can type its name or CNAME alias (recommended).
Specify a database server and a database instance.
Server:
Select...
Database Instance:
List
Use Windows Internal Database on this server
More about the AD RMS configuration database
< Previous
Next >
Install
Cancel

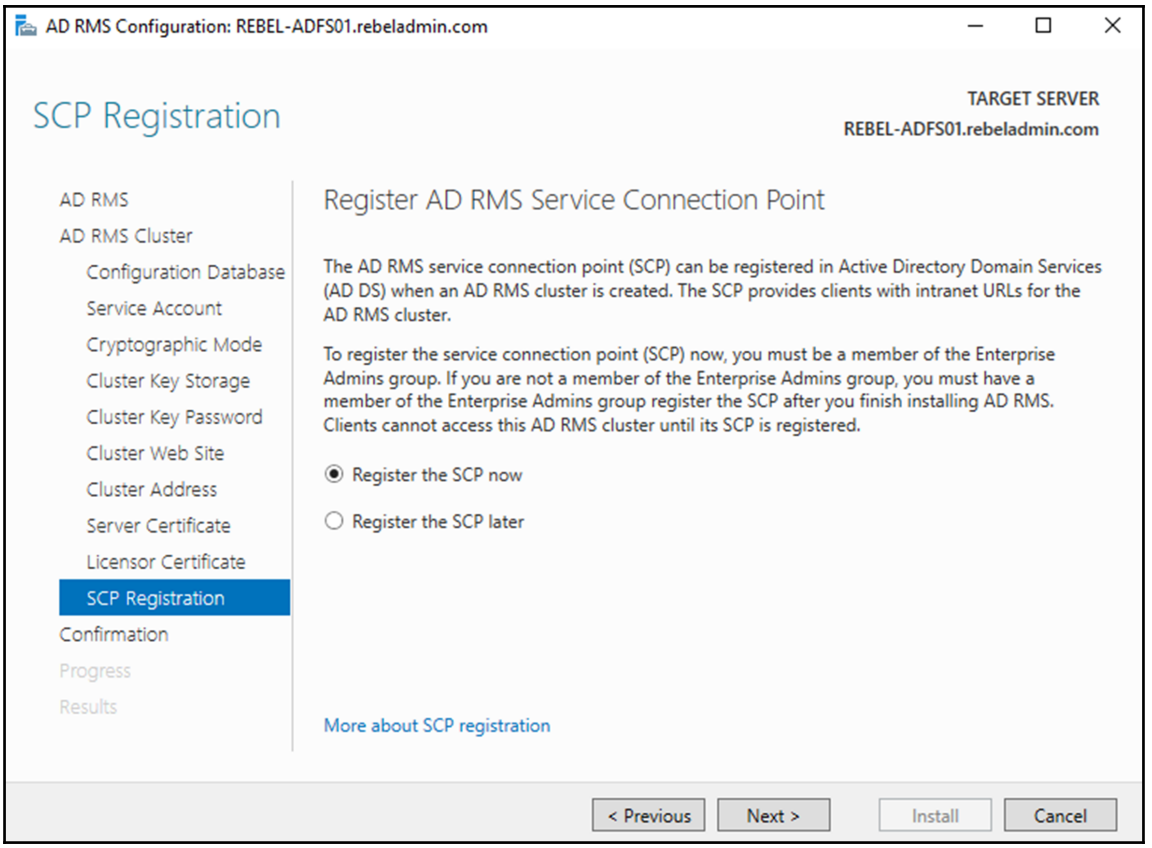

AD RMS Configuration: REBEL-ADFS01.rebeladmin.com
Service Account
TARGET SERVER
REBEL-ADFS01.rebeladmin.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify Service Account
The AD RMS cluster requires a domain user account so that it can communicate with other services and network computers. Specify a standard domain user account with no additional permissions.
Domain User Account:
REBELADMIN\adrmssrvacc
Specify...
More about the AD RMS service account
< Previous
Next >
Install
Cancel

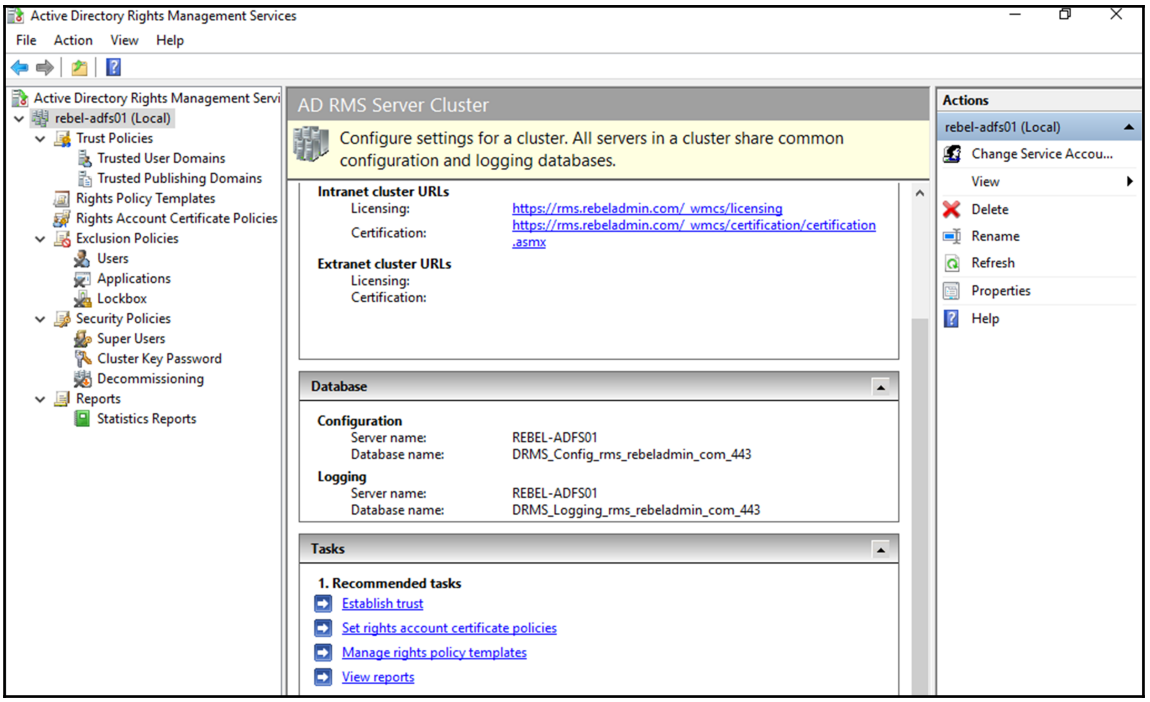

AD RMS Configuration: REBEL-ADFS01.rebeladmin.com
Cryptographic Mode
TARGET SERVER
REBEL-ADFS01.rebeladmin.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify Cryptographic Mode
AD RMS can operate under two modes which differ on the basis of the cryptographic key length and the strength of signature hashes. Cryptographic mode 2 is recommended for new cluster deployments where you have ensured that all AD RMS client computers have been updated to support it. As cryptographic mode 2 cannot be undone, if you are unsure of full support within this cluster or any other clusters that it will share a trusted user domain (TUD) relationship with, select cryptographic mode 1 instead.
Cryptographic Mode 2 (RSA 2048-bit keys/SHA-256 hashes)
Cryptographic Mode 1 (RSA 1024-bit keys/SHA-1 hashes)
More about the AD RMS cryptographic mode
< Previous
Next >
Install
Cancel

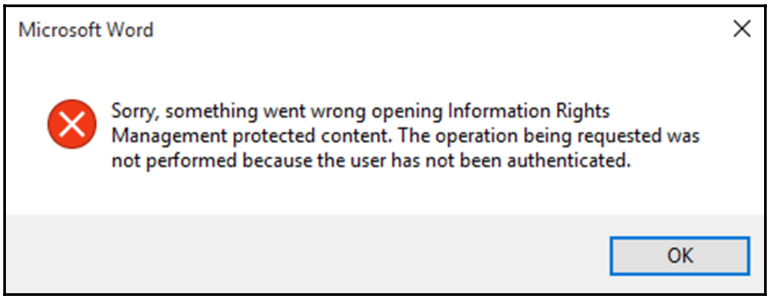

AD RMS Configuration: REBEL-ADFS01.rebeladmin.com
Cluster Web Site
TARGET SERVER
REBEL-ADFS01.rebeladmin.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Select AD RMS Cluster Web Site
AD RMS is hosted in an Internet Information Services (IIS) virtual directory, which is set up on one of the existing Web sites on this server.
Select a Web site for the virtual directory:
Default Web Site
More about the cluster web site
< Previous
Next >
Install
Cancel

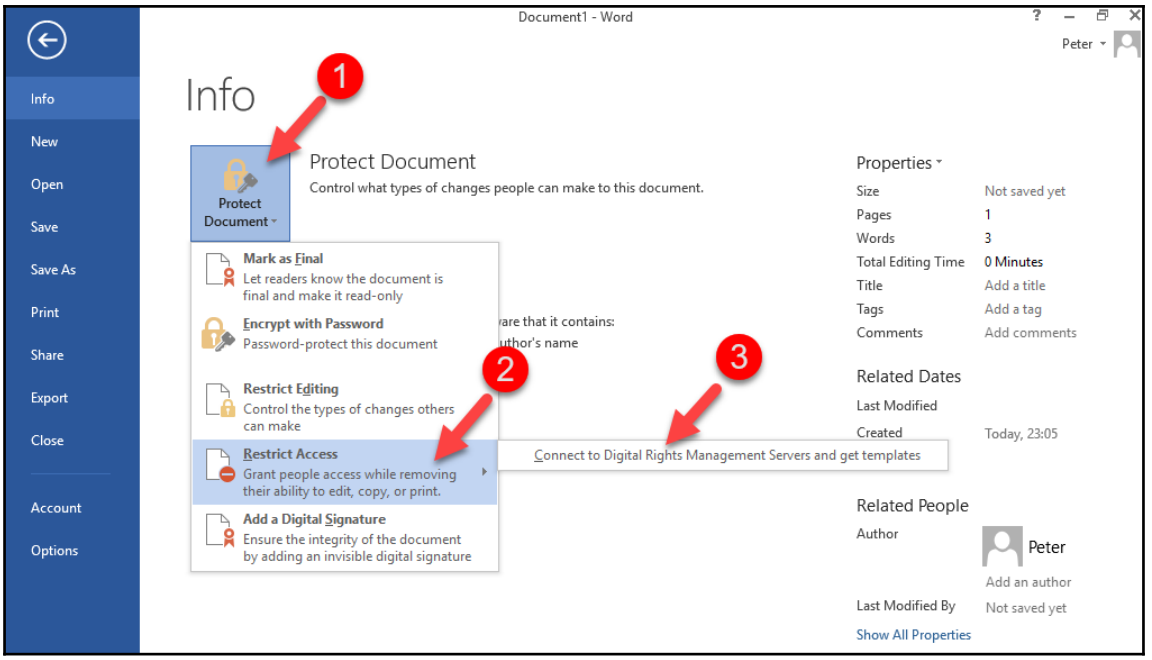

AD RMS Configuration: REBEL-ADFS01.rebeladmin.com
Cluster Address
TARGET SERVER
REBEL-ADFS01.rebeladmin.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify Cluster Address
A cluster address makes it possible for AD RMS clients to communicate with this cluster over the network. We recommend that you configure AD RMS to use the Secure Sockets Layer (SSL) protocol to encrypt network traffic between AD RMS clients and this cluster. You must use an SSL-encrypted connection if you intend to federate this cluster.
Connection Type:
Use an SSL-encrypted connection (https://)
Use an unencrypted connection (http://)
Fully-Qualified Domain Name:
Port:
https://
rms.rebeladmin.com
443
You cannot change this address or port number after AD RMS is installed and configured.
More about the cluster web site
< Previous
Next >
Install
Cancel

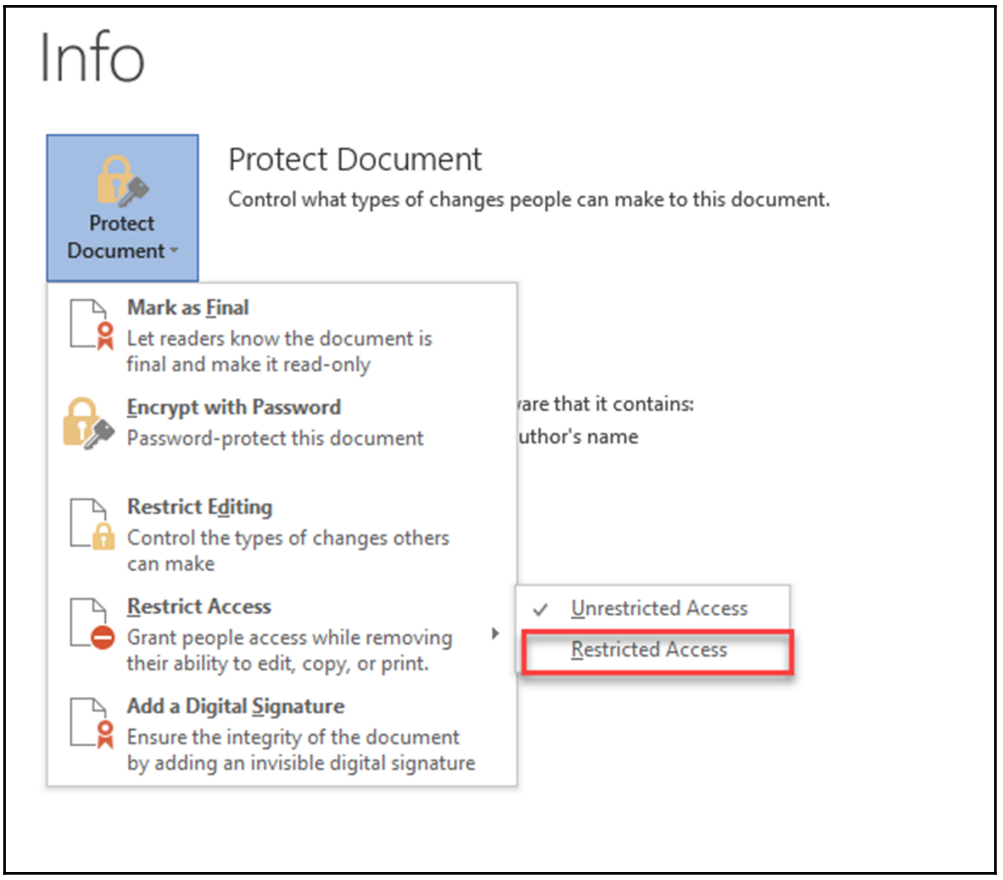

AD RMS Configuration: REBEL-ADFS01.rebeladmin.com
Server Certificate
TARGET SERVER
REBEL-ADFS01.rebeladmin.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Choose a Server Authentication Certificate
When communicating with clients, AD RMS can use Secure Sockets Layer (SSL) to encrypt network traffic. For production deployments, choose an existing SSL certificate whose subject name matches the host name of the cluster. For test deployments, you can create and use a self-signed certificate instead.
Choose an existing certificate for SSL encryption (recommended)
Issued To
Issued By
Expiration Date
adfs.rebeladmin.com
REBELAdmin IssuingCA
29/03/2019
rms.rebeladmin.com
REBELAdmin IssuingCA
06/04/2019
*.rebeladmin.com
REBELAdmin IssuingCA
29/03/2019
Properties
Refresh
Create a self-signed certificate for SSL encryption
Choose a certificate for SSL encryption later
More about the server certificate
< Previous
Next >
Install
Cancel

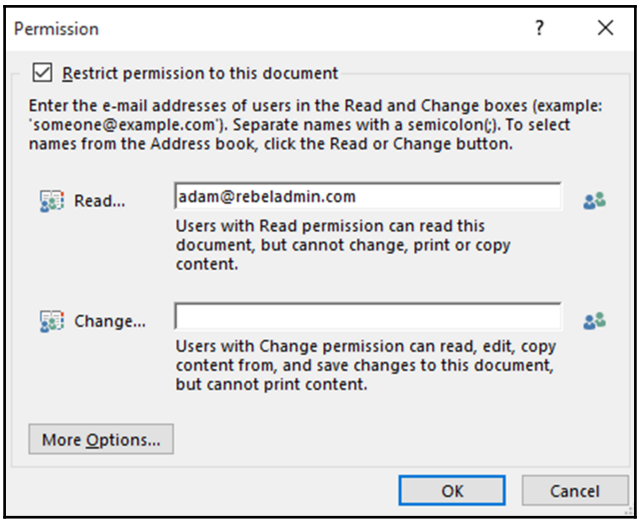

AD RMS Configuration: REBEL-ADFS01.rebeladmin.com
SCP Registration
TARGET SERVER
REBEL-ADFS01.rebeladmin.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Register AD RMS Service Connection Point
The AD RMS service connection point (SCP) can be registered in Active Directory Domain Services (AD DS) when an AD RMS cluster is created. The SCP provides clients with intranet URLs for the AD RMS cluster.
To register the service connection point (SCP) now, you must be a member of the Enterprise Admins group. If you are not a member of the Enterprise Admins group, you must have a member of the Enterprise Admins group register the SCP after you finish installing AD RMS. Clients cannot access this AD RMS cluster until its SCP is registered.
Register the SCP now
Register the SCP later
More about SCP registration
< Previous
Next >
Install
Cancel

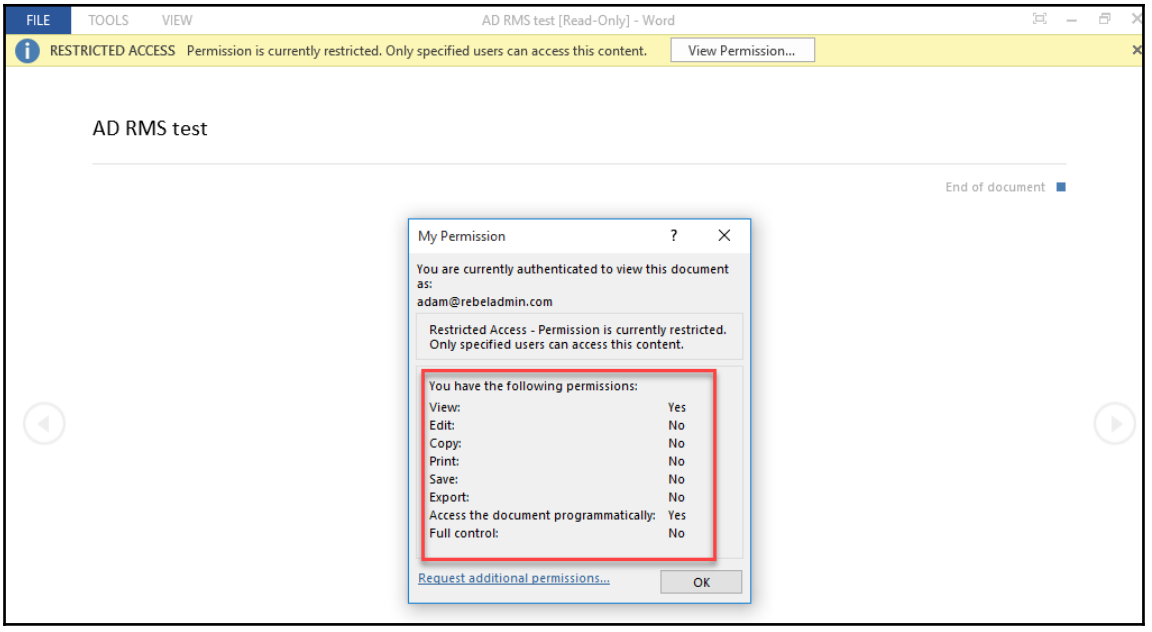

Active Directory Rights Management Services
File Action View Help
Active Directory Rights Management Servi
rebel-adfs01 (Local)
Trust Policies
Trusted User Domains
Trusted Publishing Domains
Rights Policy Templates
Rights Account Certificate Policies
Exclusion Policies
Users
Applications
Lockbox
Security Policies
Super Users
Cluster Key Password
Decommissioning
Reports
Statistics Reports
AD RMS Server Cluster
Configure settings for a cluster. All servers in a cluster share common configuration and logging databases.
Intranet cluster URLs
Licensing: https://rms.rebeladmin.com/_wmcs/licensing
Certification: https://rms.rebeladmin.com/_wmcs/certification/certification.asmx
Extranet cluster URLs
Licensing:
Certification:
Database
Configuration
Server name: REBEL-ADFS01
Database name: DRMS_Config_rms_rebeladmin_com_443
Logging
Server name: REBEL-ADFS01
Database name: DRMS_Logging_rms_rebeladmin_com_443
Tasks
1. Recommended tasks
Establish trust
Set rights account certificate policies
Manage rights policy templates
View reports
Actions
rebel-adfs01 (Local)
Change Service Accou...
View
Delete
Rename
Refresh
Properties
Help

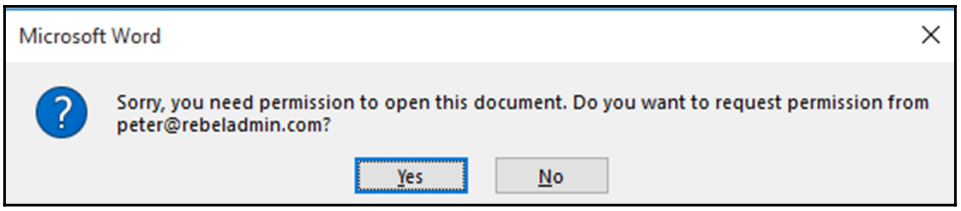

Microsoft Word
Sorry, something went wrong opening Information Rights Management protected content. The operation being requested was not performed because the user has not been authenticated.
OK


Document1 - Word
Peter
Info
New
Open
Save
Save As
Print
Share
Export
Close
Account
Options
Info
1
Protect Document
Protect Document
Control what types of changes people can make to this document.
Mark as Final
Let readers know the document is final and make it read-only
Encrypt with Password
Password-protect this document
Restrict Editing
Control the types of changes others can make
Restrict Access
Grant people access while removing their ability to edit, copy, or print.
Add a Digital Signature
Ensure the integrity of the document by adding an invisible digital signature
2
3
Connect to Digital Rights Management Servers and get templates
Properties
Size Not saved yet
Pages 1
Words 3
Total Editing Time 0 Minutes
Title Add a title
Tags Add a tag
Comments Add comments
Related Dates
Last Modified
Created Today, 23:05
Related People
Author
Peter
Add an author
Last Modified By Not saved yet
Show All Properties

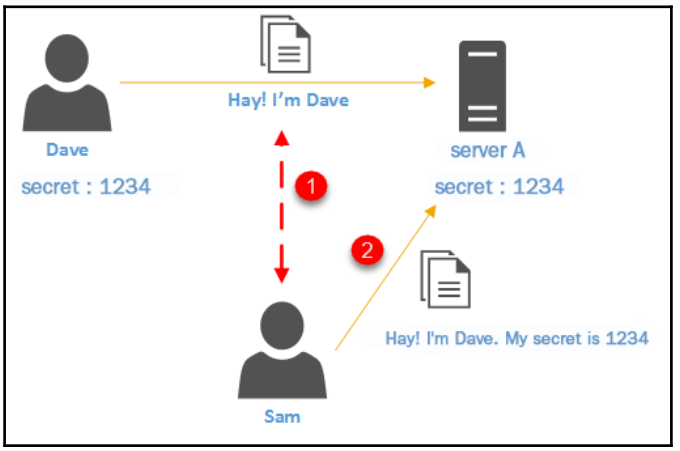

Info
Protect Document
Protect Document
Control what types of changes people can make to this document.
Mark as Final
Let readers know the document is final and make it read-only
Encrypt with Password
Password-protect this document
Restrict Editing
Control the types of changes others can make
Restrict Access
Grant people access while removing their ability to edit, copy, or print.
Add a Digital Signature
Ensure the integrity of the document by adding an invisible digital signature
Unrestricted Access
Restricted Access

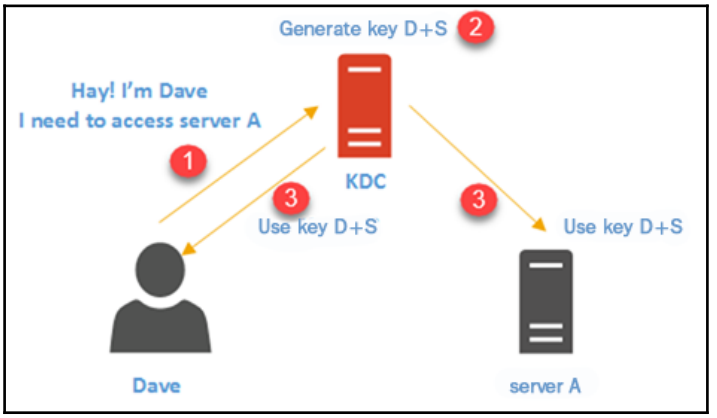

Permission
Restrict permission to this document
Enter the e-mail addresses of users in the Read and Change boxes (example: 'someone@example.com'). Separate names with a semicolon(;). To select names from the Address book, click the Read or Change button.
Read...
adam@rebeladmin.com
Users with Read permission can read this document, but cannot change, print or copy content.
Change...
Users with Change permission can read, edit, copy content from, and save changes to this document, but cannot print content.
More Options...
OK
Cancel

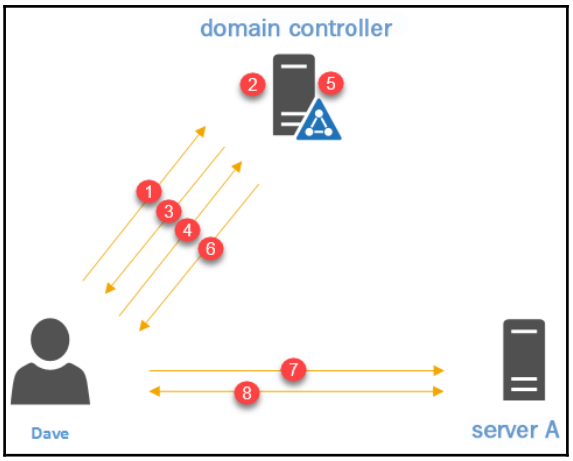

FILE
TOOLS
VIEW
AD RMS test [Read-Only] - Word
RESTRICTED ACCESS
Permission is currently restricted. Only specified users can access this content.
View Permission...
AD RMS test
End of document
My Permission
You are currently authenticated to view this document as:
adam@rebeladmin.com
Restricted Access - Permission is currently restricted. Only specified users can access this content.
You have the following permissions:
View: Yes
Edit: No
Copy: No
Print: No
Save: No
Export: No
Access the document programmatically: Yes
Full control: No
Request additional permissions...
OK


Microsoft Word
Sorry, you need permission to open this document. Do you want to request permission from peter@rebeladmin.com?
Yes
No

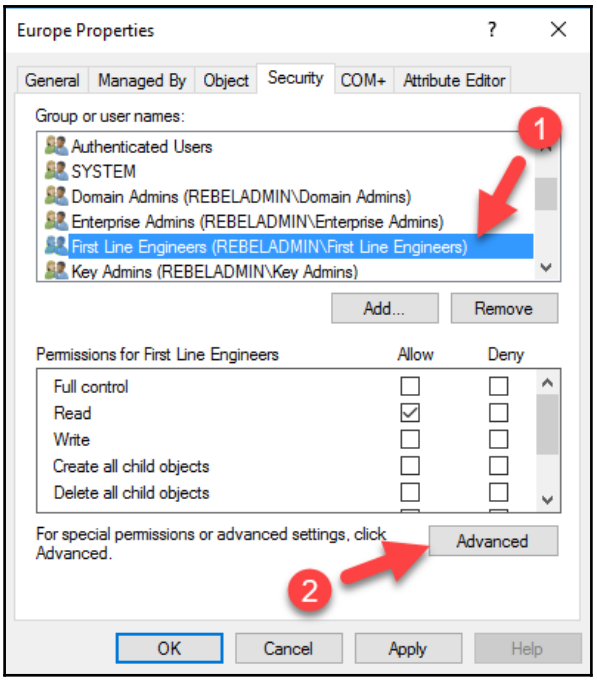
Chapter 15: Active Directory Security Best Practices

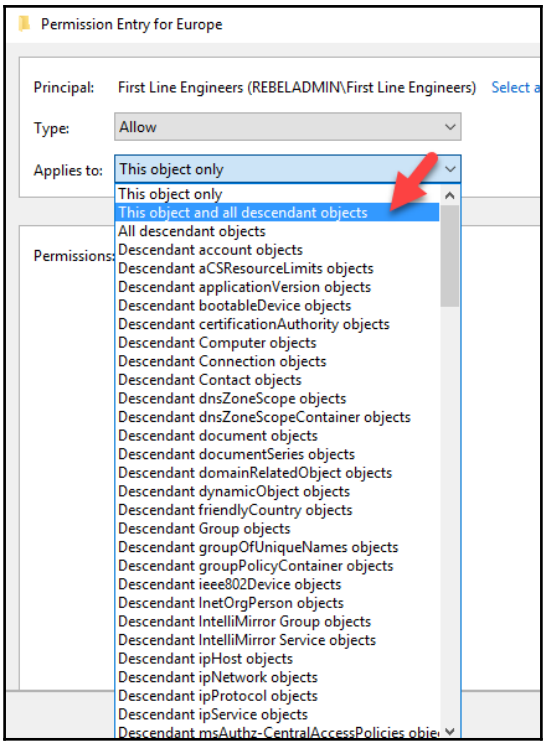







```
PS C:\Users\Administrator> Get-ADGroupMember "First Line Engineers"


distinguishedName : CN=liam,CN=Users,DC=rebeladmin,DC=com
name              : liam
objectClass       : user
objectGUID        : de876f8d-2737-4e3e-901b-a4abc5373677
SamAccountName    : liam
SID               : S-1-5-21-4041220333-1835452706-552999228-1230
```

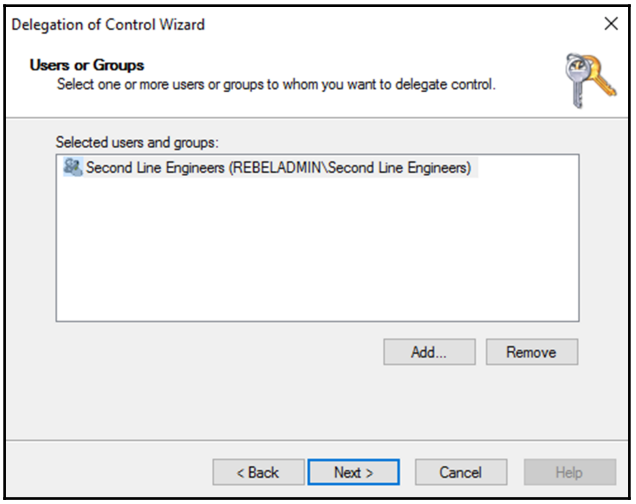

Europe Properties
General
Managed By
Object
Security
COM+
Attribute Editor
Group or user names:
Authenticated Users
SYSTEM
Domain Admins (REBELADMIN\Domain Admins)
Enterprise Admins (REBELADMIN\Enterprise Admins)
First Line Engineers (REBELADMIN\First Line Engineers)
Key Admins (REBELADMIN\Key Admins)
1
Add...
Remove
Permissions for First Line Engineers
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
For special permissions or advanced settings, click Advanced.
Advanced
2
OK
Cancel
Apply
Help

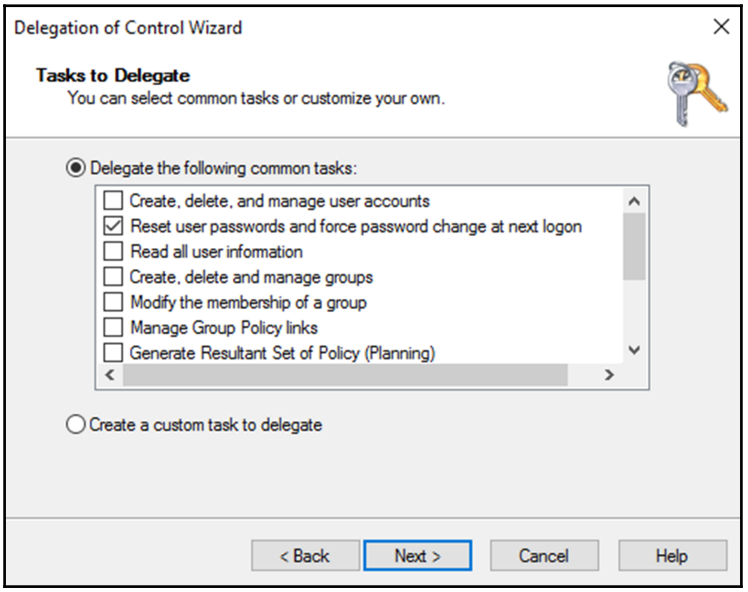



```
PS C:\Users\liam> New-ADUser -Name "Simon" -Path "OU=Users,OU=Asia,DC=rebeladmin,DC=com"
New-ADUser : Access is denied
At line:1 char:1
+ New-ADUser -Name "Simon" -Path "OU=Users,OU=Asia,DC=rebeladmin,DC=com ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (CN=Simon,OU=Use...beladmin,DC=com:String) [New-ADUser], UnauthorizedA
   ccessException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:System.UnauthorizedAccessException,Microsoft.ActiveDirectory.Manag
   ement.Commands.NewADUser

PS C:\Users\liam> _
```

```
PS C:\Users\liam> Remove-ADUser -Identity "CN=Dishan Francis,OU=Users,OU=Europe,DC=rebeladmin,DC=com"

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove" on target "CN=Dishan Francis,OU=Users,OU=Europe,DC=rebeladmin,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
Remove-ADUser : Access is denied
At line:1 char:1
+ Remove-ADUser -Identity "CN=Dishan Francis,OU=Users,OU=Europe,DC=rebe ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (CN=Dishan Franc...beladmin,DC=com:ADUser) [Remove-ADUser], Unauthoriz
   edAccessException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:System.UnauthorizedAccessException,Microsoft.ActiveDirectory.Manag
   ement.Commands.RemoveADUser

PS C:\Users\liam>
```

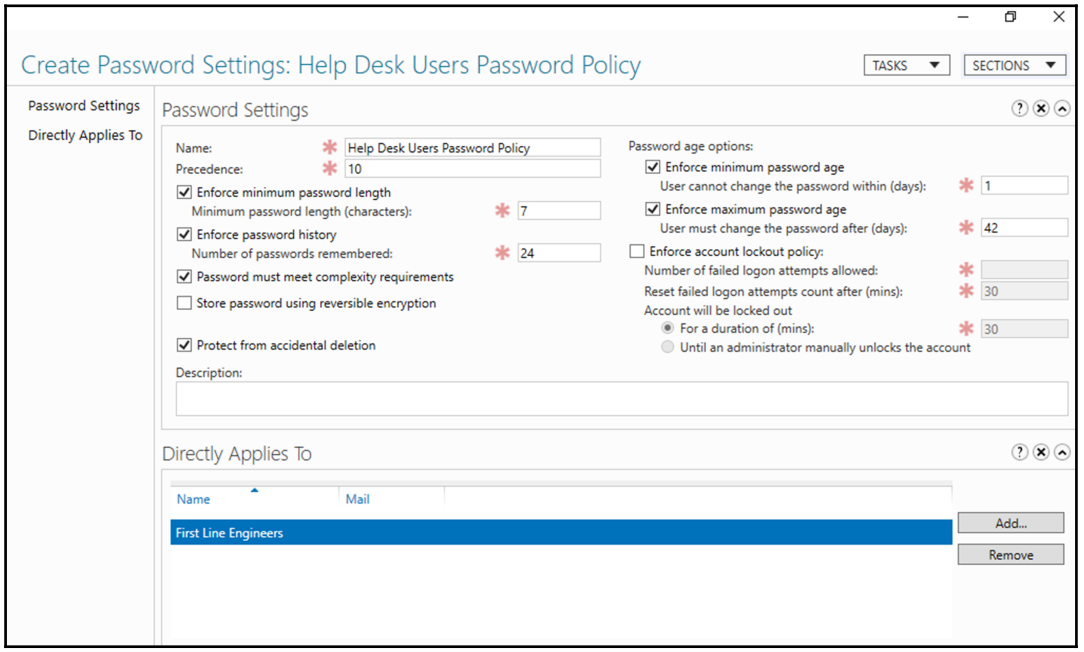
```
PS C:\Users\Administrator> Get-ADGroupMember "Second Line Engineers"

distinguishedName : CN=Scott Brewer,OU=Users,OU=Europe,DC=rebeladmin,DC=com
name              : Scott Brewer
objectClass       : user
objectGUID        : 717e5cb5-724d-4aa7-988a-de34ad7fb1e1
SamAccountName    : sbrewer
SID               : S-1-5-21-4041220333-1835452706-552999228-1200
```





```
PS C:\Users\sbrewer> Set-ADAccountPassword -Identity dfrancis
Please enter the current password for 'CN=Dishan Francis,OU=Users,OU=Europe,DC=rebeladmin,DC=com'
Password: *********
Please enter the desired password for 'CN=Dishan Francis,OU=Users,OU=Europe,DC=rebeladmin,DC=com'
Password: ************
Repeat Password: ************
PS C:\Users\sbrewer>
```

```
PS C:\Users\sbrewer> Remove-ADUser -Identity "CN=Dishan Francis,OU=Users,OU=Europe,DC=rebeladmin,DC=com"

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove" on target "CN=Dishan Francis,OU=Users,OU=Europe,DC=rebeladmin,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
Remove-ADUser : Access is denied
At line:1 char:1
+ Remove-ADUser -Identity "CN=Dishan Francis,OU=Users,OU=Europe,DC=rebe ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (CN=Dishan Franc...beladmin,DC=com:ADUser) [Remove-ADUser], Unauthoriz
   edAccessException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:System.UnauthorizedAccessException,Microsoft.ActiveDirectory.Manag
   ement.Commands.RemoveADUser

PS C:\Users\sbrewer> _
```



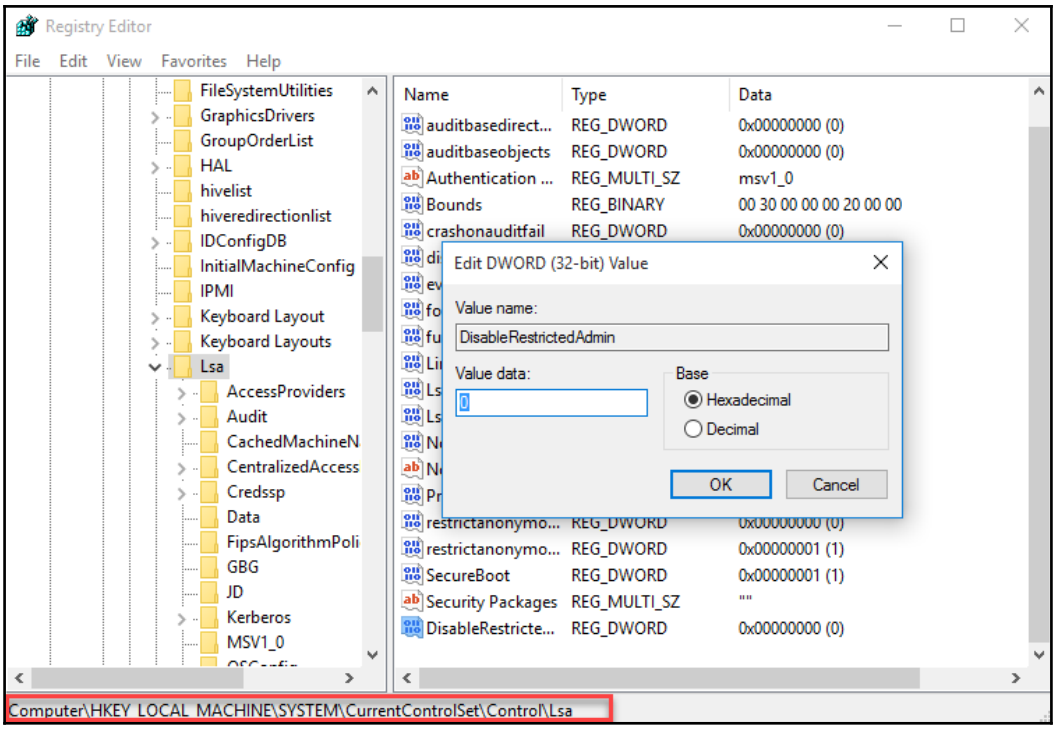
```
PS C:\Users\Administrator> Get-ADFineGrainedPasswordPolicy -Identity "Domain Admin Password Policy"


AppliesTo                   : {}
ComplexityEnabled           : True
DistinguishedName           : CN=Domain Admin Password Policy,CN=Password Settings
                              Container,CN=System,DC=rebeladmin,DC=com
LockoutDuration             : 08:00:00
LockoutObservationWindow    : 08:00:00
LockoutThreshold            : 3
MaxPasswordAge              : 30.00:00:00
MinPasswordAge              : 7.00:00:00
MinPasswordLength           : 12
Name                        : Domain Admin Password Policy
ObjectClass                 : msDS-PasswordSettings
ObjectGUID                  : 81b80dc3-4243-41b2-8e2f-0fb54c24df74
PasswordHistoryCount        : 50
Precedence                  : 1
ReversibleEncryptionEnabled : True
```

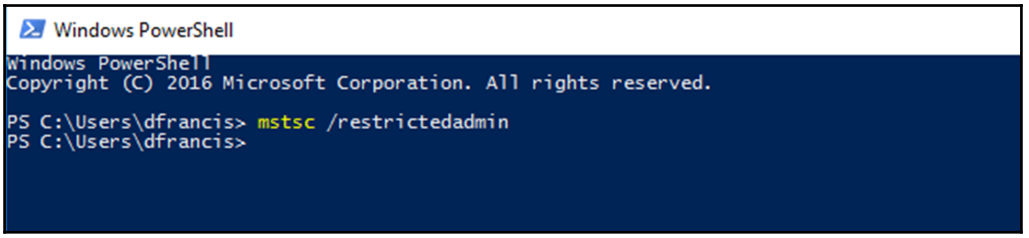
```
PS C:\Users\Administrator> Get-ADGroup -Identity "Protected Users"


DistinguishedName : CN=Protected Users,CN=Users,DC=rebeladmin,DC=com
GroupCategory     : Security
GroupScope        : Global
Name              : Protected Users
ObjectClass       : group
ObjectGUID        : 795da445-8143-41bf-93d5-e6cbc1aff863
SamAccountName    : Protected Users
SID               : S-1-5-21-4041220333-1835452706-552999228-525
```

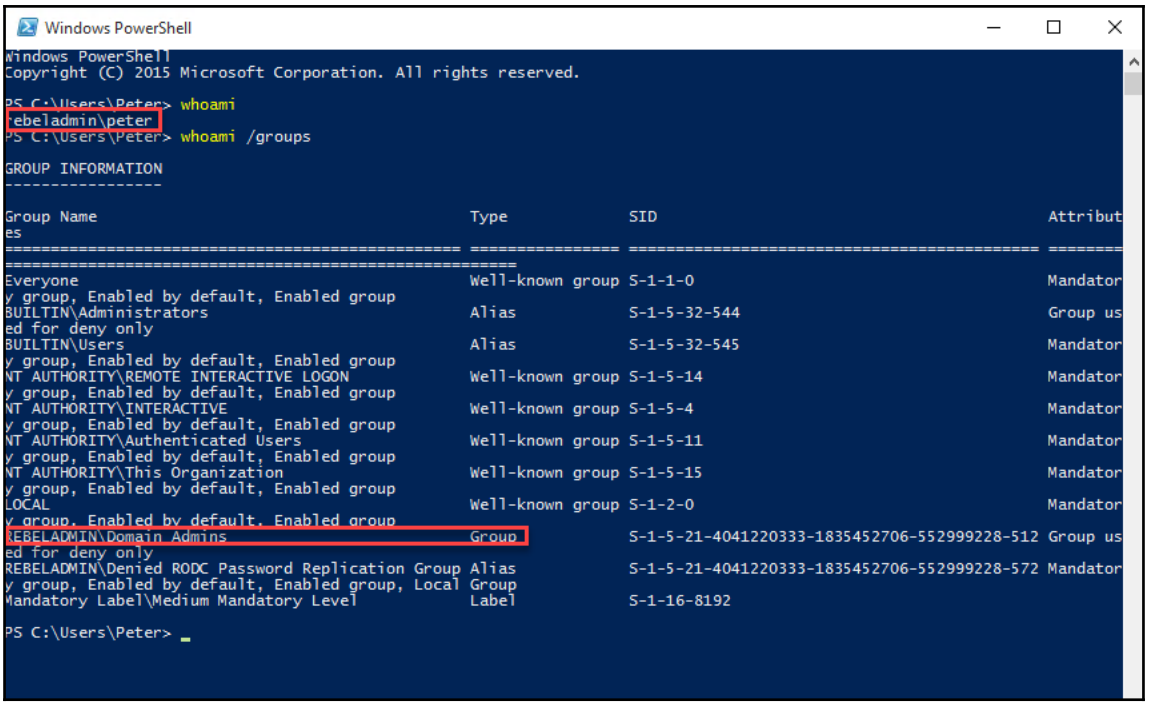
```
PS C:\Users\Administrator> Get-ADGroupMember -Identity "Protected Users"


distinguishedName : CN=Adam,CN=Users,DC=rebeladmin,DC=com
name              : Adam
objectClass       : user
objectGUID        : 7f628987-29b6-42a8-95a6-d90ba92b6128
SamAccountName    : adam
SID               : S-1-5-21-4041220333-1835452706-552999228-1229
```

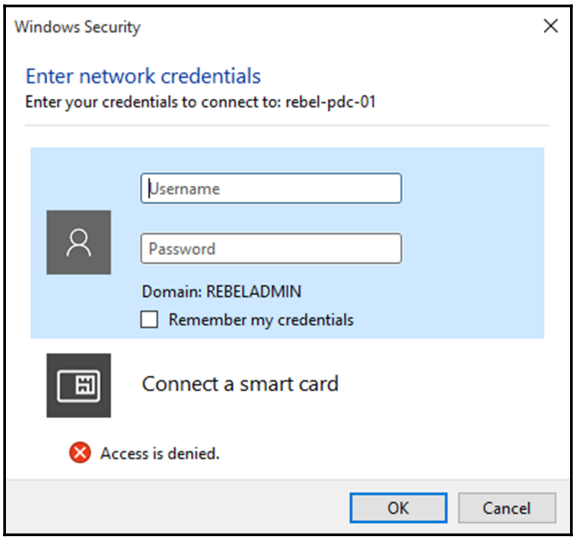
```
Authentication Id : 0 ; 3059384 (00000000:002eaeb8)
Session           : Interactive from 3
User Name         : liam
Domain            : REBELADMIN
Logon Server      : REBEL-PDC-01
Logon Time        : 15/04/2017 08:35:20
SID               : S-1-5-21-4041220333-1835452706-552999228-1230
        msv :
         [00010000] CredentialKeys
         * NTLM     : 947e1646ca81470d18fdb6d976ba8d6a
         * SHA1     : aabc44618a0645c7ddd29ca57f95bacc3f1871b6
         [00000003] Primary
         * Username : liam
         * Domain   : REBELADMIN
         * NTLM     : 947e1646ca81470d18fdb6d976ba8d6a
         * SHA1     : aabc44618a0645c7ddd29ca57f95bacc3f1871b6
        tspkg :
        wdigest :
         * Username : liam
         * Domain   : REBELADMIN
         * Password : (null)
        kerberos :
         * Username : liam
         * Domain   : REBELADMIN.COM
         * Password : (null)
        ssp :
        credman :
```

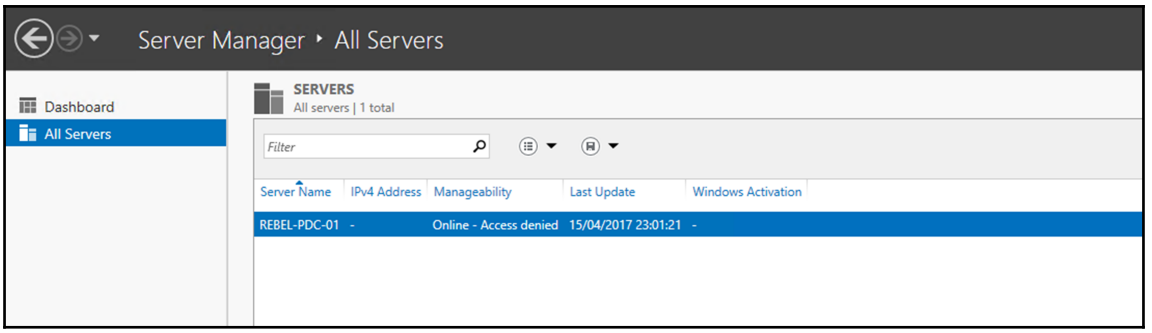
```
Authentication Id : 0 ; 3580277 (00000000:0036a175)
Session           : Interactive from 4
User Name         : adam
Domain            : REBELADMIN
Logon Server      : REBEL-PDC-01
Logon Time        : 15/04/2017 08:52:06
SID               : S-1-5-21-4041220333-1835452706-552999228-1229
        msv :
         [00010000] CredentialKeys
         * RootKey  : fc7b034be210b04c20921a5811dc1165fe4a6dcfddde33b3f939d2b41981b789
         * DPAPI    : c3ebcfb3a1e4b912d6ef928d8bd25c46
        tspkg :
        wdigest :
         * Username : adam
         * Domain   : REBELADMIN
         * Password : (null)
        kerberos :
         * Username : adam
         * Domain   : REBELADMIN.COM
         * Password : (null)
        ssp :
        credman :
```

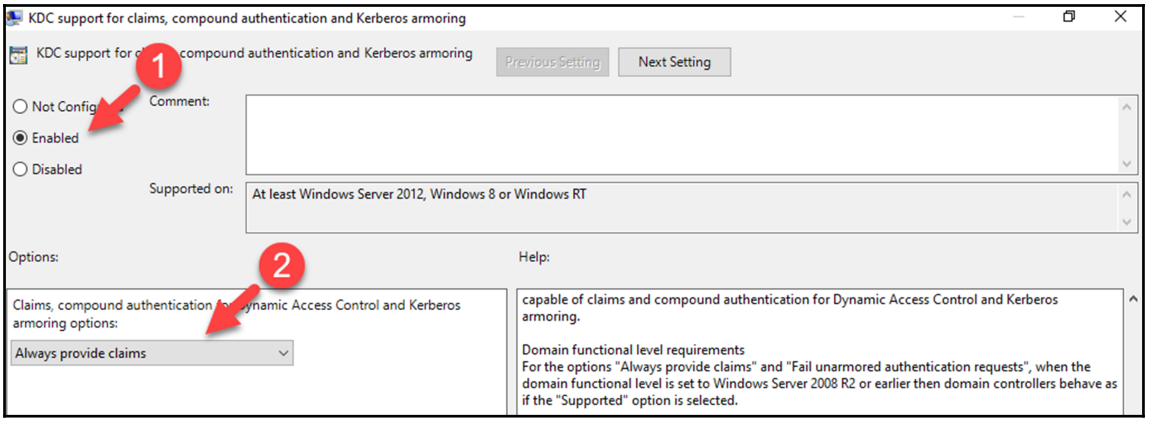

Registry Editor
File Edit View Favorites Help
FileSystemUtilities
GraphicsDrivers
GroupOrderList
HAL
hivelist
hiveredirectionlist
IDConfigDB
InitialMachineConfig
IPMI
Keyboard Layout
Keyboard Layouts
Lsa
AccessProviders
Audit
CachedMachineN
CentralizedAccess
Credssp
Data
FipsAlgorithmPoli
GBG
JD
Kerberos
MSV1_0
Name
Type
Data
auditbasedirect...
REG_DWORD
0x00000000 (0)
auditbaseobjects
REG_DWORD
0x00000000 (0)
Authentication ...
REG_MULTI_SZ
msv1_0
Bounds
REG_BINARY
00 30 00 00 00 20 00 00
crashonauditfail
REG_DWORD
0x00000000 (0)
Edit DWORD (32-bit) Value
Value name:
DisableRestrictedAdmin
Value data:
0
Base
Hexadecimal
Decimal
OK
Cancel
restrictanonymo...
REG_DWORD
0x00000001 (1)
SecureBoot
REG_DWORD
0x00000001 (1)
Security Packages
REG_MULTI_SZ
""
DisableRestricte...
REG_DWORD
0x00000000 (0)
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

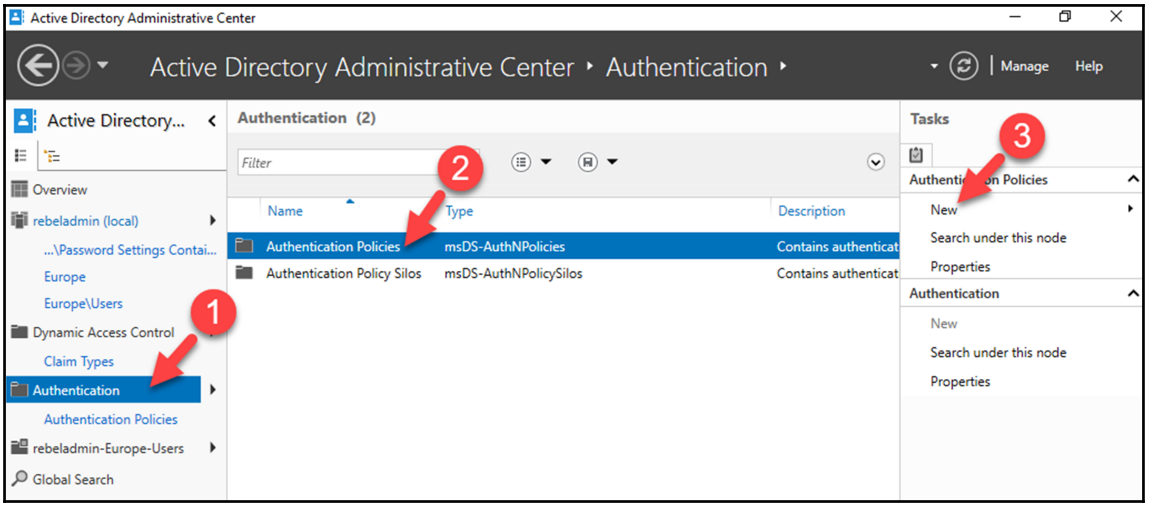

Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\dfrancis> mstsc /restrictedadmin
PS C:\Users\dfrancis>

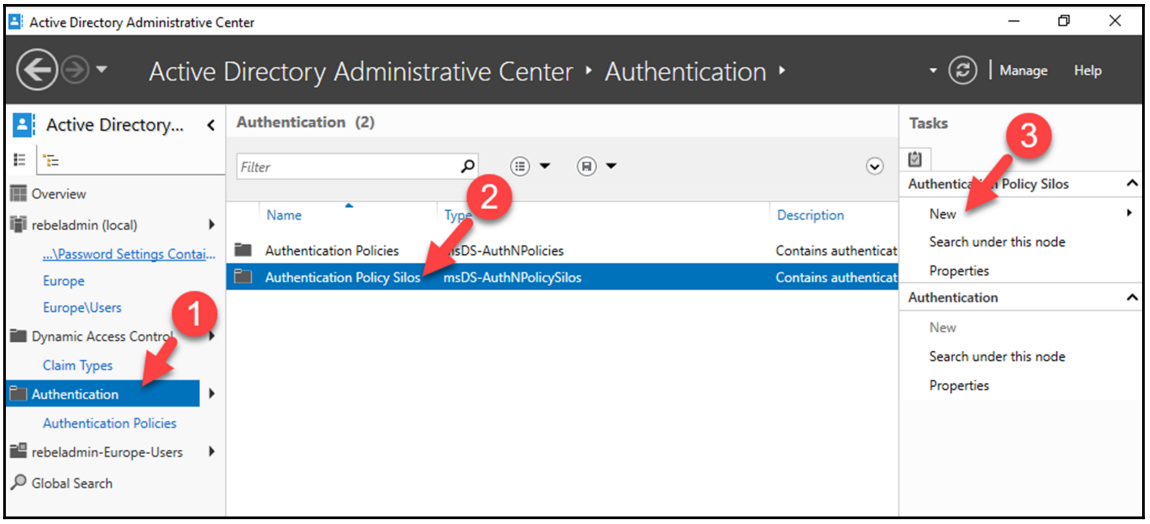

Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
PS C:\Users\Peter> whoami
rebeladmin\peter
PS C:\Users\Peter> whoami /groups
GROUP INFORMATION
Group Name Type SID Attributes
Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators Alias S-1-5-32-544 Group used for deny only
BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\REMOTE INTERACTIVE LOGON Well-known group S-1-5-14 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE Well-known group S-1-5-4 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group
LOCAL Well-known group S-1-2-0 Mandatory group, Enabled by default, Enabled group
REBELADMIN\Domain Admins Group S-1-5-21-4041220333-1835452706-552999228-512 Group used for deny only
REBELADMIN\Denied RODC Password Replication Group Alias S-1-5-21-4041220333-1835452706-552999228-572 Mandatory group, Enabled by default, Enabled group, Local Group
Mandatory Label\Medium Mandatory Level Label S-1-16-8192
PS C:\Users\Peter>

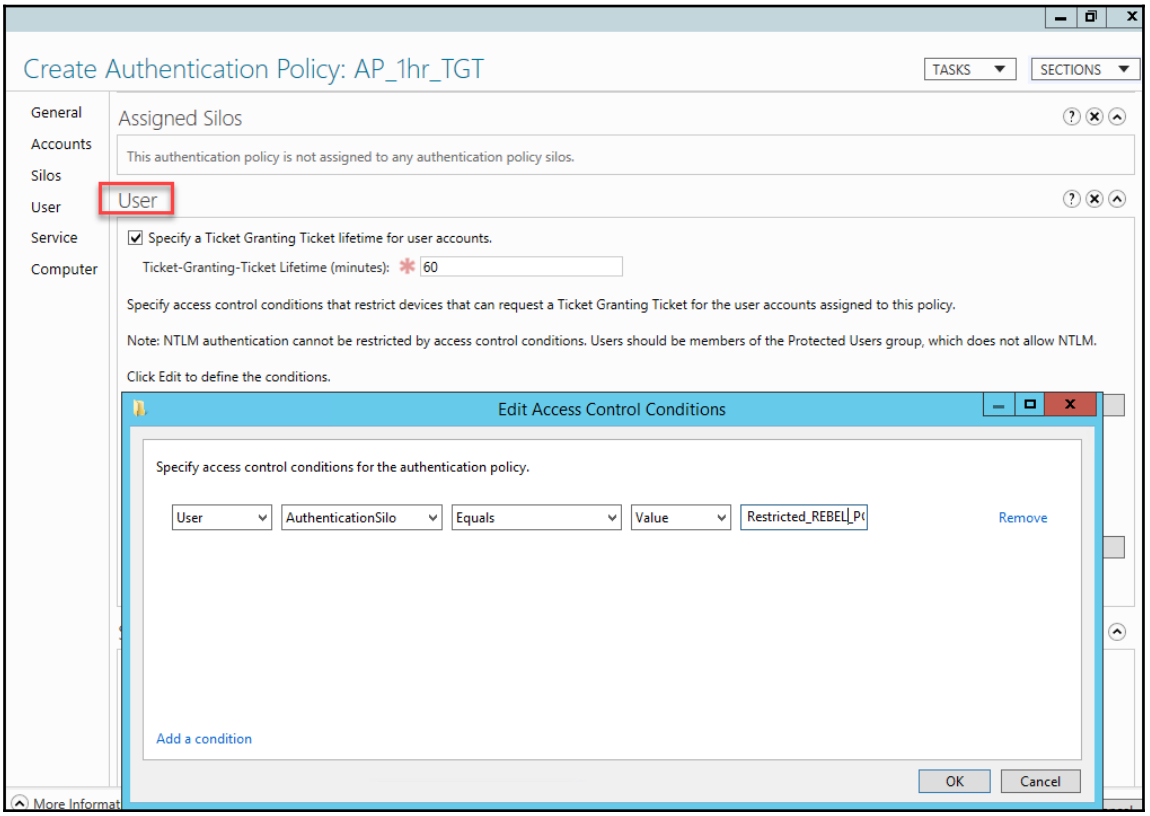

Windows Security
Enter network credentials
Enter your credentials to connect to: rebel-pdc-01
Username
Password
Domain: REBELADMIN
Remember my credentials
Connect a smart card
Access is denied.
OK
Cancel


Server Manager ‣ All Servers
Dashboard
All Servers
SERVERS
All servers | 1 total
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
REBEL-PDC-01 - Online - Access denied 15/04/2017 23:01:21 -

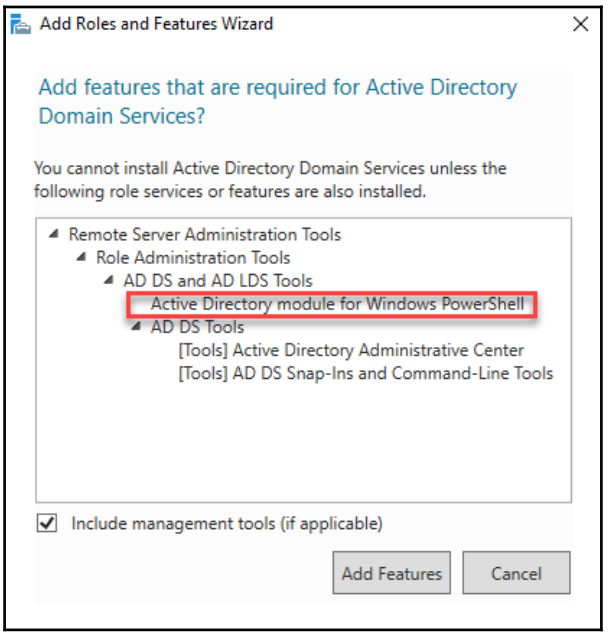

KDC support for claims, compound authentication and Kerberos armoring
Previous Setting
Next Setting
Not Config
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2012, Windows 8 or Windows RT
Options:
Help:
Always provide claims
capable of claims and compound authentication for Dynamic Access Control and Kerberos armoring.
Domain functional level requirements
For the options "Always provide claims" and "Fail unarmored authentication requests", when the domain functional level is set to Windows Server 2008 R2 or earlier then domain controllers behave as if the "Supported" option is selected.
1
2

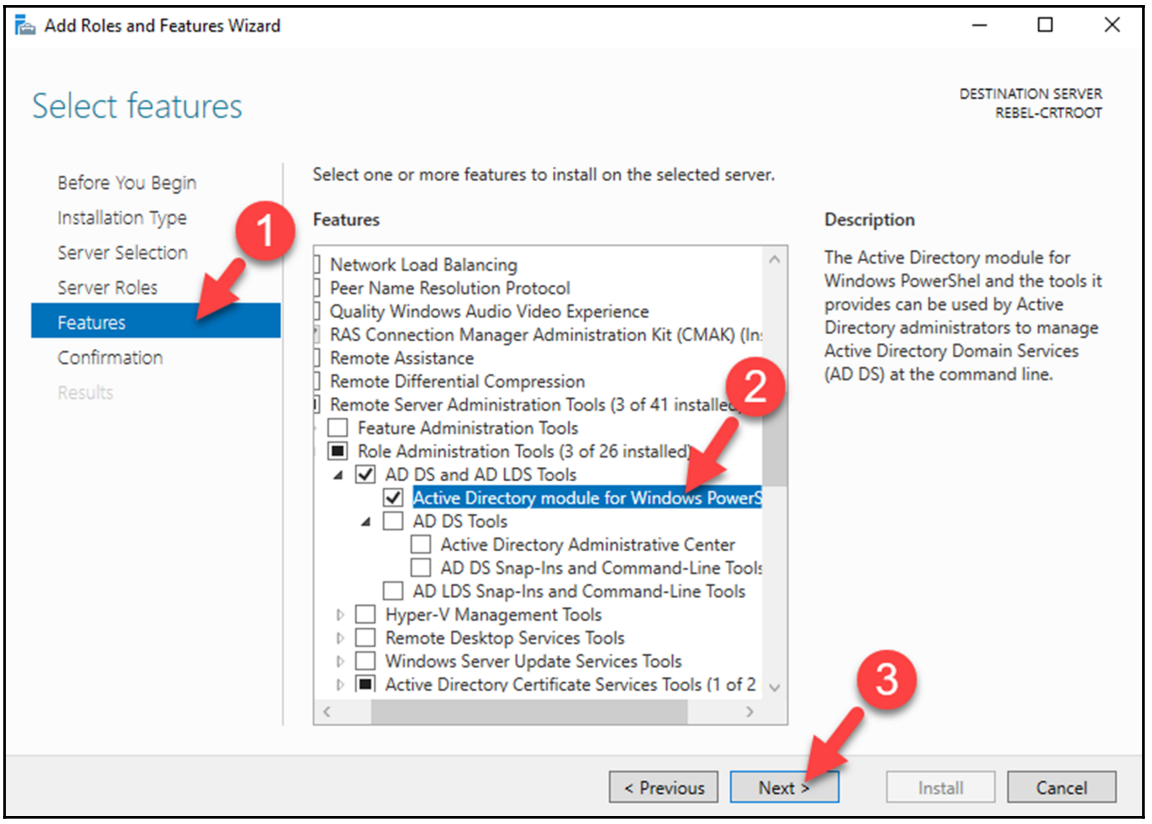

Active Directory Administrative Center
Active Directory Administrative Center ‣ Authentication ‣
Manage
Help
Active Directory...
Overview
rebeladmin (local)
...\Password Settings Contai...
Europe
Europe\Users
Dynamic Access Control
Claim Types
Authentication
Authentication Policies
rebeladmin-Europe-Users
Global Search
Authentication (2)
Filter
Name
Type
Description
Authentication Policies
msDS-AuthNPolicies
Contains authenticat
Authentication Policy Silos
msDS-AuthNPolicySilos
Contains authenticat
Tasks
New
Search under this node
Properties
Authentication
New
Search under this node
Properties
1
2
3


Active Directory Administrative Center
Active Directory Administrative Center ‣ Authentication ‣
Manage
Help
Active Directory...
Overview
rebeladmin (local)
...\Password Settings Contai...
Europe
Europe\Users
Dynamic Access Control
Claim Types
Authentication
Authentication Policies
rebeladmin-Europe-Users
Global Search
Authentication (2)
Filter
Name
Type
Description
Authentication Policies
msDS-AuthNPolicies
Contains authenticat
Authentication Policy Silos
msDS-AuthNPolicySilos
Contains authenticat
Tasks
New
Search under this node
Properties
Authentication
New
Search under this node
Properties
1
2
3


Create Authentication Policy: AP_1hr_TGT
TASKS
SECTIONS
General
Accounts
Silos
User
Service
Computer
Assigned Silos
This authentication policy is not assigned to any authentication policy silos.
User
Specify a Ticket Granting Ticket lifetime for user accounts.
Ticket-Granting-Ticket Lifetime (minutes):
60
Specify access control conditions that restrict devices that can request a Ticket Granting Ticket for the user accounts assigned to this policy.
Note: NTLM authentication cannot be restricted by access control conditions. Users should be members of the Protected Users group, which does not allow NTLM.
Click Edit to define the conditions.
Edit Access Control Conditions
Specify access control conditions for the authentication policy.
User
AuthenticationSilo
Equals
Value
Restricted_REBEL_P
Remove
Add a condition
OK
Cancel

Chapter 16: Advanced AD Management with PowerShell





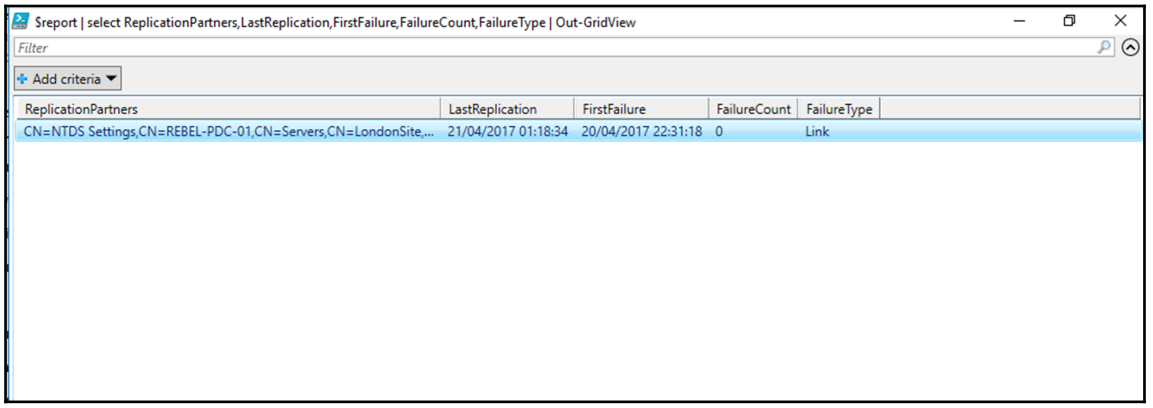

```
PS C:\Users\Administrator> Get-Command New-ADUser -Syntax

New-ADUser [-Name] <string> [-WhatIf] [-Confirm] [-AccountExpirationDate <datetime>] [-AccountNotDelegated <bool>] [-AccountPassword <securestr
ing>] [-AllowReversiblePasswordEncryption <bool>] [-AuthenticationPolicy <ADAuthenticationPolicy>] [-AuthenticationPolicySilo <ADAuthentication
PolicySilo>] [-AuthType <ADAuthType>] [-CannotChangePassword <bool>] [-Certificates <X509Certificate[]>] [-ChangePasswordAtLogon <bool>] [-City
 <string>] [-Company <string>] [-CompoundIdentitySupported <bool>] [-Country <string>] [-Credential <pscredential>] [-Department <string>] [-De
scription <string>] [-DisplayName <string>] [-Division <string>] [-EmailAddress <string>] [-EmployeeID <string>] [-EmployeeNumber <string>] [-E
nabled <bool>] [-Fax <string>] [-GivenName <string>] [-HomeDirectory <string>] [-HomeDrive <string>] [-HomePage <string>] [-HomePhone <string>]
 [-Initials <string>] [-Instance <ADUser>] [-KerberosEncryptionType <ADKerberosEncryptionType>] [-LogonWorkstations <string>] [-Manager <ADUser
>] [-MobilePhone <string>] [-Office <string>] [-OfficePhone <string>] [-Organization <string>] [-OtherAttributes <hashtable>] [-OtherName <stri
ng>] [-PassThru] [-PasswordNeverExpires <bool>] [-PasswordNotRequired <bool>] [-Path <string>] [-POBox <string>] [-PostalCode <string>] [-Princ
ipalsAllowedToDelegateToAccount <ADPrincipal[]>] [-ProfilePath <string>] [-SamAccountName <string>] [-ScriptPath <string>] [-Server <string>] [
-ServicePrincipalNames <string[]>] [-SmartcardLogonRequired <bool>] [-State <string>] [-StreetAddress <string>] [-Surname <string>] [-Title <st
ring>] [-TrustedForDelegation <bool>] [-Type <string>] [-UserPrincipalName <string>] [<CommonParameters>]
```

```
PS C:\Users\Administrator> Get-Help New-ADUser

NAME
    New-ADUser

SYNOPSIS
    Creates a new Active Directory user.


SYNTAX
    New-ADUser [-Name] <String> [-AccountExpirationDate <DateTime>] [-AccountNotDelegated <Boolean>] [-AccountPassword <SecureString>]
    [-AllowReversiblePasswordEncryption <Boolean>] [-AuthenticationPolicy <ADAuthenticationPolicy>] [-AuthenticationPolicySilo
    <ADAuthenticationPolicySilo>] [-AuthType {Negotiate | Basic}] [-CannotChangePassword <Boolean>] [-Certificates <X509Certificate[]>]
    [-ChangePasswordAtLogon <Boolean>] [-City <String>] [-Company <String>] [-CompoundIdentitySupported <Boolean>] [-Country <String>]
    [-Credential <PSCredential>] [-Department <String>] [-Description <String>] [-DisplayName <String>] [-Division <String>] [-EmailAddress
    <String>] [-EmployeeID <String>] [-EmployeeNumber <String>] [-Enabled <Boolean>] [-Fax <String>] [-GivenName <String>] [-HomeDirectory
    <String>] [-HomeDrive <String>] [-HomePage <String>] [-HomePhone <String>] [-Initials <String>] [-Instance <ADUser>]
    [-KerberosEncryptionType {None | DES | RC4 | AES128 | AES256}] [-LogonWorkstations <String>] [-Manager <ADUser>] [-MobilePhone <String>]
    [-Office <String>] [-OfficePhone <String>] [-Organization <String>] [-OtherAttributes <Hashtable>] [-OtherName <String>] [-PassThru]
    [-PasswordNeverExpires <Boolean>] [-PasswordNotRequired <Boolean>] [-Path <String>] [-POBox <String>] [-PostalCode <String>]
    [-PrincipalsAllowedToDelegateToAccount <ADPrincipal[]>] [-ProfilePath <String>] [-SamAccountName <String>] [-ScriptPath <String>]
    [-Server <String>] [-ServicePrincipalNames <String[]>] [-SmartcardLogonRequired <Boolean>] [-State <String>] [-StreetAddress <String>]
    [-Surname <String>] [-Title <String>] [-TrustedForDelegation <Boolean>] [-Type <String>] [-UserPrincipalName <String>] [-Confirm]
    [-WhatIf] [<CommonParameters>]


DESCRIPTION
    The New-ADUser cmdlet creates a new Active Directory user. You can set commonly used user property values by using the cmdlet parameters.

    Property values that are not associated with cmdlet parameters can be set by using the OtherAttributes parameter.  When using this
    parameter be sure to place single quotes around the attribute name as in the following example.

    New-ADUser -SamAccountName "glenjohn"  -GivenName "Glen" -Surname "John" -DisplayName "Glen John" -Path 'CN=Users,DC=fabrikam,DC=local'
    -OtherAttributes @{'msDS-PhoneticDisplayName'="GlenJohn"}

    You must specify the SAMAccountName parameter to create a user.

    You can use the New-ADUser cmdlet to create different types of user accounts such as iNetOrgPerson accounts. To do this in AD DS, set the
    Type parameter to the LDAP display name for the type of account you want to create. This type can be any class in the Active Directory
    schema that is a subclass of user and that has an object category of person.

    The Path parameter specifies the container or organizational unit (OU) for the new user. When you do not specify the Path parameter, the
    cmdlet creates a user object in the default container for user objects in the domain.

    The following methods explain different ways to create an object by using this cmdlet.

    Method 1: Use the New-ADUser cmdlet, specify the required parameters, and set any additional property values by using the cmdlet
    parameters.
```

```
PS C:\Users\Administrator> Get-Help New-ADUser -Example

NAME
    New-ADUser

SYNOPSIS
    Creates a new Active Directory user.


    -------------------------- EXAMPLE 1 --------------------------

    C:\PS>New-ADUser GlenJohn -Certificate (new-object System.Security.Cryptography.X509Certificates.X509Certificate -ArgumentList
    "export.cer")

    Description

    -----------

    Create a new user named 'GlenJohn' with a certicate imported from the file "export.cer".
    -------------------------- EXAMPLE 2 --------------------------

    C:\PS>New-ADUser GlenJohn -OtherAttributes @{title="director";mail="glenjohn@fabrikam.com"}

    Description

    -----------

    Create a new user named 'GlenJohn' and set the title and mail properties on the new object.
    -------------------------- EXAMPLE 3 --------------------------

    C:\PS>New-ADUser GlenJohn -Type iNetOrgPerson -Path "DC=AppNC" -server lds.Fabrikam.com:50000

    Description

    -----------

    Create a new inetOrgPerson named 'GlenJohn' on an AD LDS instance.
```

```
PS C:\Users\administrator.REBELADMIN> Get-ADrootDSE


configurationNamingContext    : CN=Configuration,DC=rebeladmin,DC=com
currentTime                   : 19/04/2017 21:28:57
defaultNamingContext          : DC=rebeladmin,DC=com
dnsHostName                   : REBEL-SDC01.rebeladmin.com
domainControllerFunctionality : Windows2016
domainFunctionality           : Windows2016Domain
dsServiceName                 : CN=NTDS Settings,CN=REBEL-SDC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Confi
                                guration,DC=rebeladmin,DC=com
forestFunctionality           : Windows2016Forest
highestCommittedUSN           : 41039
isGlobalCatalogReady          : {TRUE}
isSynchronized                : {TRUE}
ldapServiceName               : rebeladmin.com:rebel-sdc01$@REBELADMIN.COM
namingContexts                : {DC=rebeladmin,DC=com, CN=Configuration,DC=rebeladmin,DC=com,
                                CN=Schema,CN=Configuration,DC=rebeladmin,DC=com,
                                DC=DomainDnsZones,DC=rebeladmin,DC=com...}
rootDomainNamingContext       : DC=rebeladmin,DC=com
schemaNamingContext           : CN=Schema,CN=Configuration,DC=rebeladmin,DC=com
serverName                    : CN=REBEL-SDC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=rebel
                                admin,DC=com
subschemaSubentry             : CN=Aggregate,CN=Schema,CN=Configuration,DC=rebeladmin,DC=com
supportedCapabilities         : {1.2.840.113556.1.4.800 (LDAP_CAP_ACTIVE_DIRECTORY_OID), 1.2.840.113556.1.4.1670
                                (LDAP_CAP_ACTIVE_DIRECTORY_V51_OID), 1.2.840.113556.1.4.1791
                                (LDAP_CAP_ACTIVE_DIRECTORY_LDAP_INTEG_OID), 1.2.840.113556.1.4.1935
                                (LDAP_CAP_ACTIVE_DIRECTORY_V61_OID)...}
supportedControl              : {1.2.840.113556.1.4.319 (LDAP_PAGED_RESULT_OID_STRING), 1.2.840.113556.1.4.801
                                (LDAP_SERVER_SD_FLAGS_OID), 1.2.840.113556.1.4.473 (LDAP_SERVER_SORT_OID),
                                1.2.840.113556.1.4.528 (LDAP_SERVER_NOTIFICATION_OID)...}
supportedLDAPPolicies         : {MaxPoolThreads, MaxPercentDirSyncRequests, MaxDatagramRecv, MaxReceiveBuffer...}
supportedLDAPVersion          : {3, 2}
supportedSASLMechanisms       : {GSSAPI, GSS-SPNEGO, EXTERNAL, DIGEST-MD5}
```

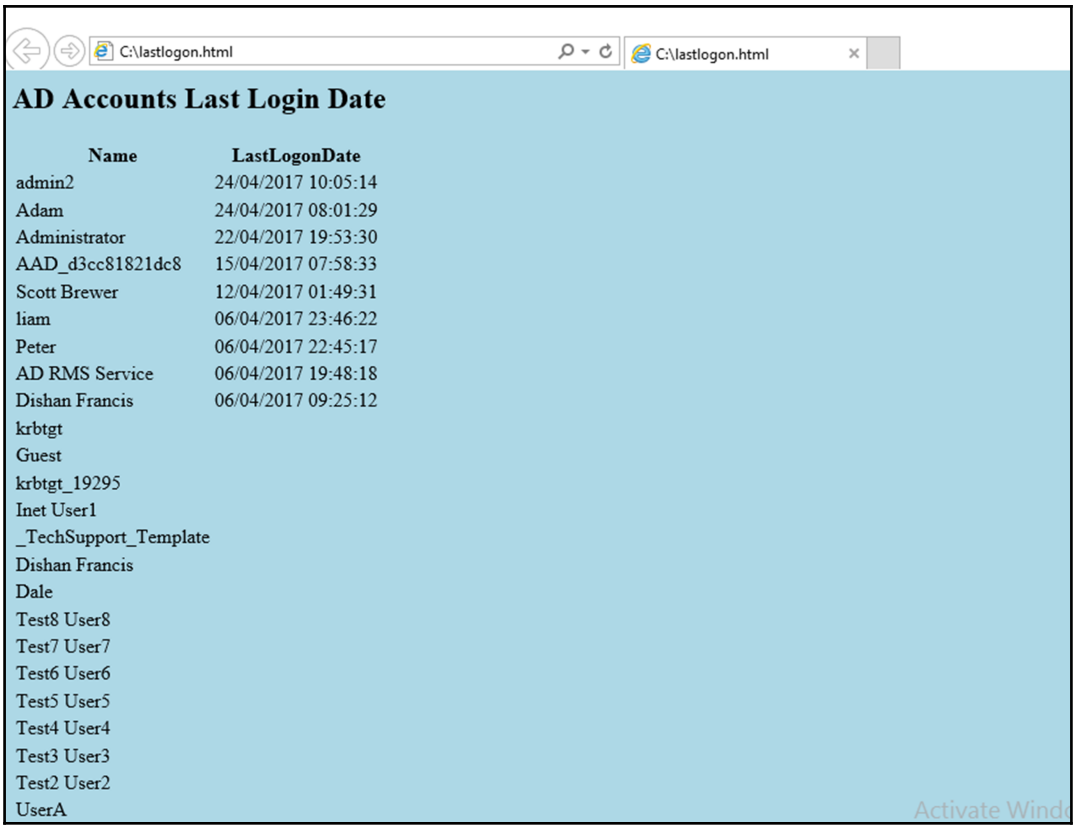
```
PS C:\Windows\system32> $Domain = Read-Host 'What is your Domain Name ?'
Get-ADDomain -Identity $Domain | select ReplicaDirectoryServers,ReadOnlyReplicaDirectoryServers

What is your Domain Name ?: rebeladmin.com

ReplicaDirectoryServers       ReadOnlyReplicaDirectoryServers
-----------------------       -------------------------------
{REBEL-PDC-01.rebeladmin.com} {REBEL-RODC-01.rebeladmin.com}
```

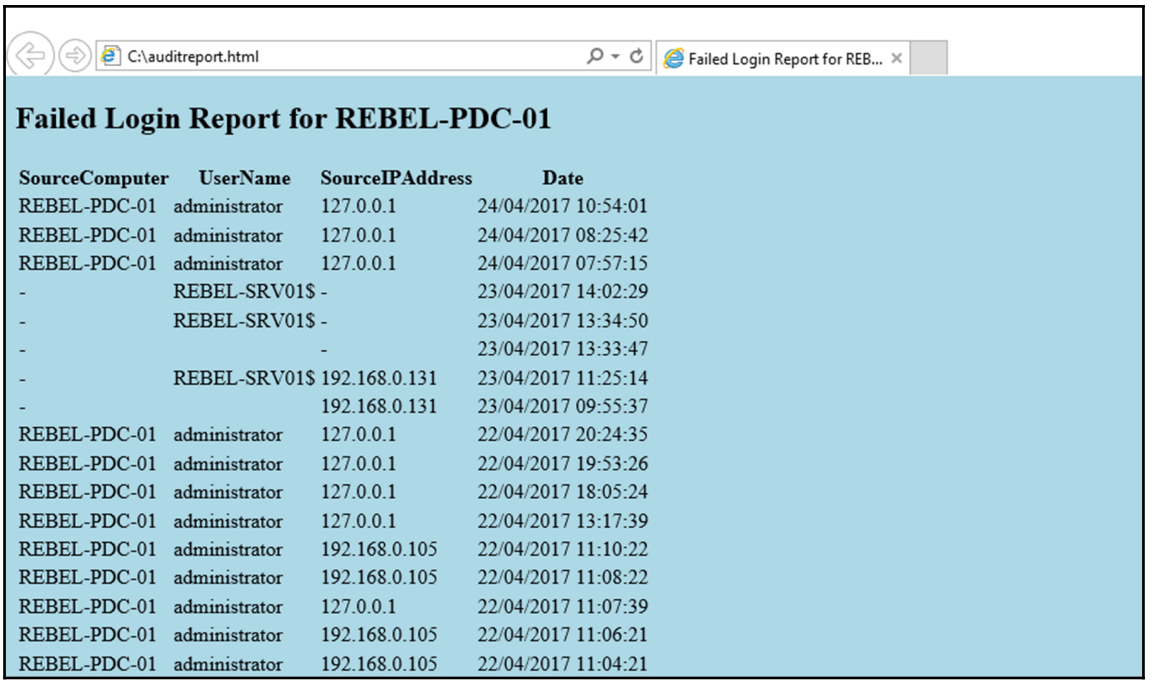


```
PS C:\Users\Administrator> Get-ADReplicationSite -Filter *


Description                     : UK AD Site
DistinguishedName               : CN=LondonSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
InterSiteTopologyGenerator      : CN=NTDS Settings,CN=REBEL-PDC-01,CN=Servers,CN=LondonSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
ManagedBy                       :
Name                            : LondonSite
ObjectClass                     : site
ObjectGUID                      : fbef3a2c-2de8-44d2-bde9-c37403c9f3a9
ReplicationSchedule             : System.DirectoryServices.ActiveDirectory.ActiveDirectorySchedule
UniversalGroupCachingRefreshSite :

Description                     : Canada AD Site
DistinguishedName               : CN=CanadaSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
InterSiteTopologyGenerator      : CN=NTDS Settings\0ADEL:816b7b06-7427-4ccb-8303-ab229caa9931,CN=REBEL-SDC-02\0ADEL:1ed99178-bfb2-4717-80b2-c
                                  48d3c5f80ad,CN=Servers,CN=LondonSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
ManagedBy                       :
Name                            : CanadaSite
ObjectClass                     : site
ObjectGUID                      : 1bc04b4a-0f69-4ef5-8083-98d9bb0e88ca
ReplicationSchedule             :
UniversalGroupCachingRefreshSite :
```

```
PS C:\Users\Administrator> Get-ADReplicationSubnet -Filter * | Format-Table Name,Site -A

Name           Site
----           ----
192.168.0.0/24 CN=LondonSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
10.11.0.0/24   CN=CanadaSite,CN=Sites,CN=Configuration,DC=rebeladmin,DC=com
```

```
PS C:\Windows\system32> ## Replicate Objects to Domain Controllers ##
$myobject = Read-Host 'What is your AD Object Includes ?'
$sourcedc = Read-Host 'What is the Source DC ?'
$destinationdc = Read-Host 'What is the Destination DC ?'
$passobject = (Get-ADObject -Filter {Name -Like $myobject})
Sync-ADObject -object $passobject -source $sourcedc -destination $destinationdc
Write-Host "Given Object Replicated to" $destinationdc
What is your AD Object Includes ?: Adam
What is the Source DC ?: REBEL-PDC-01
What is the Destination DC ?: REBEL-SRV01
Given Object Replicated to REBEL-SRV01

PS C:\Windows\system32>
```

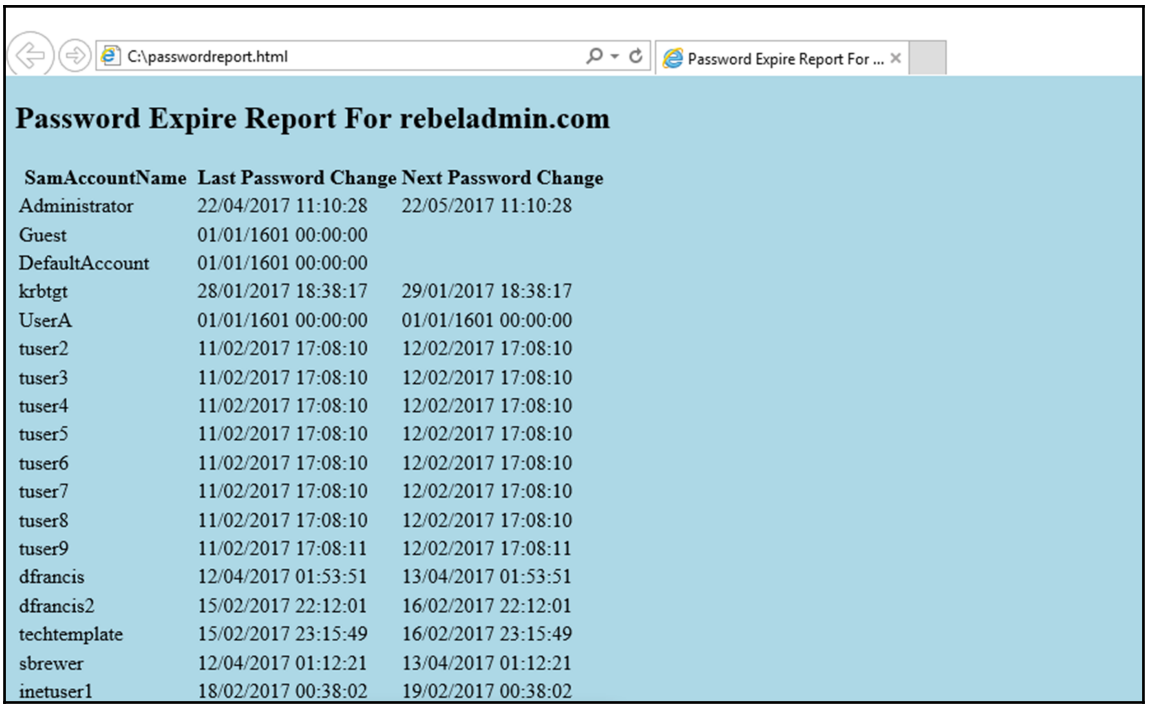

C:\lastlogon.html
C:\lastlogon.html
AD Accounts Last Login Date
Name LastLogonDate
admin2 24/04/2017 10:05:14
Adam 24/04/2017 08:01:29
Administrator 22/04/2017 19:53:30
AAD_d3cc81821dc8 15/04/2017 07:58:33
Scott Brewer 12/04/2017 01:49:31
liam 06/04/2017 23:46:22
Peter 06/04/2017 22:45:17
AD RMS Service 06/04/2017 19:48:18
Dishan Francis 06/04/2017 09:25:12
krbtgt
Guest
krbtgt_19295
Inet User1
_TechSupport_Template
Dishan Francis
Dale
Test8 User8
Test7 User7
Test6 User6
Test5 User5
Test4 User4
Test3 User3
Test2 User2
UserA



Failed Login Report for REBEL-PDC-01

SourceComputer	UserName	SourceIPAddress	Date
REBEL-PDC-01	administrator	127.0.0.1	24/04/2017 10:54:01
REBEL-PDC-01	administrator	127.0.0.1	24/04/2017 08:25:42
REBEL-PDC-01	administrator	127.0.0.1	24/04/2017 07:57:15
-	REBEL-SRV01$	-	23/04/2017 14:02:29
-	REBEL-SRV01$	-	23/04/2017 13:34:50
-		-	23/04/2017 13:33:47
-	REBEL-SRV01$	192.168.0.131	23/04/2017 11:25:14
-		192.168.0.131	23/04/2017 09:55:37
REBEL-PDC-01	administrator	127.0.0.1	22/04/2017 20:24:35
REBEL-PDC-01	administrator	127.0.0.1	22/04/2017 19:53:26
REBEL-PDC-01	administrator	127.0.0.1	22/04/2017 18:05:24
REBEL-PDC-01	administrator	127.0.0.1	22/04/2017 13:17:39
REBEL-PDC-01	administrator	192.168.0.105	22/04/2017 11:10:22
REBEL-PDC-01	administrator	192.168.0.105	22/04/2017 11:08:22
REBEL-PDC-01	administrator	127.0.0.1	22/04/2017 11:07:39
REBEL-PDC-01	administrator	192.168.0.105	22/04/2017 11:06:21
REBEL-PDC-01	administrator	192.168.0.105	22/04/2017 11:04:21

```
PS C:\Users\Administrator> Search-ADAccount -LockedOut | select Name,samAccountName,LockedOut

Name        samAccountName LockedOut
----        -------------- ---------
Test4 User4 tuser4             True
Test7 User7 tuser7             True
```



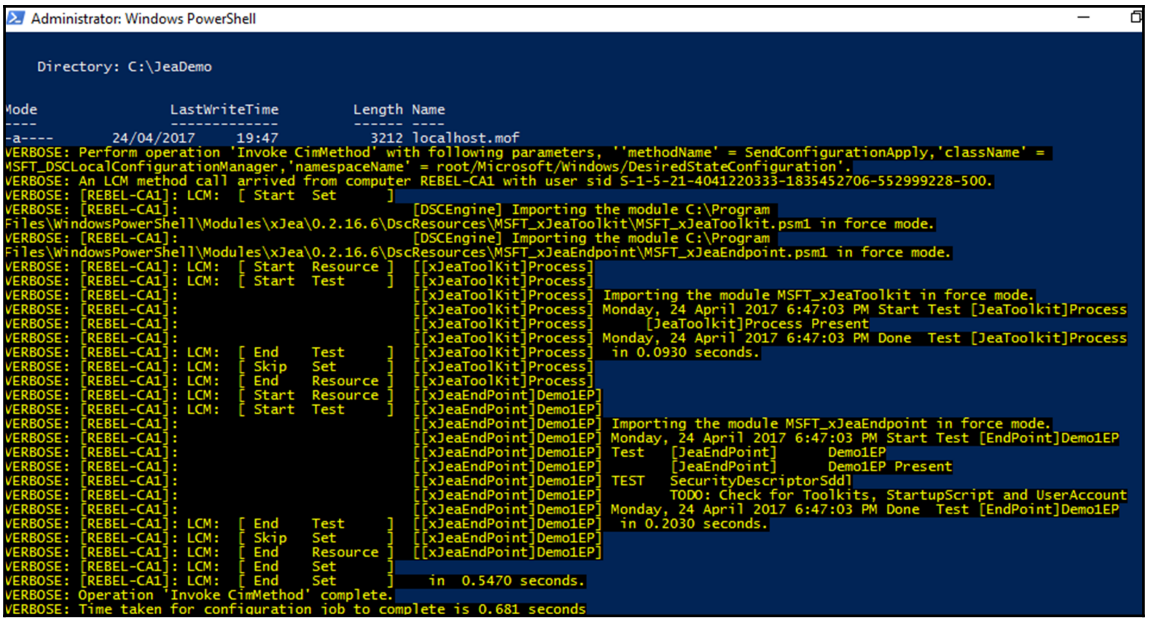
Password Expire Report For rebeladmin.com

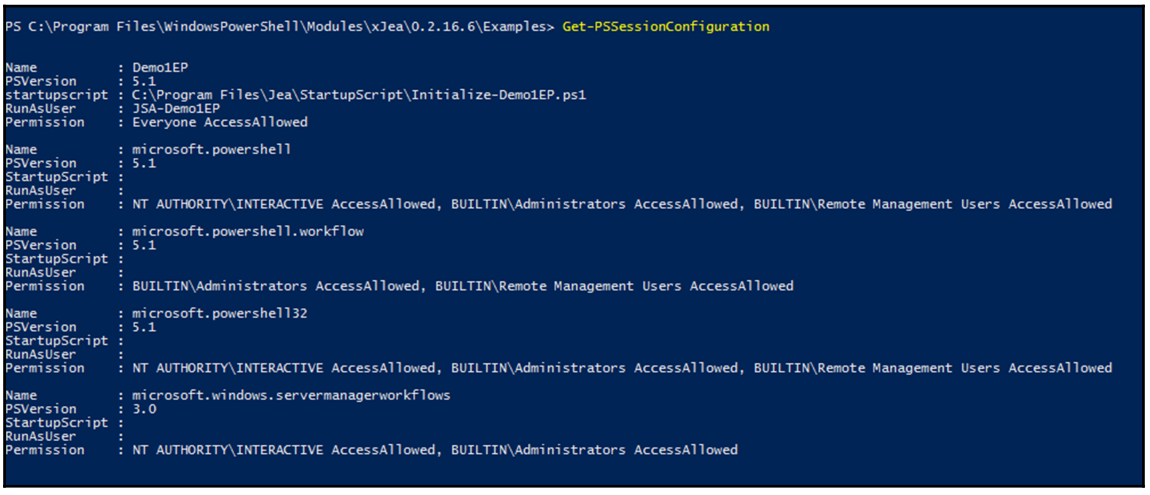
SamAccountName	Last Password Change	Next Password Change
Administrator	22/04/2017 11:10:28	22/05/2017 11:10:28
Guest	01/01/1601 00:00:00	
DefaultAccount	01/01/1601 00:00:00	
krbtgt	28/01/2017 18:38:17	29/01/2017 18:38:17
UserA	01/01/1601 00:00:00	01/01/1601 00:00:00
tuser2	11/02/2017 17:08:10	12/02/2017 17:08:10
tuser3	11/02/2017 17:08:10	12/02/2017 17:08:10
tuser4	11/02/2017 17:08:10	12/02/2017 17:08:10
tuser5	11/02/2017 17:08:10	12/02/2017 17:08:10
tuser6	11/02/2017 17:08:10	12/02/2017 17:08:10
tuser7	11/02/2017 17:08:10	12/02/2017 17:08:10
tuser8	11/02/2017 17:08:10	12/02/2017 17:08:10
tuser9	11/02/2017 17:08:11	12/02/2017 17:08:11
dfrancis	12/04/2017 01:53:51	13/04/2017 01:53:51
dfrancis2	15/02/2017 22:12:01	16/02/2017 22:12:01
techtemplate	15/02/2017 23:15:49	16/02/2017 23:15:49
sbrewer	12/04/2017 01:12:21	13/04/2017 01:12:21
inetuser1	18/02/2017 00:38:02	19/02/2017 00:38:02

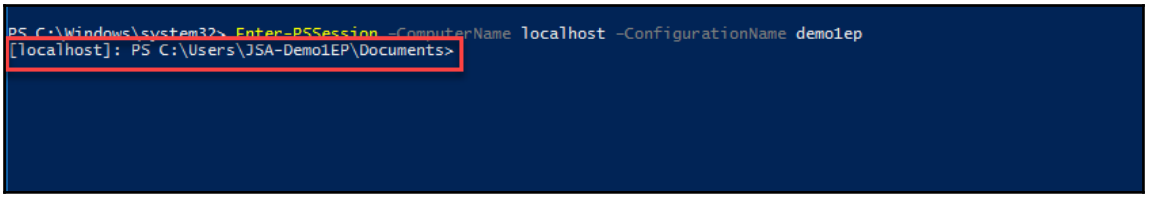
```
PS C:\Windows\system32> Install-Module xJEA

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
 provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\admin2\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): A
PS C:\Windows\system32>
```

```
PS C:\Windows\system32> Find-Module -Name xJEA | fl


Name                           : xJea
Version                        : 0.2.16.6
Type                           : Module
Description                    : Module with DSC Resources for Just Enough Admin (JEA).  Jea makes it simple to create
                                 custom RBAC solutions using PowerShell.
Author                         : Microsoft Corporation
CompanyName                    : {PowerShellTeam, jsnover}
Copyright                      : (c) 2014 Microsoft Corporation. All rights reserved.
PublishedDate                  : 14/05/2015 19:51:23
InstalledDate                  :
UpdatedDate                    :
LicenseUri                     :
ProjectUri                     :
IconUri                        :
Tags                           : {PSModule}
Includes                       : {Function, RoleCapability, Command, DscResource...}
PowerShellGetFormatVersion     :
ReleaseNotes                   :
Dependencies                   : {}
RepositorySourceLocation       : https://www.powershellgallery.com/api/v2/
Repository                     : PSGallery
PackageManagementProvider      : NuGet
AdditionalMetadata             : {versionDownloadCount, ItemType, copyright, description...}
```

```
PS C:\Program Files\WindowsPowerShell\Modules\xJea\0.2.16.6\Examples> .\SetupJEA.ps1


    Directory: C:\JeaDemo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        24/04/2017     19:07           1984 localhost.mof
-a----        24/04/2017     19:07           1188 localhost.meta.mof
VERBOSE: Performing the operation "Start-DscConfiguration: SendMetaConfigurationApply" on target
"MSFT_DSCLocalConfigurationManager".
VERBOSE: Perform operation 'Invoke CimMethod' with following parameters, ''methodName' =
SendMetaConfigurationApply,'className' = MSFT_DSCLocalConfigurationManager,'namespaceName' =
root/Microsoft/Windows/DesiredStateConfiguration'.
VERBOSE: An LCM method call arrived from computer REBEL-CA1 with user sid S-1-5-21-4041220333-1835452706-552999228-500.
VERBOSE: [REBEL-CA1]: LCM:  [ Start  Set      ]
VERBOSE: [REBEL-CA1]: LCM:  [ Start  Resource ]  [MSFT_DSCMetaConfiguration]
VERBOSE: [REBEL-CA1]: LCM:  [ Start  Set      ]  [MSFT_DSCMetaConfiguration]
VERBOSE: [REBEL-CA1]: LCM:  [ End    Set      ]  [MSFT_DSCMetaConfiguration]  in 0.1250 seconds.
VERBOSE: [REBEL-CA1]: LCM:  [ End    Resource ]  [MSFT_DSCMetaConfiguration]
VERBOSE: [REBEL-CA1]: LCM:  [ End    Set      ]
VERBOSE: [REBEL-CA1]: LCM:  [ End    Set      ]  in  0.3910 seconds.
VERBOSE: Operation 'Invoke CimMethod' complete.
VERBOSE: Set-DscLocalConfigurationManager finished in 1.095 seconds.
VERBOSE: Perform operation 'Invoke CimMethod' with following parameters, ''methodName' =
SendConfigurationApply,'className' = MSFT_DSCLocalConfigurationManager,'namespaceName' =
root/Microsoft/Windows/DesiredStateConfiguration'.
VERBOSE: An LCM method call arrived from computer REBEL-CA1 with user sid S-1-5-21-4041220333-1835452706-552999228-500.
VERBOSE: [REBEL-CA1]: LCM:  [ Start  Set      ]
VERBOSE: [REBEL-CA1]:                            [DSCEngine] Importing the module C:\Program
Files\WindowsPowerShell\Modules\xJea\0.2.16.6\DscResources\MSFT_xJeaEndpoint\MSFT_xJeaEndpoint.psm1 in force mode.
VERBOSE: [REBEL-CA1]: LCM:  [ Start  Resource ]  [[xJeaEndPoint]CleanAll]
VERBOSE: [REBEL-CA1]: LCM:  [ Start  Test     ]  [[xJeaEndPoint]CleanAll]
VERBOSE: [REBEL-CA1]:                            [[xJeaEndPoint]CleanAll] Importing the module MSFT_xJeaEndpoint in
force mode.
VERBOSE: [REBEL-CA1]:                            [[xJeaEndPoint]CleanAll] Monday, 24 April 2017 6:07:45 PM Start Test
[EndPoint]CleanALL
VERBOSE: [REBEL-CA1]:                            [[xJeaEndPoint]CleanAll] Monday, 24 April 2017 6:07:45 PM Done  Test
[EndPoint]CleanALL
VERBOSE: [REBEL-CA1]: LCM:  [ End    Test     ]  [[xJeaEndPoint]CleanAll]  in 0.1720 seconds.
VERBOSE: [REBEL-CA1]: LCM:  [ Start  Set      ]  [[xJeaEndPoint]CleanAll]
VERBOSE: [REBEL-CA1]:                            [[xJeaEndPoint]CleanAll] Importing the module MSFT_xJeaEndpoint in
force mode.
VERBOSE: [REBEL-CA1]:                            [[xJeaEndPoint]CleanAll] Monday, 24 April 2017 6:07:45 PM Start Set
[EndPoint]CleanALL
VERBOSE: [REBEL-CA1]:                            [[xJeaEndPoint]CleanAll] Remove [JeaEndpoints]    *
VERBOSE: [REBEL-CA1]:                            [[xJeaEndPoint]CleanAll] Remove [JSAUserAccount]*
VERBOSE: [REBEL-CA1]:                            [[xJeaEndPoint]CleanAll] Perform operation 'Query CimInstances' with
following parameters, ''queryExpression' = select * from Win32_UserAccount Where Name Like "JSA-%" AND
LocalAccount="TRUE",'queryDialect' = WQL,'namespaceName' = root\cimv2'.
VERBOSE: [REBEL-CA1]:                            [[xJeaEndPoint]CleanAll] Operation 'Query CimInstances' complete.
VERBOSE: [REBEL-CA1]:                            [[xJeaEndPoint]CleanAll] Perform operation 'Query CimInstances' with
following parameters, ''queryExpression' = select * from Win32_UserAccount Where Name = "JeaSchTaskAccount" AND
LocalAccount="TRUE",'queryDialect' = WQL,'namespaceName' = root\cimv2'.
```


Administrator: Windows PowerShell
Directory: C:\JeaDemo
Mode LastWriteTime Length Name
-a---- 24/04/2017 19:47 3212 localhost.mof
VERBOSE: Perform operation 'Invoke CimMethod' with following parameters, ''methodName' = SendConfigurationApply,'className' = MSFT_DSCLocalConfigurationManager,'namespaceName' = root/Microsoft/Windows/DesiredStateConfiguration'.
VERBOSE: An LCM method call arrived from computer REBEL-CA1 with user sid S-1-5-21-4041220333-1835452706-552999228-500.
VERBOSE: [REBEL-CA1]: LCM: [Start Set]
VERBOSE: [REBEL-CA1]: [DSCEngine] Importing the module C:\Program Files\WindowsPowerShell\Modules\xJea\0.2.16.6\DscResources\MSFT_xJeaToolkit\MSFT_xJeaToolkit.psm1 in force mode.
VERBOSE: [REBEL-CA1]: [DSCEngine] Importing the module C:\Program Files\WindowsPowerShell\Modules\xJea\0.2.16.6\DscResources\MSFT_xJeaEndpoint\MSFT_xJeaEndpoint.psm1 in force mode.
VERBOSE: [REBEL-CA1]: LCM: [Start Resource] [[xJeaToolKit]Process]
VERBOSE: [REBEL-CA1]: LCM: [Start Test] [[xJeaToolKit]Process]
VERBOSE: [REBEL-CA1]: [[xJeaToolKit]Process] Importing the module MSFT_xJeaToolkit in force mode.
VERBOSE: [REBEL-CA1]: [[xJeaToolKit]Process] Monday, 24 April 2017 6:47:03 PM Start Test [JeaToolkit]Process
VERBOSE: [REBEL-CA1]: [[xJeaToolKit]Process] [JeaToolkit]Process Present
VERBOSE: [REBEL-CA1]: [[xJeaToolKit]Process] Monday, 24 April 2017 6:47:03 PM Done Test [JeaToolkit]Process
VERBOSE: [REBEL-CA1]: LCM: [End Test] [[xJeaToolKit]Process] in 0.0930 seconds.
VERBOSE: [REBEL-CA1]: LCM: [Skip Set] [[xJeaToolKit]Process]
VERBOSE: [REBEL-CA1]: LCM: [End Resource] [[xJeaToolKit]Process]
VERBOSE: [REBEL-CA1]: LCM: [Start Resource] [[xJeaEndPoint]Demo1EP]
VERBOSE: [REBEL-CA1]: LCM: [Start Test] [[xJeaEndPoint]Demo1EP]
VERBOSE: [REBEL-CA1]: [[xJeaEndPoint]Demo1EP] Importing the module MSFT_xJeaEndpoint in force mode.
VERBOSE: [REBEL-CA1]: [[xJeaEndPoint]Demo1EP] Monday, 24 April 2017 6:47:03 PM Start Test [EndPoint]Demo1EP
VERBOSE: [REBEL-CA1]: [[xJeaEndPoint]Demo1EP] Test [JeaEndPoint] Demo1EP
VERBOSE: [REBEL-CA1]: [[xJeaEndPoint]Demo1EP] [JeaEndPoint] Demo1EP Present
VERBOSE: [REBEL-CA1]: [[xJeaEndPoint]Demo1EP] TEST SecurityDescriptorSddl
VERBOSE: [REBEL-CA1]: [[xJeaEndPoint]Demo1EP] TODO: Check for Toolkits, StartupScript and UserAccount
VERBOSE: [REBEL-CA1]: [[xJeaEndPoint]Demo1EP] Monday, 24 April 2017 6:47:03 PM Done Test [EndPoint]Demo1EP
VERBOSE: [REBEL-CA1]: LCM: [End Test] [[xJeaEndPoint]Demo1EP] in 0.2030 seconds.
VERBOSE: [REBEL-CA1]: LCM: [Skip Set] [[xJeaEndPoint]Demo1EP]
VERBOSE: [REBEL-CA1]: LCM: [End Resource] [[xJeaEndPoint]Demo1EP]
VERBOSE: [REBEL-CA1]: LCM: [End Set]
VERBOSE: [REBEL-CA1]: LCM: [End Set] in 0.5470 seconds.
VERBOSE: Operation 'Invoke CimMethod' complete.
VERBOSE: Time taken for configuration job to complete is 0.681 seconds


PS C:\Program Files\WindowsPowerShell\Modules\xJea\0.2.16.6\Examples> Get-PSSessionConfiguration
Name : Demo1EP
PSVersion : 5.1
startupscript : C:\Program Files\Jea\StartupScript\Initialize-Demo1EP.ps1
RunAsUser : JSA-Demo1EP
Permission : Everyone AccessAllowed
Name : microsoft.powershell
PSVersion : 5.1
StartupScript :
RunAsUser :
Permission : NT AUTHORITY\INTERACTIVE AccessAllowed, BUILTIN\Administrators AccessAllowed, BUILTIN\Remote Management Users AccessAllowed
Name : microsoft.powershell.workflow
PSVersion : 5.1
StartupScript :
RunAsUser :
Permission : BUILTIN\Administrators AccessAllowed, BUILTIN\Remote Management Users AccessAllowed
Name : microsoft.powershell32
PSVersion : 5.1
StartupScript :
RunAsUser :
Permission : NT AUTHORITY\INTERACTIVE AccessAllowed, BUILTIN\Administrators AccessAllowed, BUILTIN\Remote Management Users AccessAllowed
Name : microsoft.windows.servermanagerworkflows
PSVersion : 3.0
StartupScript :
RunAsUser :
Permission : NT AUTHORITY\INTERACTIVE AccessAllowed, BUILTIN\Administrators AccessAllowed


PS C:\Windows\system32> Enter-PSSession -ComputerName localhost -ConfigurationName demo1ep
[localhost]: PS C:\Users\JSA-Demo1EP\Documents>

```
PS C:\Windows\system32> get-localuser

Name               Enabled Description
----               ------- -----------
Administrator      True    Built-in account for administering the computer/domain
DefaultAccount     False   A user account managed by the system.
demo               True
Guest              False   Built-in account for guest access to the computer/domain
JeaSchTaskAccount  True    This is a special jea account to run the ResetJeaSessionAccountPasswords Scheduled task
JSA-Demo1EP        True    PowerShell Session Acount
```

```
PS C:\Windows\system32> Get-LocalGroupMember -Group "Administrators"

ObjectClass Name                        PrincipalSource
----------- ----                        ---------------
User        REBELADMIN\adam             ActiveDirectory
User        REBELADMIN\Administrator    ActiveDirectory
Group       REBELADMIN\Domain Admins    ActiveDirectory
User        REBEL-CA1\Administrator     Local
User        REBEL-CA1\demo              Local
User        REBEL-CA1\JeaSchTaskAccount Local
User        REBEL-CA1\JSA-Demo1EP       Local
```

```
PS C:\Windows\system32> Enter-PSSession -ComputerName localhost -ConfigurationName demo1ep
[localhost]: PS C:\Users\JSA-Demo1EP\Documents> get-service

Status   Name               DisplayName
------   ----               -----------
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Running  AppHostSvc         Application Host Helper Service
Stopped  AppIDSvc           Application Identity
Running  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Stopped  AppReadiness       App Readiness
Stopped  AppVClient         Microsoft App-V Client
Stopped  AppXSvc            AppX Deployment Service (AppXSVC)
Stopped  AudioEndpointBu... Windows Audio Endpoint Builder
Stopped  Audiosrv           Windows Audio
Stopped  AxInstSV           ActiveX Installer (AxInstSV)
Running  BFE                Base Filtering Engine
Stopped  BITS               Background Intelligent Transfer Ser...
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Stopped  Browser            Computer Browser
Stopped  bthserv            Bluetooth Support Service
Running  CDPSvc             Connected Devices Platform Service
Running  CDPUserSvc_32e3f2  CDPUserSvc_32e3f2
Running  CertPropSvc        Certificate Propagation
Running  CertSvc            Active Directory Certificate Services
Stopped  ClipSVC            Client License Service (ClipSVC)
Stopped  COMSysApp          COM+ System Application
Running  CoreMessagingRe... CoreMessaging
Running  CryptSvc           Cryptographic Services
Stopped  CscService         Offline Files
Running  DcomLaunch         DCOM Server Process Launcher
Stopped  DcpSvc             DataCollectionPublishingService
Stopped  defragsvc          Optimize drives
Stopped  DeviceAssociati... Device Association Service
Stopped  DeviceInstall      Device Install Service
Stopped  DevQueryBroker     DevQuery Background Discovery Broker
Running  Dhcp               DHCP Client
Stopped  diagnosticshub.... Microsoft (R) Diagnostics Hub Stand...
Running  DiagTrack          Connected User Experiences and Tele...
Stopped  DmEnrollmentSvc    Device Management Enrollment Service
Stopped  dmwappushservice   dmwappushsvc
Running  Dnscache           DNS Client
Stopped  dot3svc            Wired AutoConfig
Running  DPS                Diagnostic Policy Service
Stopped  DsmSvc             Device Setup Manager
```

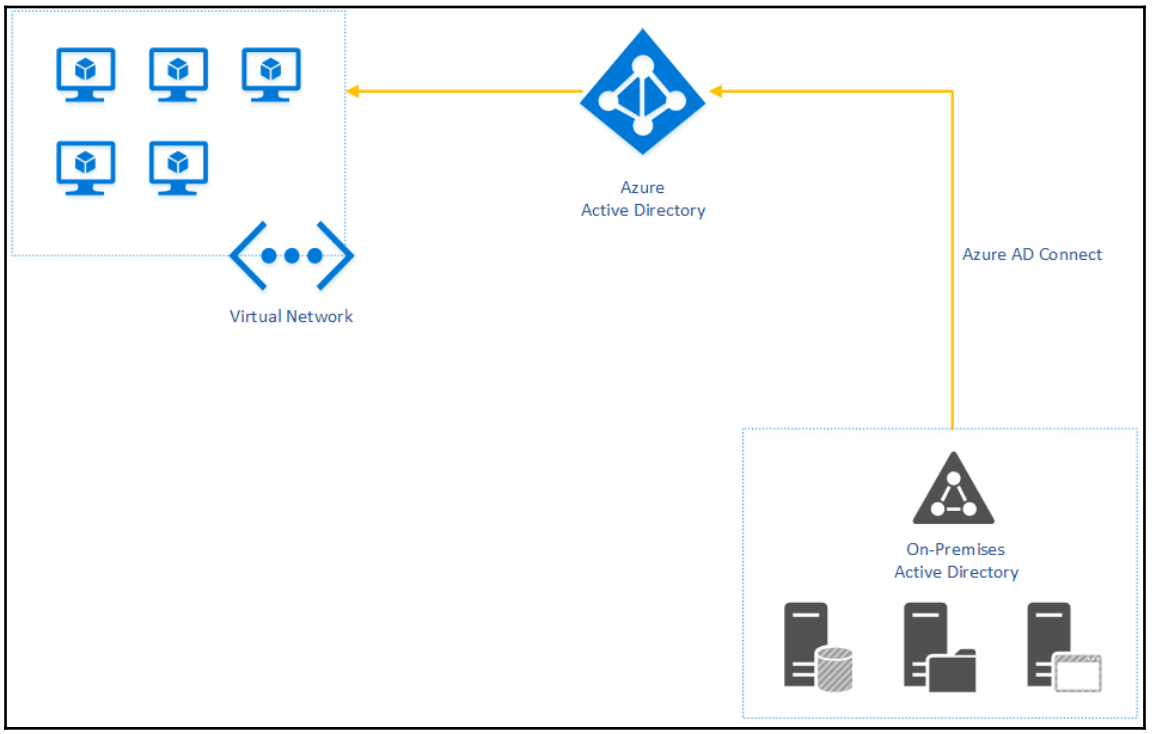
```
[localhost]: PS C:\Users\JSA-Demo1EP\Documents> restart-computer
The term 'Restart-Computer' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
    + CategoryInfo          : ObjectNotFound: (Restart-Computer:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

[localhost]: PS C:\Users\JSA-Demo1EP\Documents> _
```

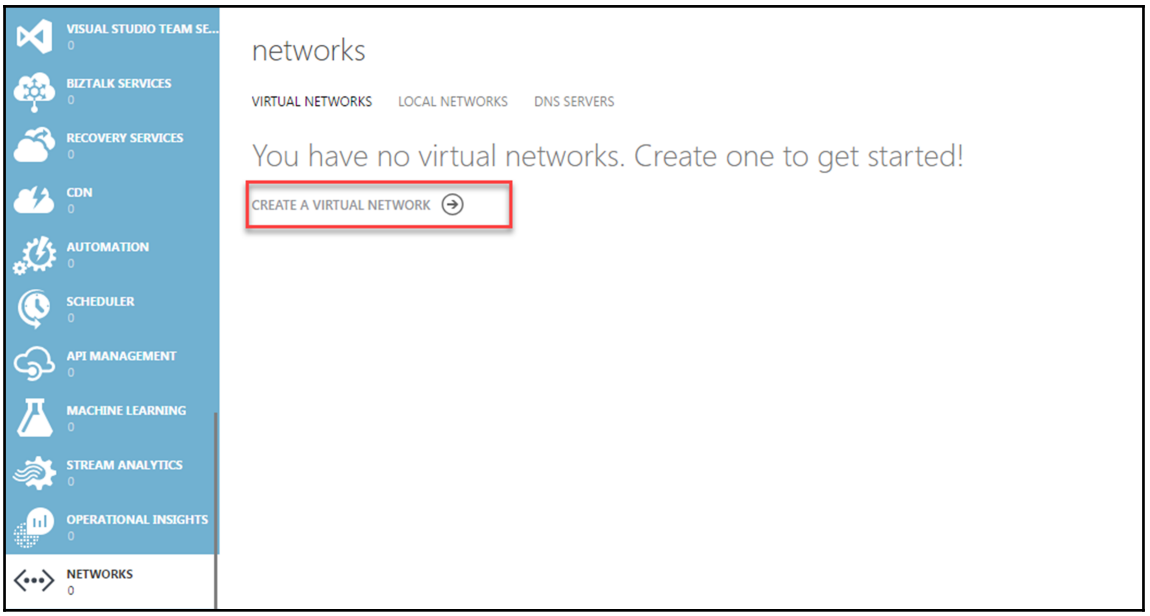
```
PS C:\Program Files\WindowsPowerShell\Modules\xJea\0.2.16.6\Examples> Get-PSSessionConfiguration


Name          : Demo1EP
PSVersion     : 5.1
startupscript : C:\Program Files\Jea\StartupScript\Initialize-Demo1EP.ps1
RunAsUser     : JSA-Demo1EP
Permission    : Everyone AccessAllowed

Name          : Demo2EP
PSVersion     : 5.1
startupscript : C:\Program Files\Jea\StartupScript\Initialize-Demo2EP.ps1
RunAsUser     : JSA-Demo2EP
Permission    : Everyone AccessAllowed

Name          : microsoft.powershell
PSVersion     : 5.1
StartupScript :
RunAsUser     :
Permission    : NT AUTHORITY\INTERACTIVE AccessAllowed, BUILTIN\Administrators AccessAllowed, BUILTIN\Remote
                Management Users AccessAllowed

Name          : microsoft.powershell.workflow
PSVersion     : 5.1
StartupScript :
RunAsUser     :
Permission    : BUILTIN\Administrators AccessAllowed, BUILTIN\Remote Management Users AccessAllowed

Name          : microsoft.powershell32
PSVersion     : 5.1
StartupScript :
RunAsUser     :
Permission    : NT AUTHORITY\INTERACTIVE AccessAllowed, BUILTIN\Administrators AccessAllowed, BUILTIN\Remote
                Management Users AccessAllowed
```

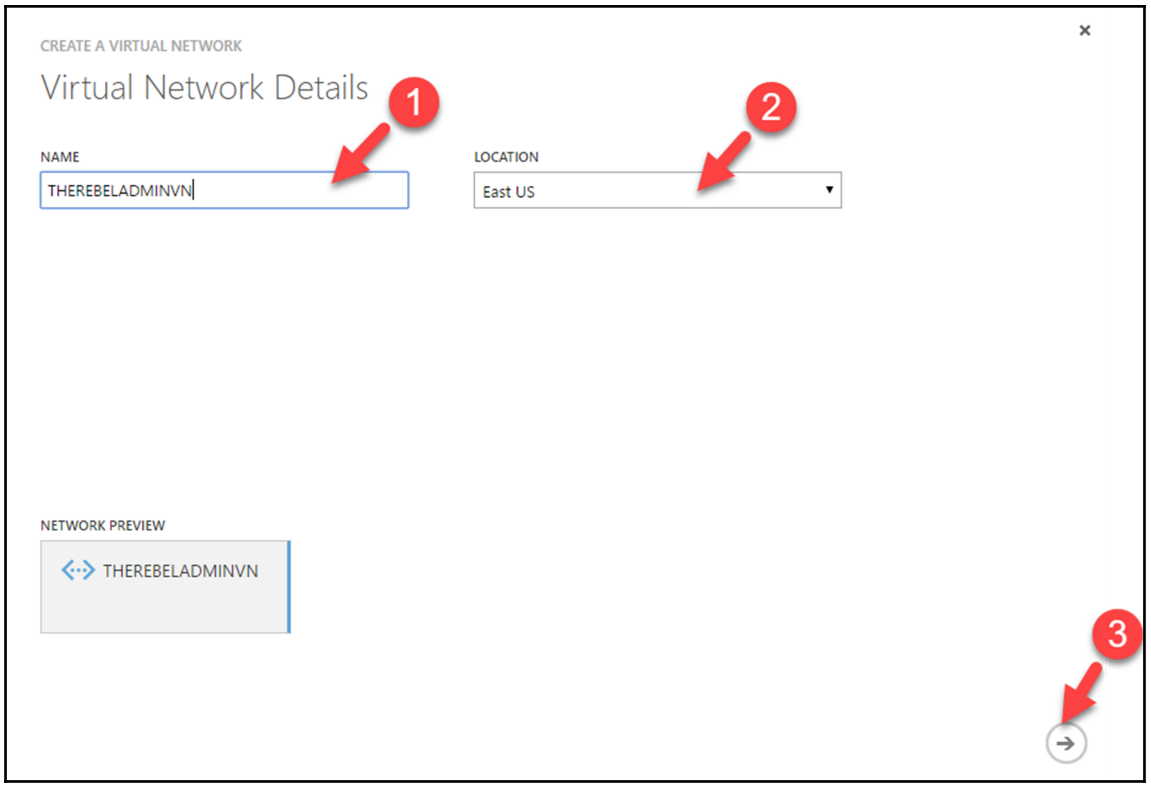
```
PS C:\Windows\system32> Enter-PSSession -ComputerName localhost -ConfigurationName demo2ep
[localhost]: PS C:\Users\JSA-Demo2EP\Documents> get-command

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        A:
Function        B:
Function        C:
Function        cd..
Function        cd\
Function        Clear-Host
Function        D:
Function        E:
Function        F:
Function        format-list                                        0.0        SafeProxy
Function        format-table                                       0.0        SafeProxy
Function        G:
Function        Get-SmbBandwidthLimit                              0.0        SMBGet-Toolkit
Function        Get-SmbClientConfiguration                         0.0        SMBGet-Toolkit
Function        Get-SmbClientNetworkInterface                      0.0        SMBGet-Toolkit
Function        Get-SmbConnection                                  0.0        SMBGet-Toolkit
Function        Get-SmbDelegation                                  0.0        SMBGet-Toolkit
Function        Get-SmbMapping                                     0.0        SMBGet-Toolkit
Function        Get-SmbMultichannelConnection                      0.0        SMBGet-Toolkit
Function        Get-SmbMultichannelConstraint                      0.0        SMBGet-Toolkit
Function        Get-SmbOpenFile                                    0.0        SMBGet-Toolkit
Function        Get-SmbServerConfiguration                         0.0        SMBGet-Toolkit
Function        Get-SmbServerNetworkInterface                      0.0        SMBGet-Toolkit
Function        Get-SmbSession                                     0.0        SMBGet-Toolkit
Function        Get-SmbShare                                       0.0        SMBGet-Toolkit
Function        Get-SmbShareAccess                                 0.0        SMBGet-Toolkit
Function        Get-Verb
Function        Group-Object                                       0.0        SafeProxy
Function        H:
Function        help
Function        I:
Function        ImportSystemModules
Function        J:
Function        K:
Function        L:
Function        M:
Function        mkdir
Function        more
Function        N:
Function        O:
Function        oss
Function        P:
```

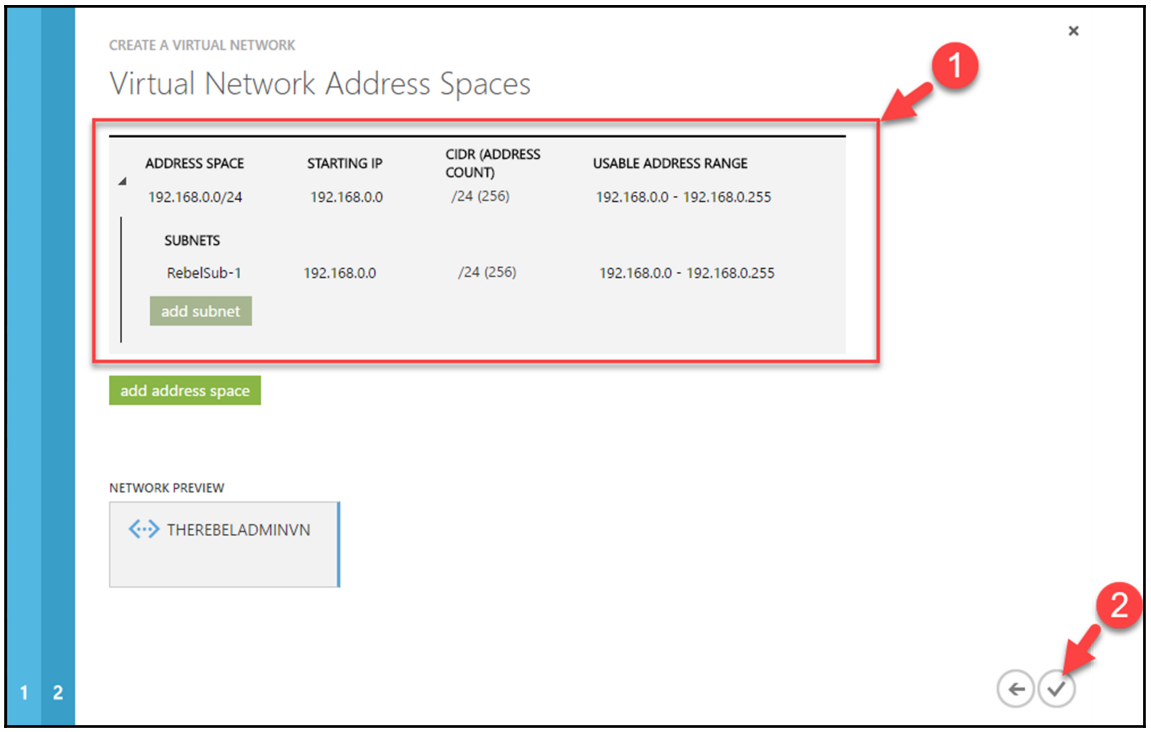
```
[localhost]: PS C:\Users\JSA-Demo2EP\Documents> get-smbshare

Name        ScopeName Path                                  Description
----        --------- ----                                  -----------
ADMIN$      *         C:\Windows                            Remote Admin
C$          *         C:\                                   Default share
CertEnroll  *         C:\Windows\system32\CertSrv\CertEnroll Active Directory Certificate Services share
IPC$        *                                               Remote IPC


[localhost]: PS C:\Users\JSA-Demo2EP\Documents> restart-computer
The term 'Restart-Computer' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
    + CategoryInfo          : ObjectNotFound: (Restart-Computer:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

[localhost]: PS C:\Users\JSA-Demo2EP\Documents> _
```

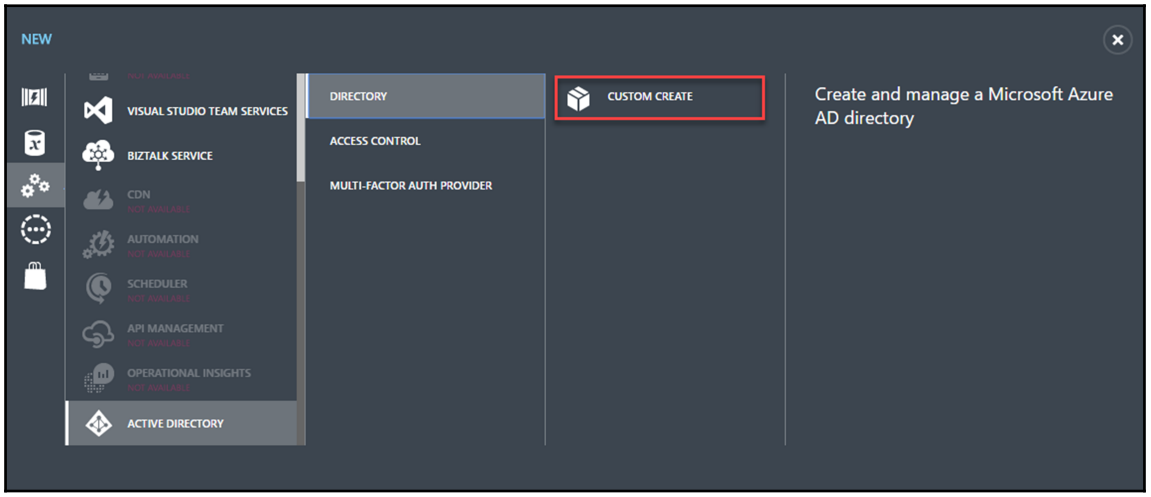
Chapter 17: Azure Active Directory Hybrid Setup

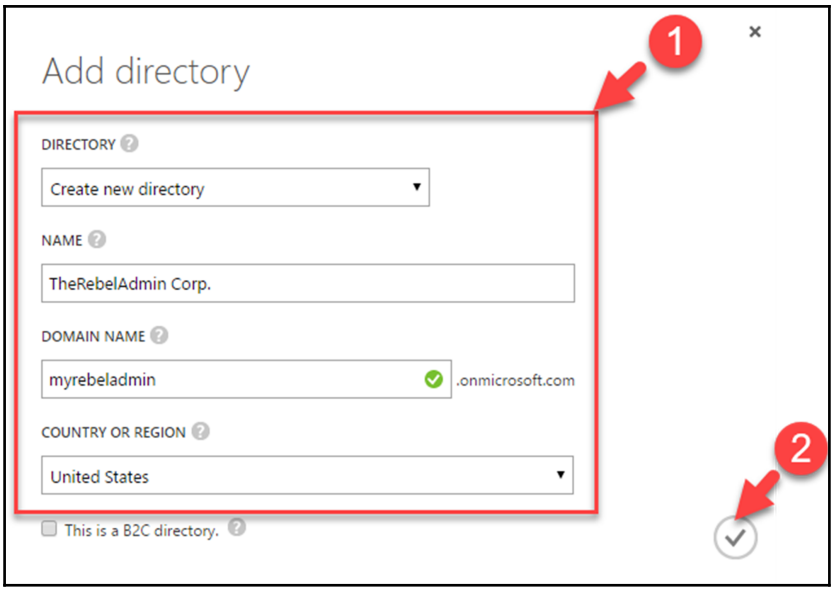


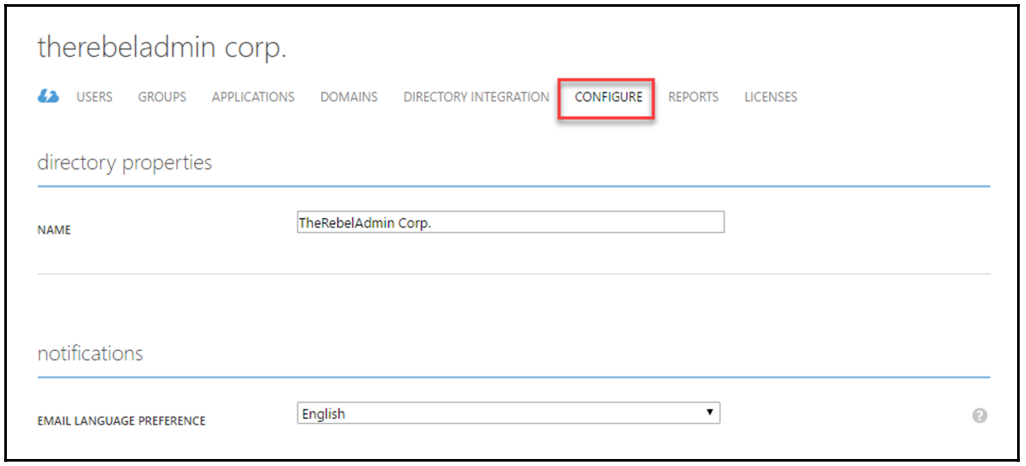

VISUAL STUDIO TEAM SE...
0
BIZTALK SERVICES
0
RECOVERY SERVICES
0
CDN
0
AUTOMATION
0
SCHEDULER
0
API MANAGEMENT
0
MACHINE LEARNING
0
STREAM ANALYTICS
0
OPERATIONAL INSIGHTS
0
NETWORKS
0
networks
VIRTUAL NETWORKS
LOCAL NETWORKS
DNS SERVERS
You have no virtual networks. Create one to get started!
CREATE A VIRTUAL NETWORK

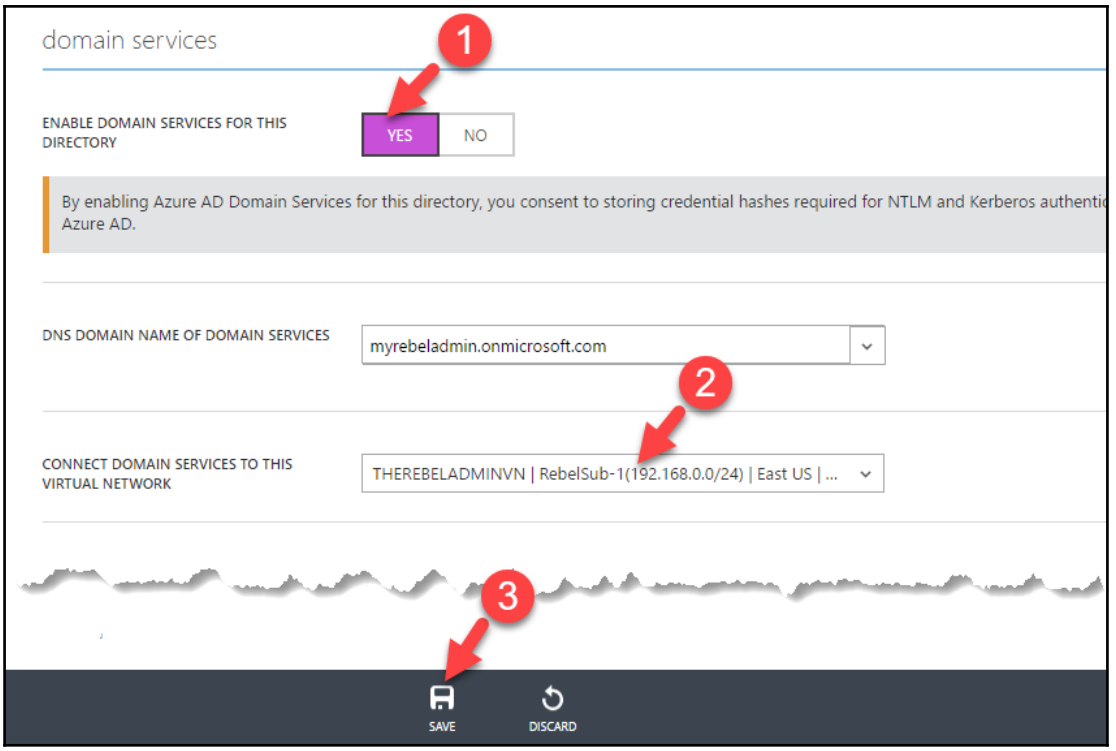

CREATE A VIRTUAL NETWORK
Virtual Network Details
1
2
NAME
THEREBELADMINVN
LOCATION
East US
NETWORK PREVIEW
THEREBELADMINVN
3

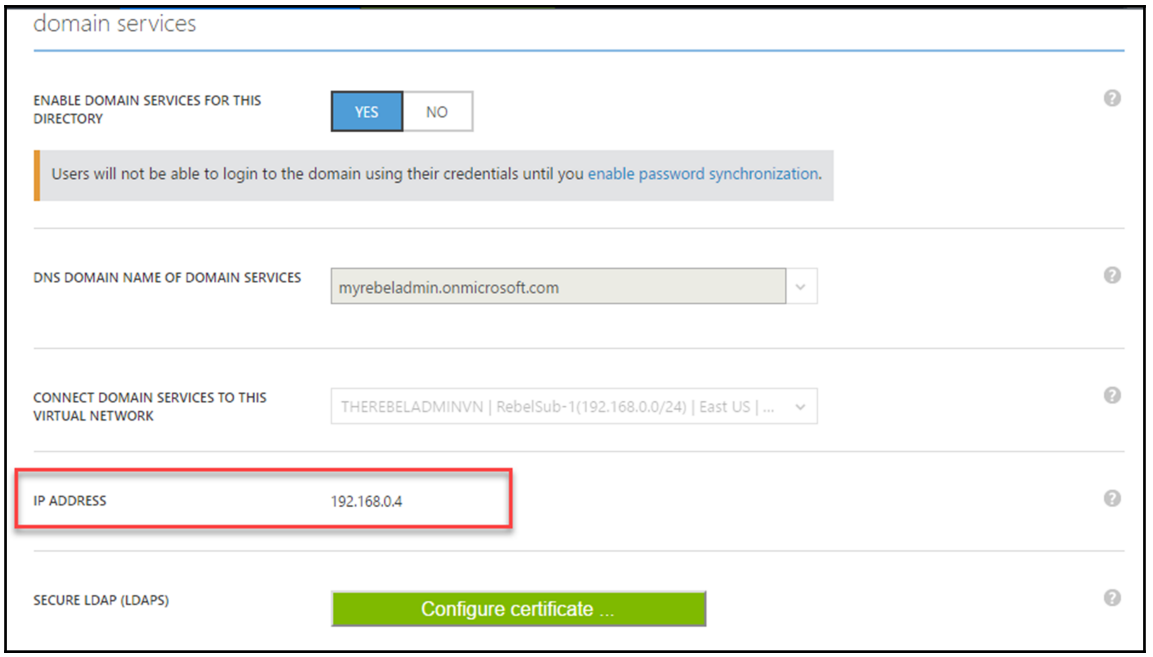

CREATE A VIRTUAL NETWORK
Virtual Network Address Spaces
1
ADDRESS SPACE
STARTING IP
CIDR (ADDRESS COUNT)
USABLE ADDRESS RANGE
192.168.0.0/24
192.168.0.0
/24 (256)
192.168.0.0 - 192.168.0.255
SUBNETS
RebelSub-1
192.168.0.0
/24 (256)
192.168.0.0 - 192.168.0.255
add subnet
add address space
NETWORK PREVIEW
THEREBELADMINVN
2
1 2


NEW
VISUAL STUDIO TEAM SERVICES
BIZTALK SERVICE
CDN
AUTOMATION
SCHEDULER
API MANAGEMENT
OPERATIONAL INSIGHTS
ACTIVE DIRECTORY
DIRECTORY
ACCESS CONTROL
MULTI-FACTOR AUTH PROVIDER
CUSTOM CREATE
Create and manage a Microsoft Azure AD directory

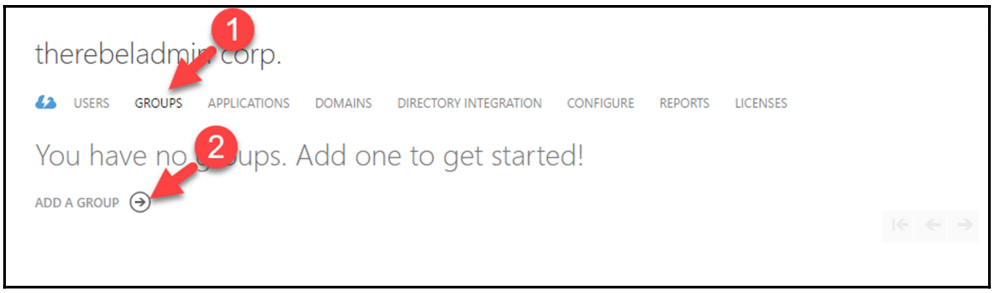

Add directory
1
DIRECTORY
Create new directory
NAME
TheRebelAdmin Corp.
DOMAIN NAME
myrebeladmin
.onmicrosoft.com
COUNTRY OR REGION
United States
This is a B2C directory.
2

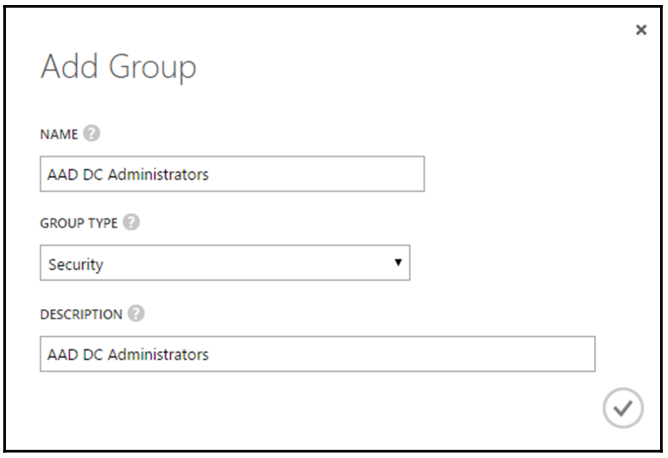

therebeladmin corp.
USERS
GROUPS
APPLICATIONS
DOMAINS
DIRECTORY INTEGRATION
CONFIGURE
REPORTS
LICENSES
directory properties
NAME
TheRebelAdmin Corp.
notifications
EMAIL LANGUAGE PREFERENCE
English

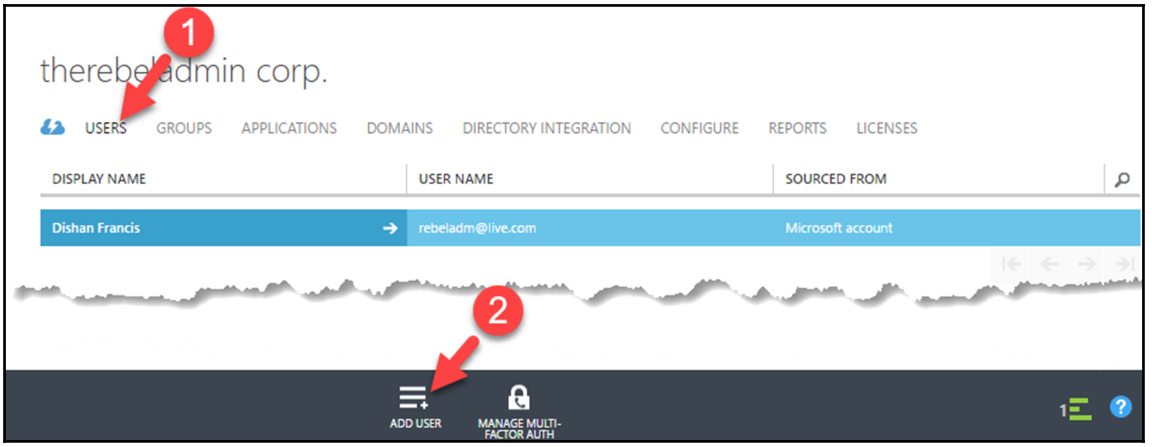

domain services
1
ENABLE DOMAIN SERVICES FOR THIS DIRECTORY
YES
NO
By enabling Azure AD Domain Services for this directory, you consent to storing credential hashes required for NTLM and Kerberos authentic
Azure AD.
DNS DOMAIN NAME OF DOMAIN SERVICES
myrebeladmin.onmicrosoft.com
2
CONNECT DOMAIN SERVICES TO THIS VIRTUAL NETWORK
THEREBELADMINVN | RebelSub-1(192.168.0.0/24) | East US | ...
3
SAVE
DISCARD

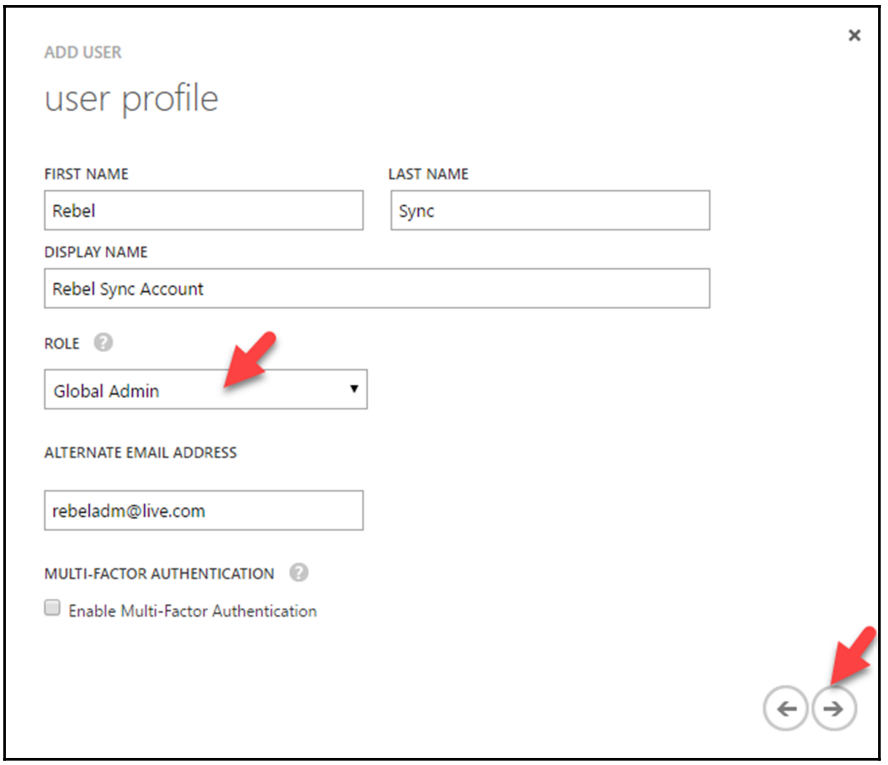

domain services
ENABLE DOMAIN SERVICES FOR THIS DIRECTORY
YES
NO
Users will not be able to login to the domain using their credentials until you enable password synchronization.
DNS DOMAIN NAME OF DOMAIN SERVICES
myrebeladmin.onmicrosoft.com
CONNECT DOMAIN SERVICES TO THIS VIRTUAL NETWORK
THEREBELADMINVN | RebelSub-1(192.168.0.0/24) | East US | ...
IP ADDRESS
192.168.0.4
SECURE LDAP (LDAPS)
Configure certificate ...

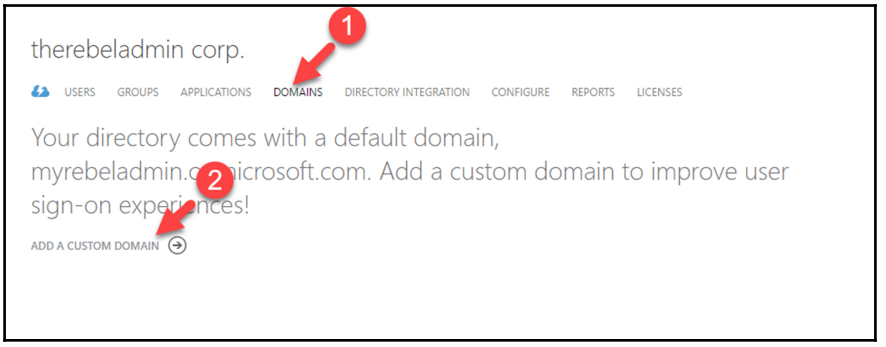

therebeladminvn
DASHBOARD
CONFIGURE
CERTIFICATES
dns servers
therebeladmin ns1
192.168.0.4
SELECT OR ENTER NAM
IP ADDRESS
SAVE
DISCARD
1
2
3

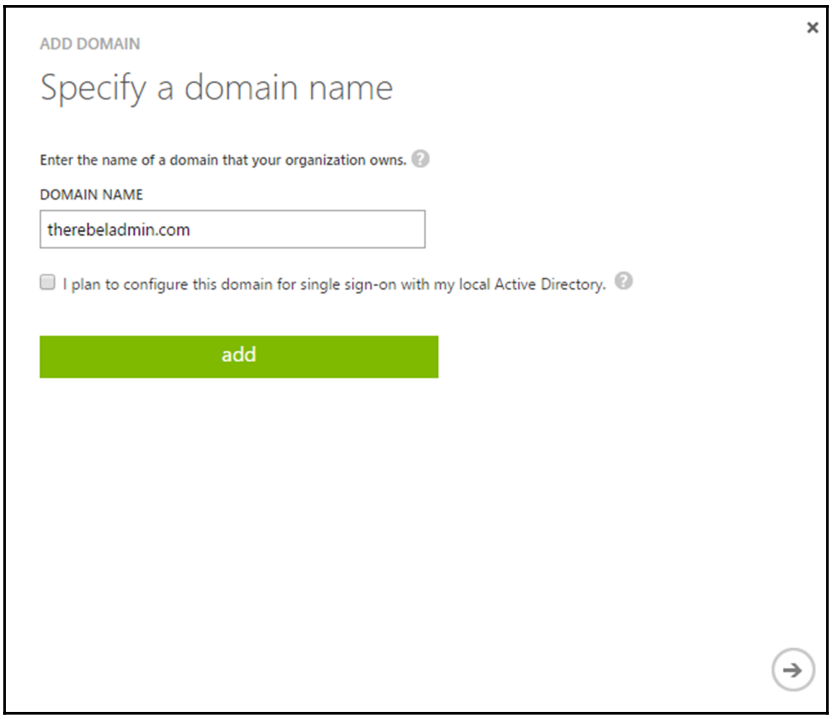

1
therebeladmin corp.
USERS
GROUPS
APPLICATIONS
DOMAINS
DIRECTORY INTEGRATION
CONFIGURE
REPORTS
LICENSES
2
You have no groups. Add one to get started!
ADD A GROUP

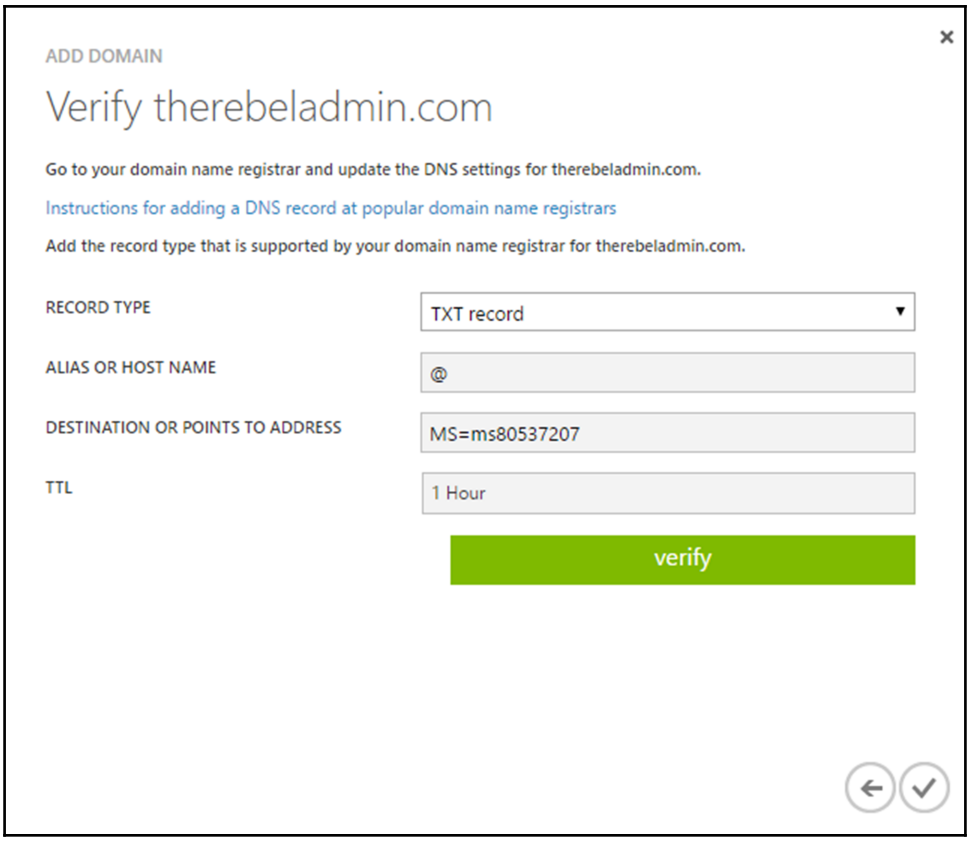

Add Group
NAME
AAD DC Administrators
GROUP TYPE
Security
DESCRIPTION
AAD DC Administrators

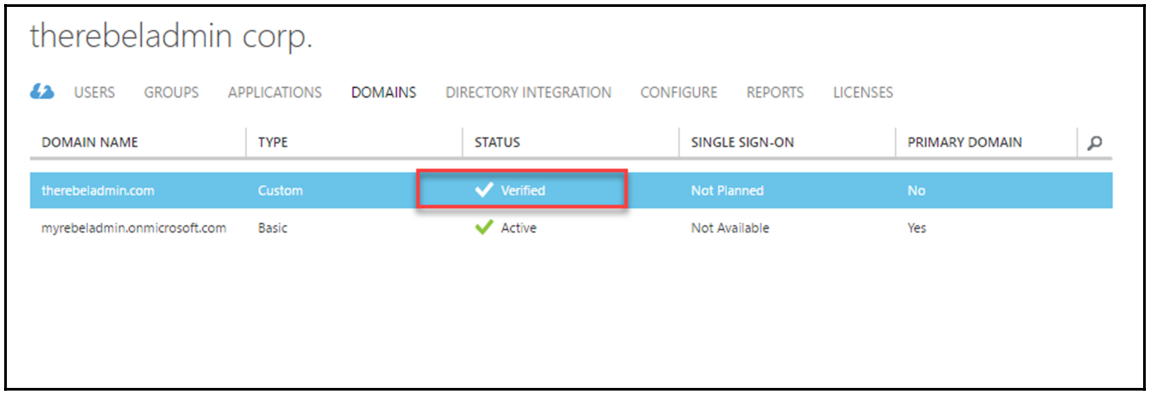

1
therebeladmin corp.
USERS
GROUPS
APPLICATIONS
DOMAINS
DIRECTORY INTEGRATION
CONFIGURE
REPORTS
LICENSES
DISPLAY NAME
USER NAME
SOURCED FROM
Dishan Francis
rebeladm@live.com
Microsoft account
2
ADD USER
MANAGE MULTI-FACTOR AUTH

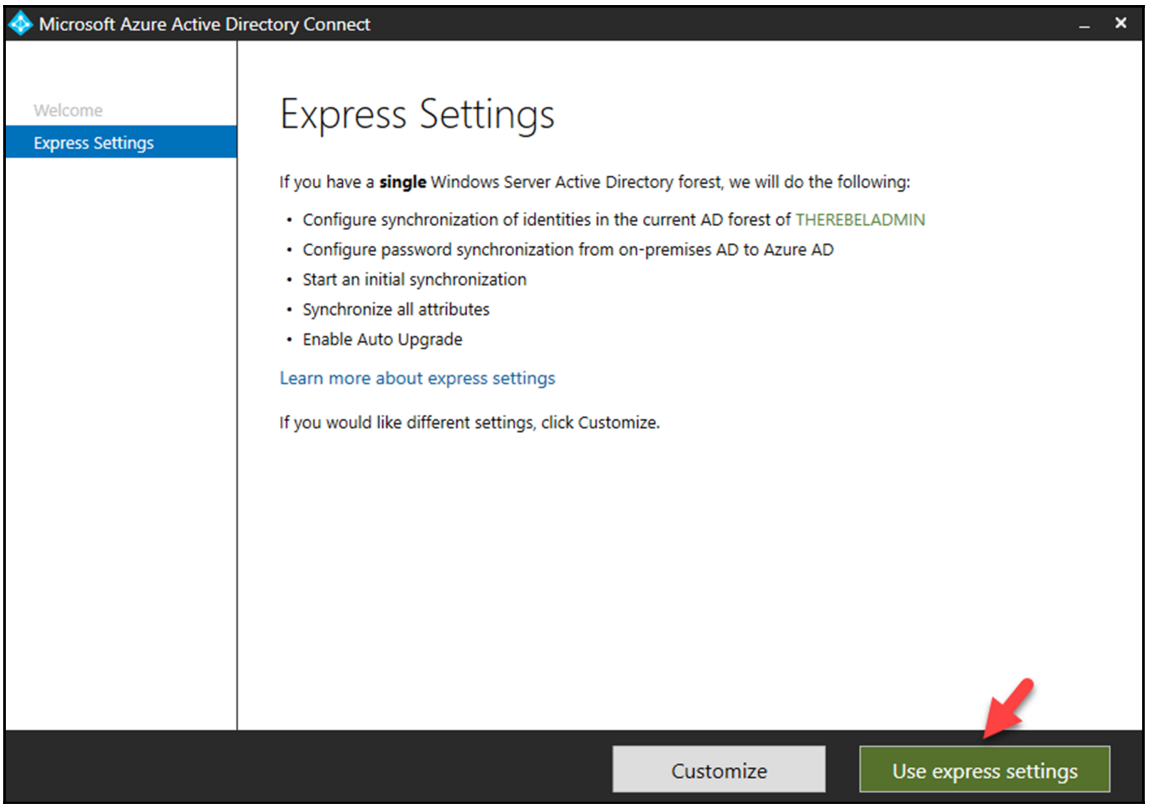

ADD USER
user profile
FIRST NAME
Rebel
LAST NAME
Sync
DISPLAY NAME
Rebel Sync Account
ROLE
Global Admin
ALTERNATE EMAIL ADDRESS
rebeladm@live.com
MULTI-FACTOR AUTHENTICATION
Enable Multi-Factor Authentication

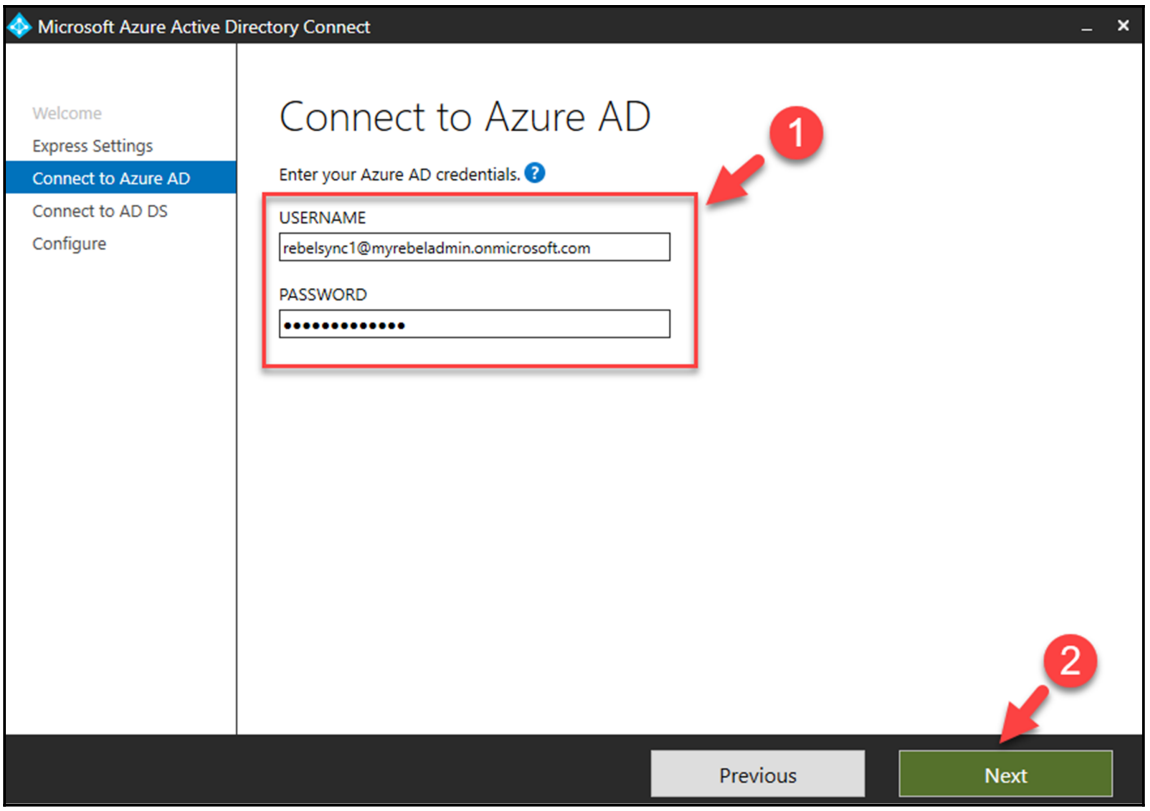

1
therebeladmin corp.
USERS
GROUPS
APPLICATIONS
DOMAINS
DIRECTORY INTEGRATION
CONFIGURE
REPORTS
LICENSES
Your directory comes with a default domain,
myrebeladmin.onmicrosoft.com. Add a custom domain to improve user
sign-on experiences!
2
ADD A CUSTOM DOMAIN

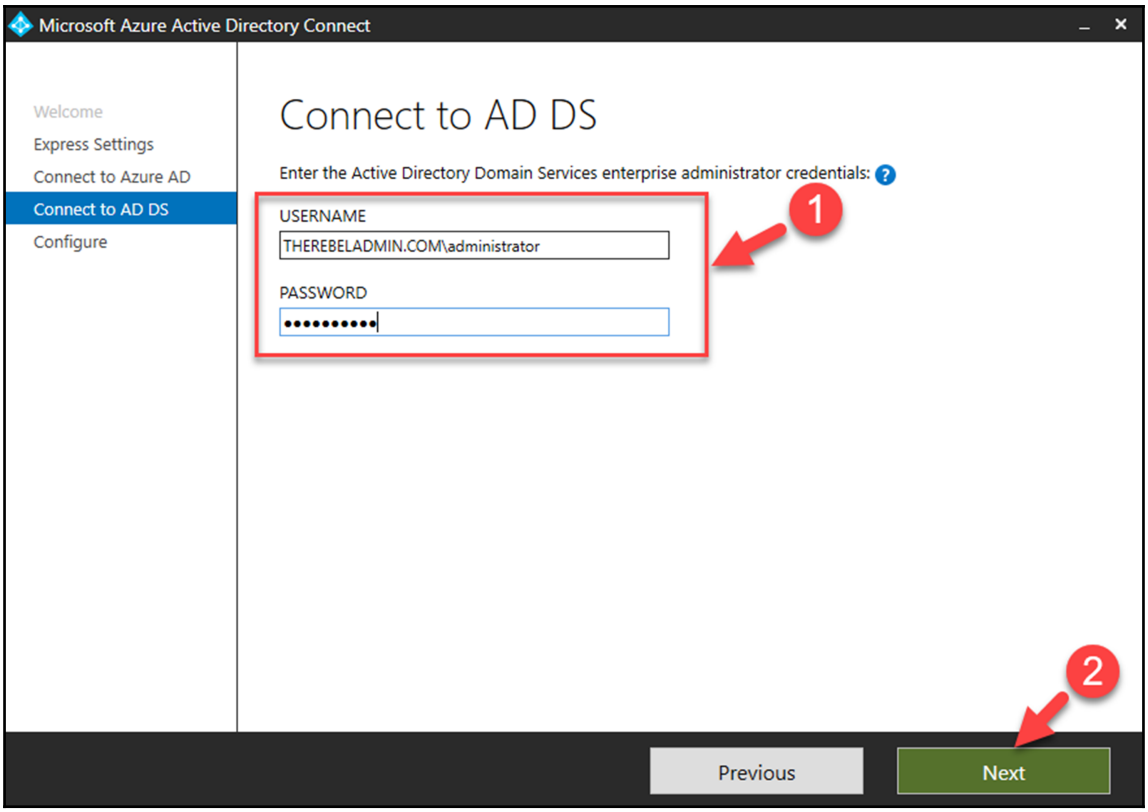

ADD DOMAIN
Specify a domain name
Enter the name of a domain that your organization owns.
DOMAIN NAME
therebeladmin.com
I plan to configure this domain for single sign-on with my local Active Directory.
add

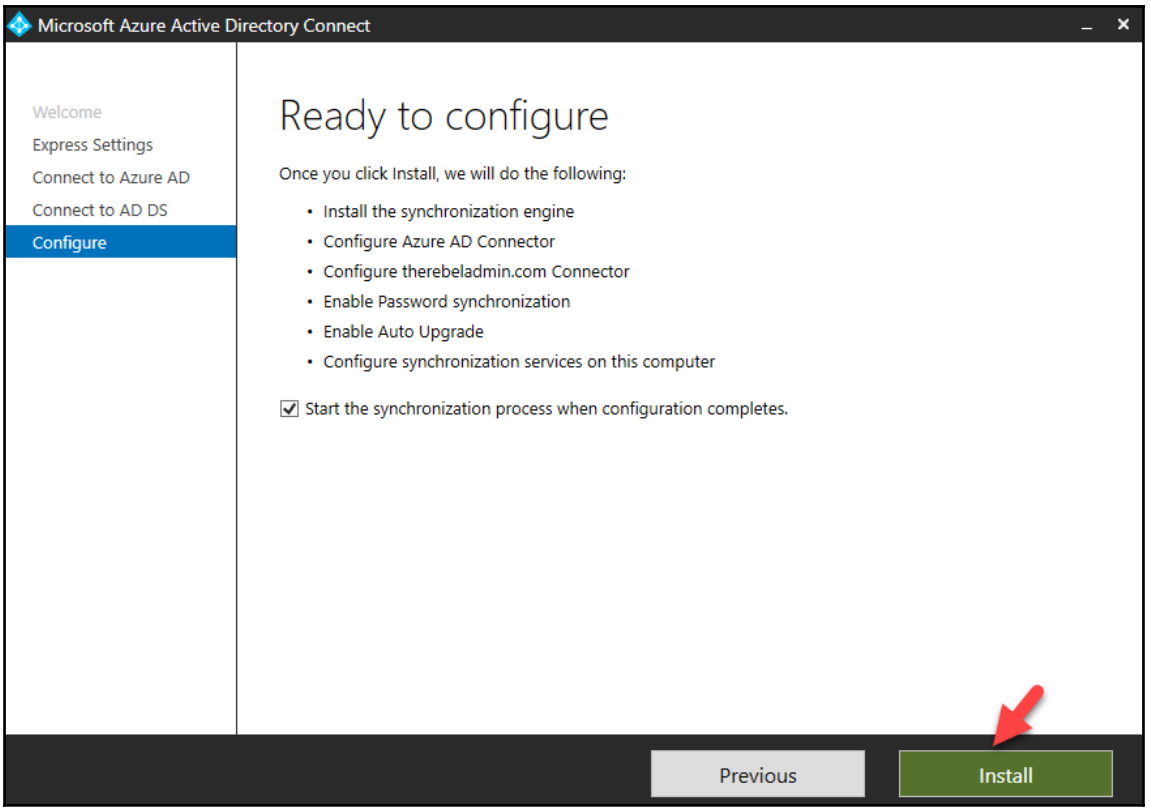

ADD DOMAIN
Verify therebeladmin.com
Go to your domain name registrar and update the DNS settings for therebeladmin.com.
Instructions for adding a DNS record at popular domain name registrars
Add the record type that is supported by your domain name registrar for therebeladmin.com.
RECORD TYPE
TXT record
ALIAS OR HOST NAME
@
DESTINATION OR POINTS TO ADDRESS
MS=ms80537207
TTL
1 Hour
verify

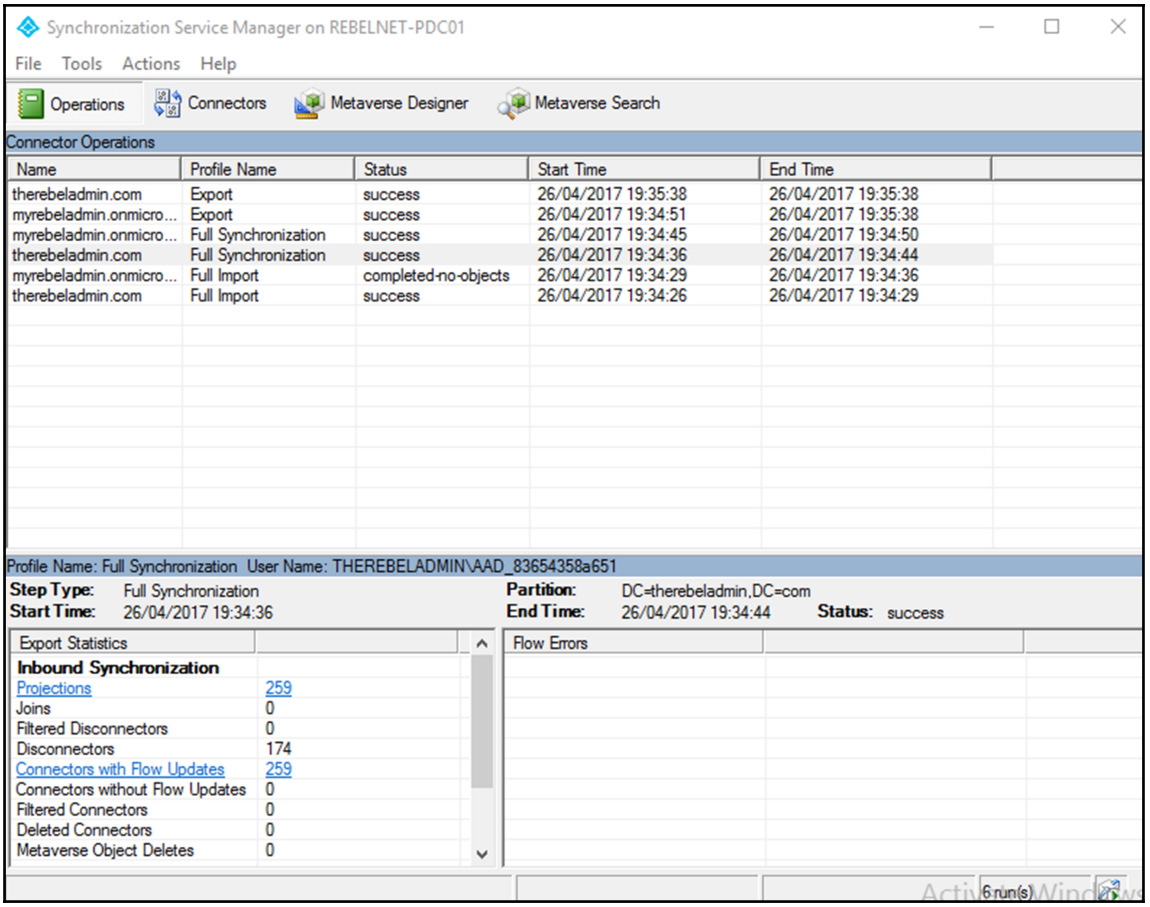

therebeladmin corp.
USERS
GROUPS
APPLICATIONS
DOMAINS
DIRECTORY INTEGRATION
CONFIGURE
REPORTS
LICENSES
DOMAIN NAME
TYPE
STATUS
SINGLE SIGN-ON
PRIMARY DOMAIN
therebeladmin.com
Custom
Verified
Not Planned
No
myrebeladmin.onmicrosoft.com
Basic
Active
Not Available
Yes

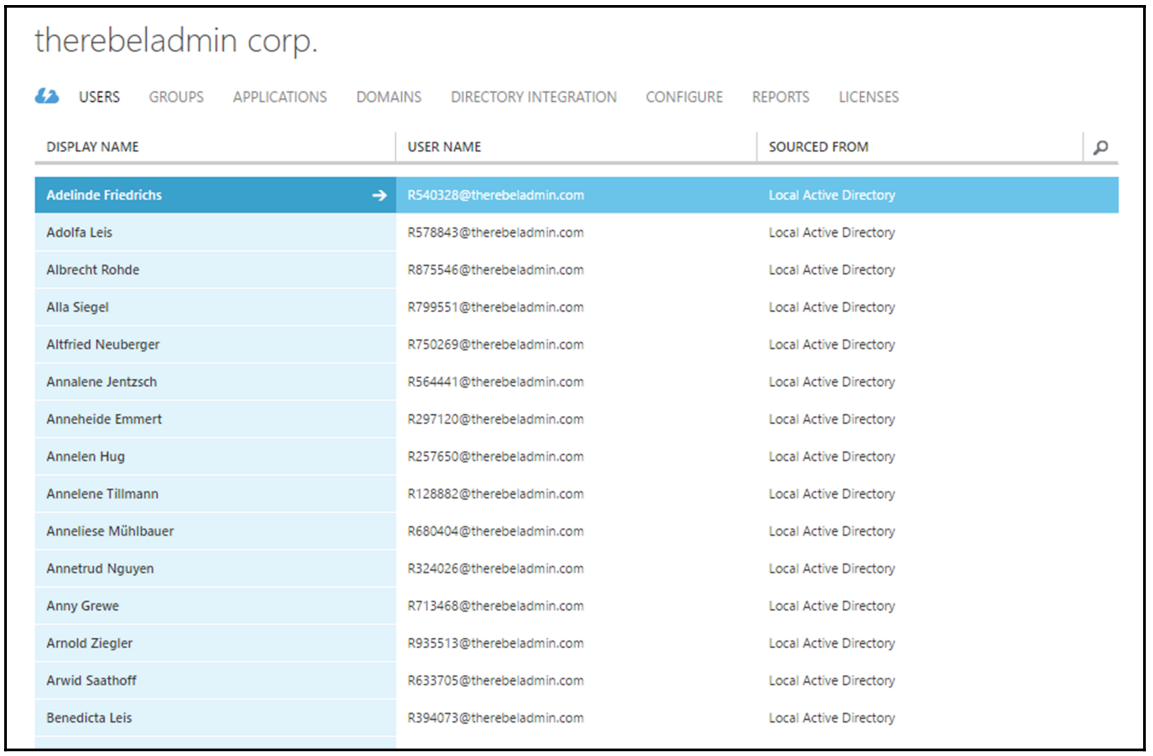

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Express Settings
If you have a single Windows Server Active Directory forest, we will do the following:
Configure synchronization of identities in the current AD forest of THEREBELADMIN
Configure password synchronization from on-premises AD to Azure AD
Start an initial synchronization
Synchronize all attributes
Enable Auto Upgrade
Learn more about express settings
If you would like different settings, click Customize.
Customize
Use express settings

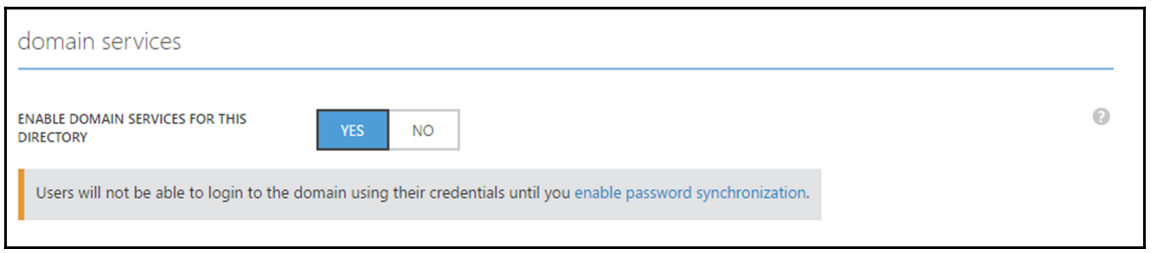

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Connect to Azure AD
Connect to AD DS
Configure
Connect to Azure AD
Enter your Azure AD credentials.
USERNAME
rebelsync1@myrebeladmin.onmicrosoft.com
PASSWORD
1
2
Previous
Next

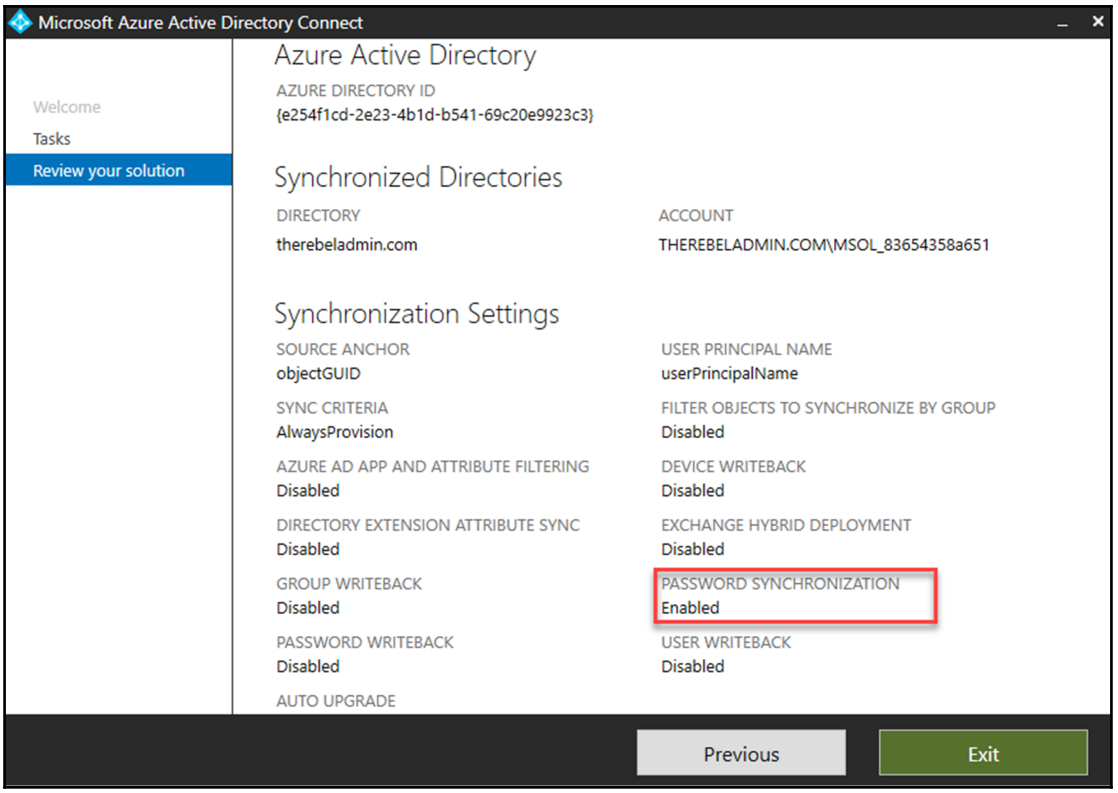

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Connect to Azure AD
Connect to AD DS
Configure
Connect to AD DS
Enter the Active Directory Domain Services enterprise administrator credentials:
USERNAME
THEREBELADMIN.COM\administrator
PASSWORD
1
2
Previous
Next

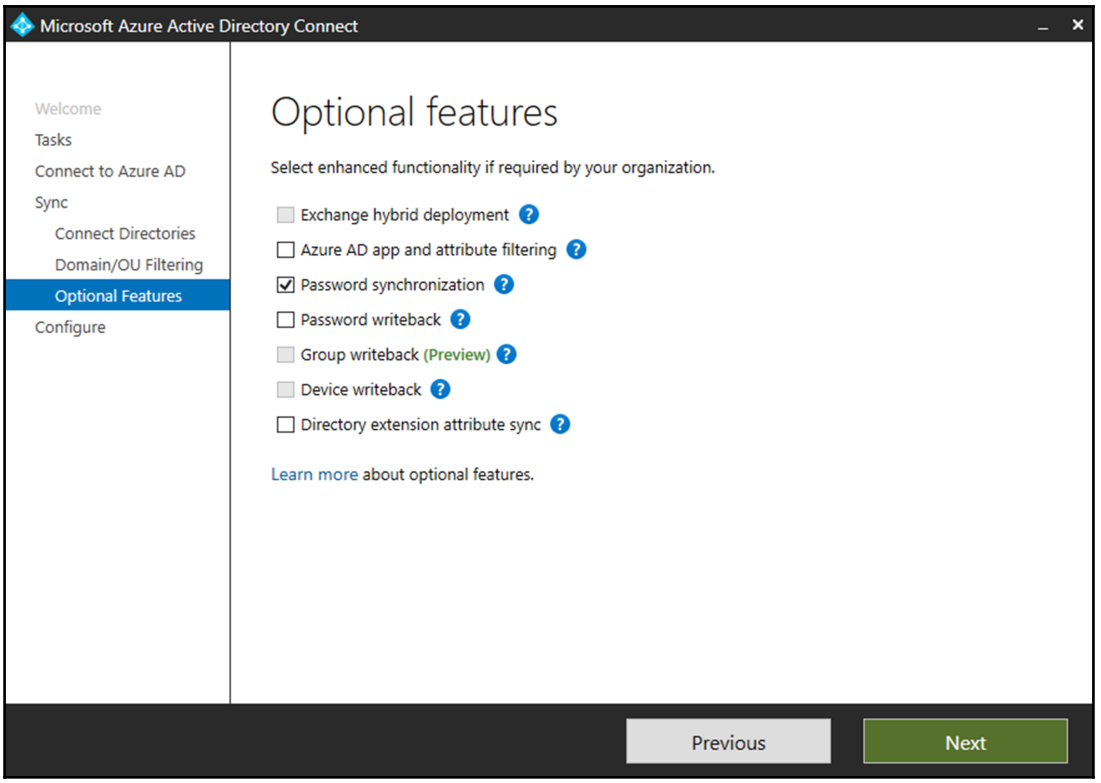

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Connect to Azure AD
Connect to AD DS
Configure
Ready to configure
Once you click Install, we will do the following:
• Install the synchronization engine
• Configure Azure AD Connector
• Configure therebeladmin.com Connector
• Enable Password synchronization
• Enable Auto Upgrade
• Configure synchronization services on this computer
Start the synchronization process when configuration completes.
Previous
Install

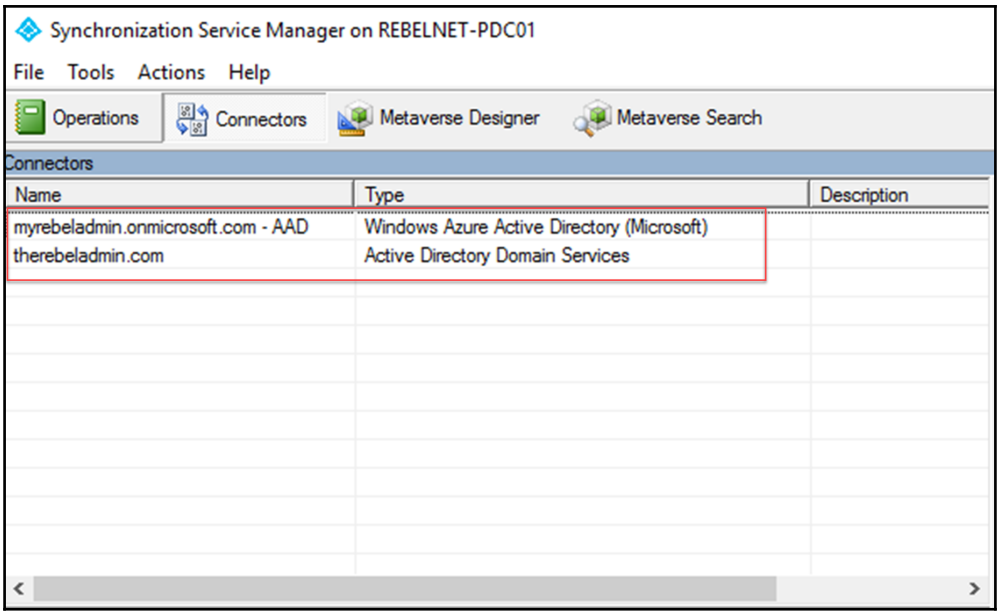

Synchronization Service Manager on REBELNET-PDC01
File Tools Actions Help
Operations
Connectors
Metaverse Designer
Metaverse Search
Connector Operations
Name | Profile Name | Status | Start Time | End Time
therebeladmin.com | Export | success | 26/04/2017 19:35:38 | 26/04/2017 19:35:38
myrebeladmin.onmicro... | Export | success | 26/04/2017 19:34:51 | 26/04/2017 19:35:38
myrebeladmin.onmicro... | Full Synchronization | success | 26/04/2017 19:34:45 | 26/04/2017 19:34:50
therebeladmin.com | Full Synchronization | success | 26/04/2017 19:34:36 | 26/04/2017 19:34:44
myrebeladmin.onmicro... | Full Import | completed-no-objects | 26/04/2017 19:34:29 | 26/04/2017 19:34:36
therebeladmin.com | Full Import | success | 26/04/2017 19:34:26 | 26/04/2017 19:34:29
Profile Name: Full Synchronization User Name: THEREBELADMIN\AAD_83654358a651
Step Type: Full Synchronization
Start Time: 26/04/2017 19:34:36
Partition: DC=therebeladmin,DC=com
End Time: 26/04/2017 19:34:44
Status: success
Export Statistics
Inbound Synchronization
Projections 259
Joins 0
Filtered Disconnectors 0
Disconnectors 174
Connectors with Flow Updates 259
Connectors without Flow Updates 0
Filtered Connectors 0
Deleted Connectors 0
Metaverse Object Deletes 0
Flow Errors
6 run(s)

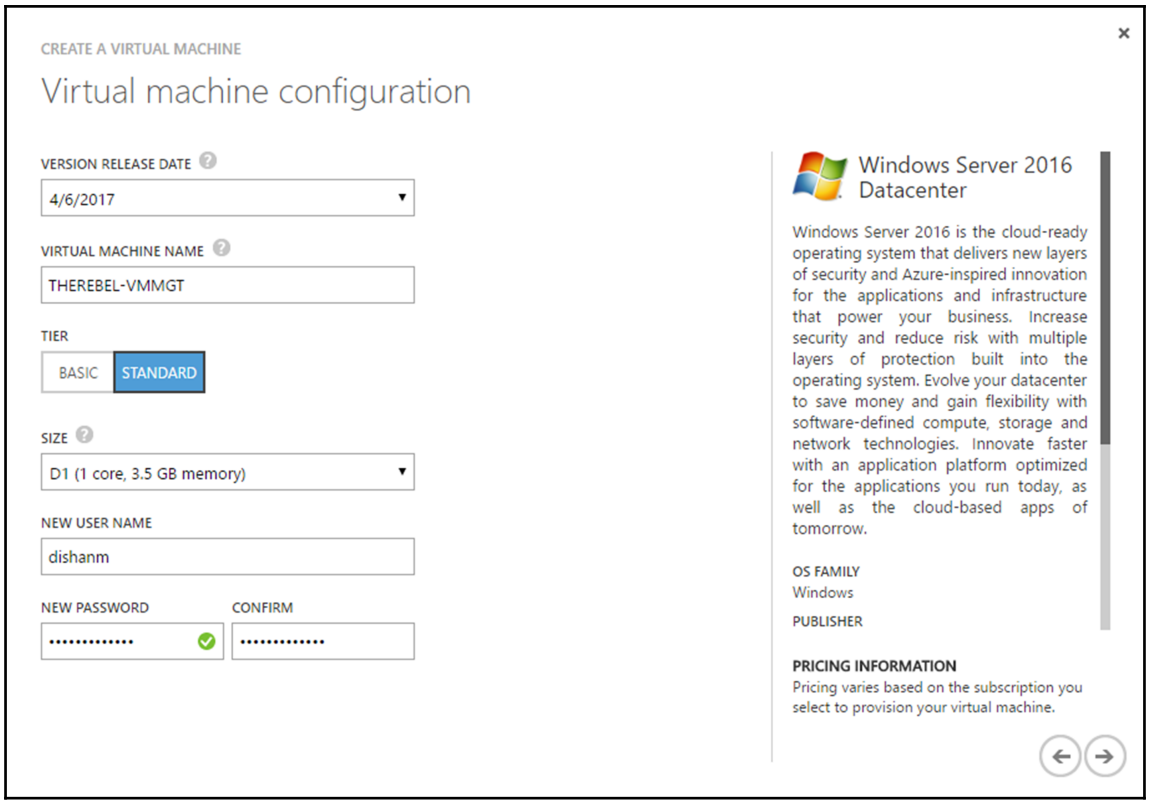

therebeladmin corp.
USERS
GROUPS
APPLICATIONS
DOMAINS
DIRECTORY INTEGRATION
CONFIGURE
REPORTS
LICENSES
DISPLAY NAME
USER NAME
SOURCED FROM
Adelinde Friedrichs
R540328@therebeladmin.com
Local Active Directory
Adolfa Leis
R578843@therebeladmin.com
Local Active Directory
Albrecht Rohde
R875546@therebeladmin.com
Local Active Directory
Alla Siegel
R799551@therebeladmin.com
Local Active Directory
Altfried Neuberger
R750269@therebeladmin.com
Local Active Directory
Annalene Jentzsch
R564441@therebeladmin.com
Local Active Directory
Anneheide Emmert
R297120@therebeladmin.com
Local Active Directory
Annelen Hug
R257650@therebeladmin.com
Local Active Directory
Annelene Tillmann
R128882@therebeladmin.com
Local Active Directory
Anneliese Mühlbauer
R680404@therebeladmin.com
Local Active Directory
Annetrud Nguyen
R324026@therebeladmin.com
Local Active Directory
Anny Grewe
R713468@therebeladmin.com
Local Active Directory
Arnold Ziegler
R935513@therebeladmin.com
Local Active Directory
Arwid Saathoff
R633705@therebeladmin.com
Local Active Directory
Benedicta Leis
R394073@therebeladmin.com
Local Active Directory

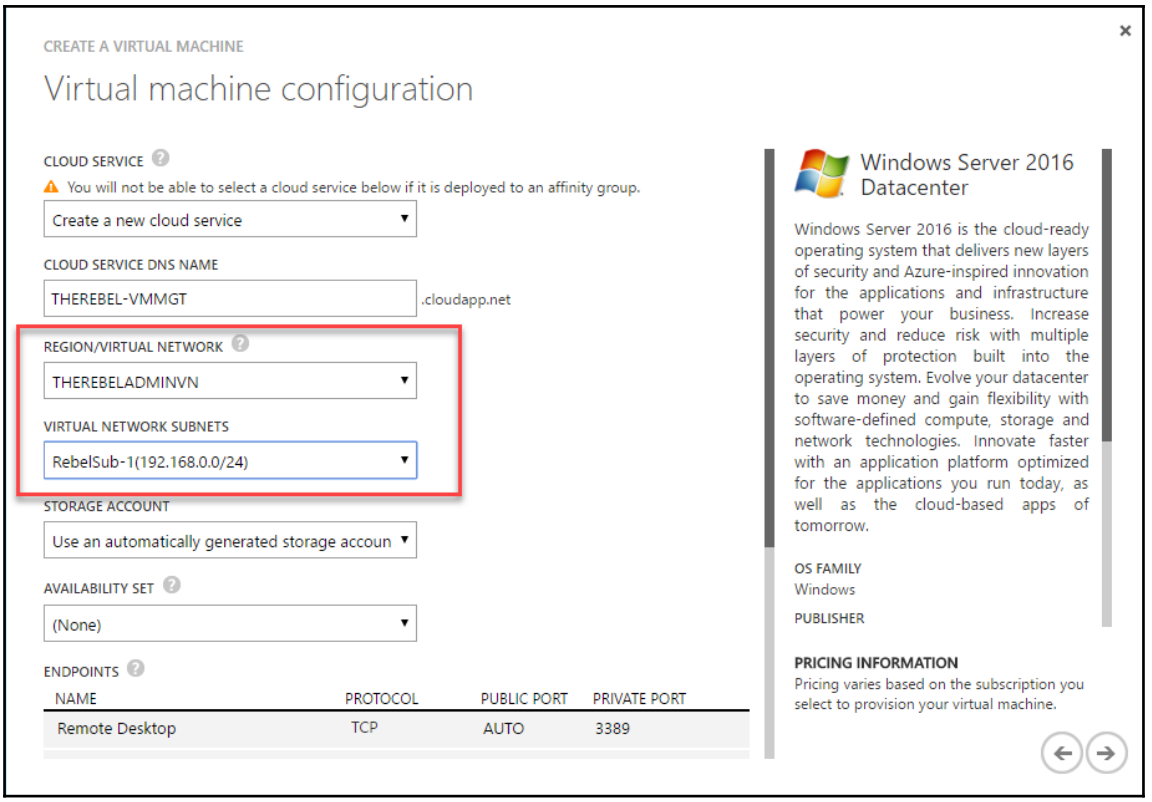

domain services
ENABLE DOMAIN SERVICES FOR THIS DIRECTORY
YES
NO
Users will not be able to login to the domain using their credentials until you enable password synchronization.

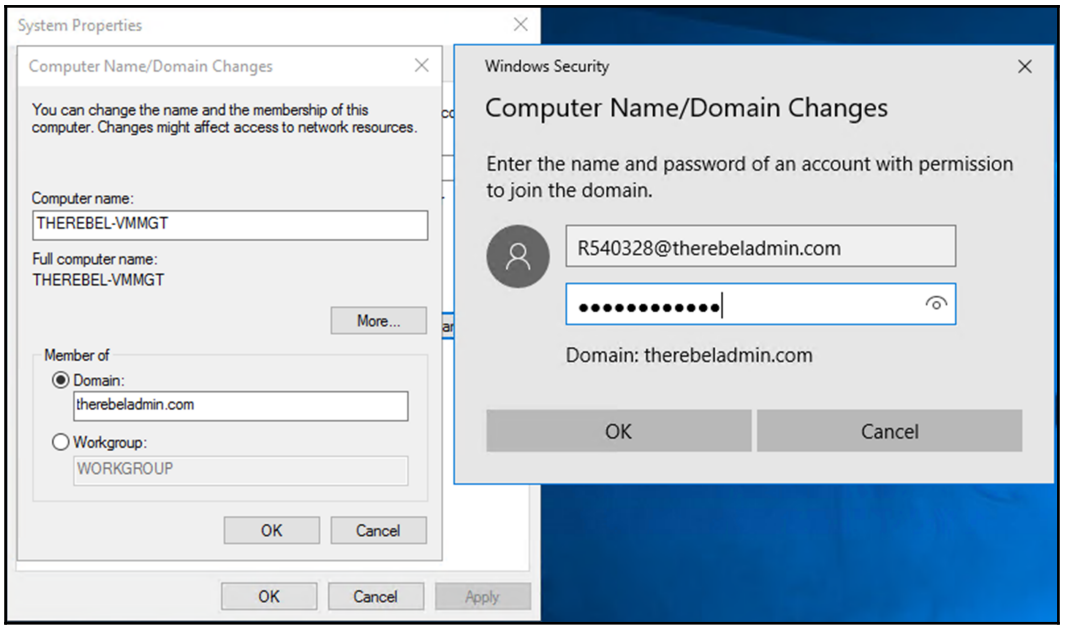

Microsoft Azure Active Directory Connect
Welcome
Tasks
Review your solution
Azure Active Directory
AZURE DIRECTORY ID
{e254f1cd-2e23-4b1d-b541-69c20e9923c3}
Synchronized Directories
DIRECTORY
therebeladmin.com
ACCOUNT
THEREBELADMIN.COM\MSOL_83654358a651
Synchronization Settings
SOURCE ANCHOR
objectGUID
USER PRINCIPAL NAME
userPrincipalName
SYNC CRITERIA
AlwaysProvision
FILTER OBJECTS TO SYNCHRONIZE BY GROUP
Disabled
AZURE AD APP AND ATTRIBUTE FILTERING
Disabled
DEVICE WRITEBACK
Disabled
DIRECTORY EXTENSION ATTRIBUTE SYNC
Disabled
EXCHANGE HYBRID DEPLOYMENT
Disabled
GROUP WRITEBACK
Disabled
PASSWORD SYNCHRONIZATION
Enabled
PASSWORD WRITEBACK
Disabled
USER WRITEBACK
Disabled
AUTO UPGRADE
Previous
Exit

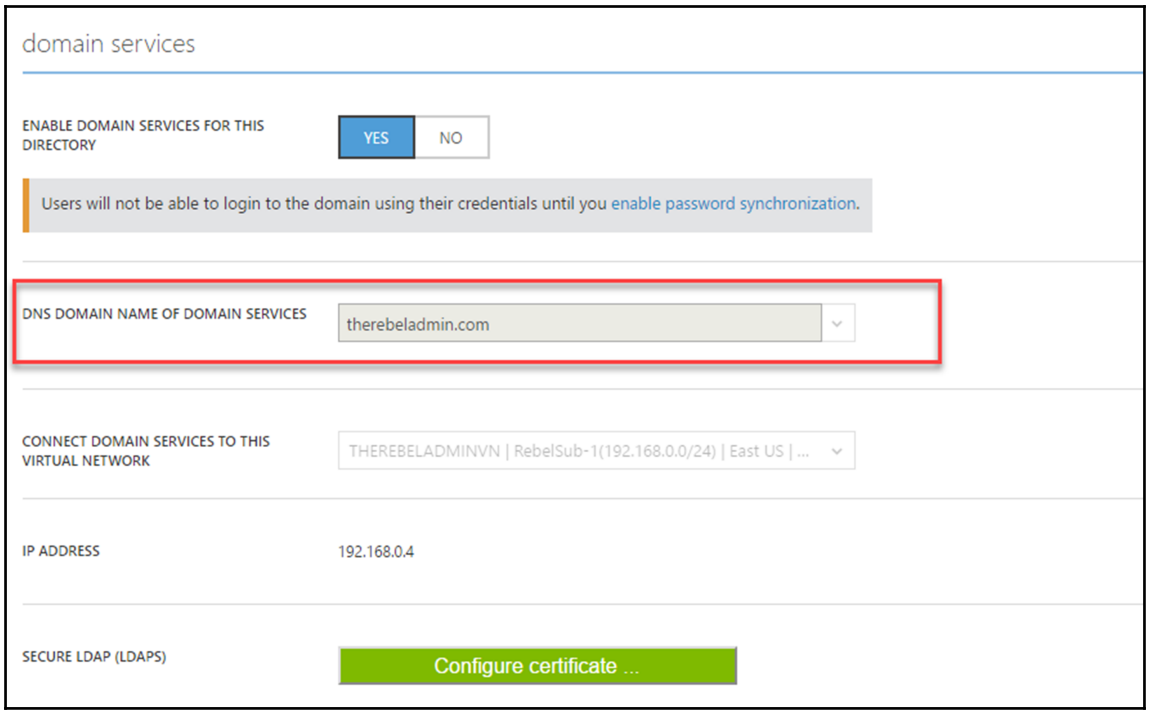

Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Domain/OU Filtering
Optional Features
Configure
Optional features
Select enhanced functionality if required by your organization.
Exchange hybrid deployment
Azure AD app and attribute filtering
Password synchronization
Password writeback
Group writeback (Preview)
Device writeback
Directory extension attribute sync
Learn more about optional features.
Previous
Next

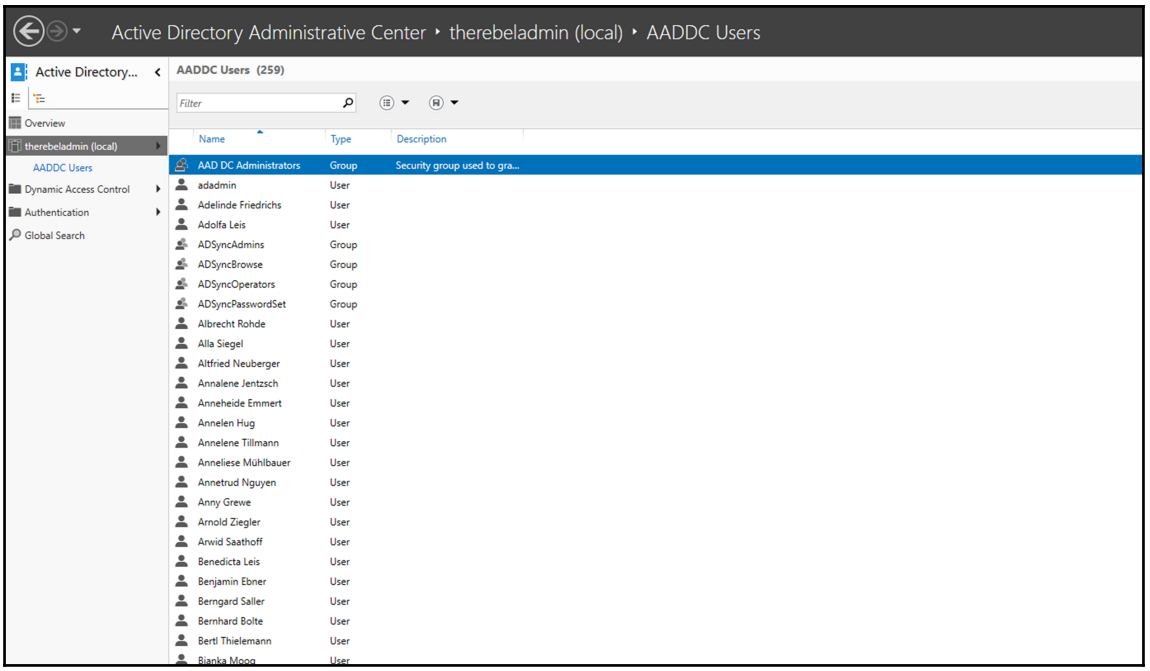

Synchronization Service Manager on REBELNET-PDC01
File Tools Actions Help
Operations
Connectors
Metaverse Designer
Metaverse Search
Connectors
Name
Type
Description
myrebeladmin.onmicrosoft.com - AAD
Windows Azure Active Directory (Microsoft)
therebeladmin.com
Active Directory Domain Services


CREATE A VIRTUAL MACHINE
Virtual machine configuration
VERSION RELEASE DATE
4/6/2017
VIRTUAL MACHINE NAME
THEREBEL-VMMGT
TIER
BASIC
STANDARD
SIZE
D1 (1 core, 3.5 GB memory)
NEW USER NAME
dishanm
NEW PASSWORD
CONFIRM
Windows Server 2016 Datacenter
Windows Server 2016 is the cloud-ready operating system that delivers new layers of security and Azure-inspired innovation for the applications and infrastructure that power your business. Increase security and reduce risk with multiple layers of protection built into the operating system. Evolve your datacenter to save money and gain flexibility with software-defined compute, storage and network technologies. Innovate faster with an application platform optimized for the applications you run today, as well as the cloud-based apps of tomorrow.
OS FAMILY
Windows
PUBLISHER
PRICING INFORMATION
Pricing varies based on the subscription you select to provision your virtual machine.

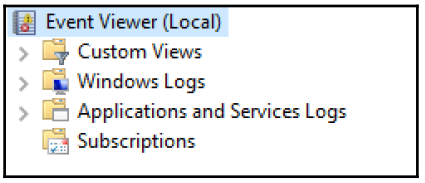

CREATE A VIRTUAL MACHINE
Virtual machine configuration
CLOUD SERVICE
You will not be able to select a cloud service below if it is deployed to an affinity group.
Create a new cloud service
CLOUD SERVICE DNS NAME
THEREBEL-VMMGT
.cloudapp.net
REGION/VIRTUAL NETWORK
THEREBELADMINVN
VIRTUAL NETWORK SUBNETS
RebelSub-1(192.168.0.0/24)
STORAGE ACCOUNT
Use an automatically generated storage accoun
AVAILABILITY SET
(None)
ENDPOINTS
NAME
PROTOCOL
PUBLIC PORT
PRIVATE PORT
Remote Desktop
TCP
AUTO
3389
Windows Server 2016 Datacenter
Windows Server 2016 is the cloud-ready operating system that delivers new layers of security and Azure-inspired innovation for the applications and infrastructure that power your business. Increase security and reduce risk with multiple layers of protection built into the operating system. Evolve your datacenter to save money and gain flexibility with software-defined compute, storage and network technologies. Innovate faster with an application platform optimized for the applications you run today, as well as the cloud-based apps of tomorrow.
OS FAMILY
Windows
PUBLISHER
PRICING INFORMATION
Pricing varies based on the subscription you select to provision your virtual machine.

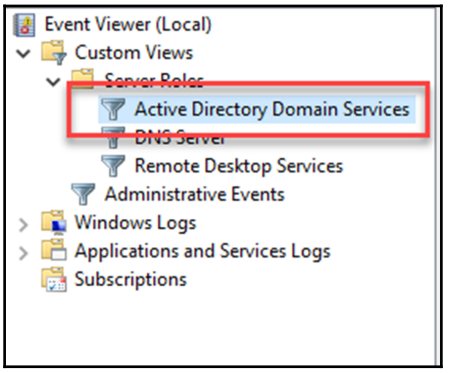

System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
THEREBEL-VMMGT
Full computer name:
THEREBEL-VMMGT
More...
Member of
Domain:
therebeladmin.com
Workgroup:
WORKGROUP
OK
Cancel
OK
Cancel
Apply
Windows Security
Computer Name/Domain Changes
Enter the name and password of an account with permission to join the domain.
R540328@therebeladmin.com
Domain: therebeladmin.com
OK
Cancel

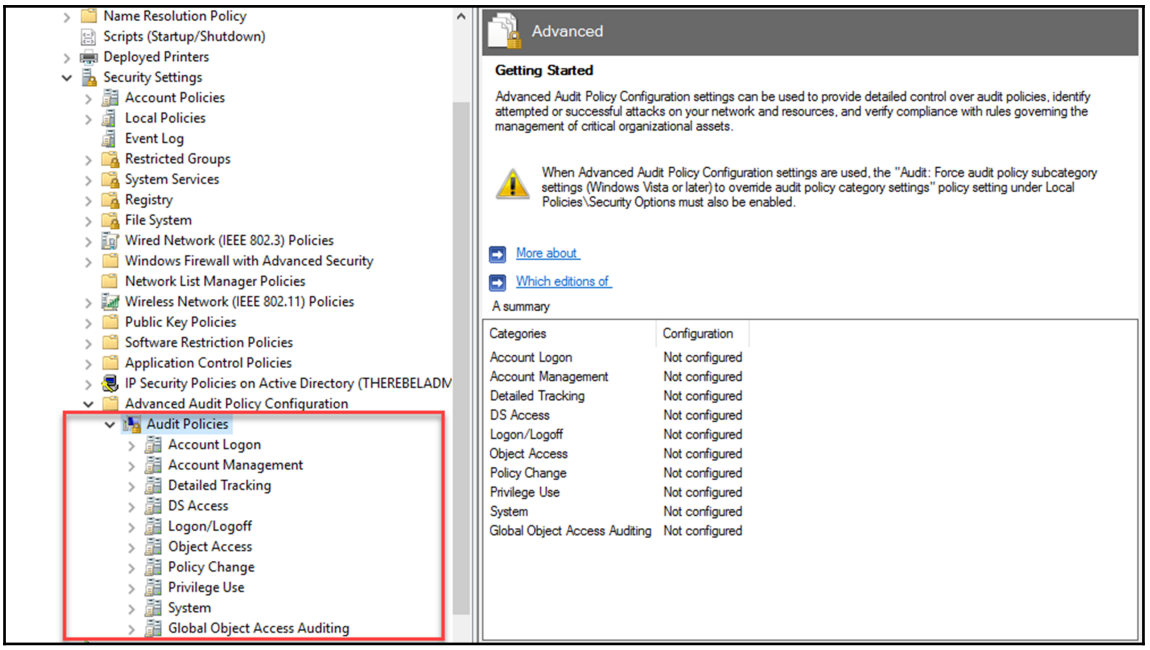

domain services
ENABLE DOMAIN SERVICES FOR THIS DIRECTORY
YES
NO
Users will not be able to login to the domain using their credentials until you enable password synchronization.
DNS DOMAIN NAME OF DOMAIN SERVICES
therebeladmin.com
CONNECT DOMAIN SERVICES TO THIS VIRTUAL NETWORK
THEREBELADMINVN | RebelSub-1(192.168.0.0/24) | East US | ...
IP ADDRESS
192.168.0.4
SECURE LDAP (LDAPS)
Configure certificate ...

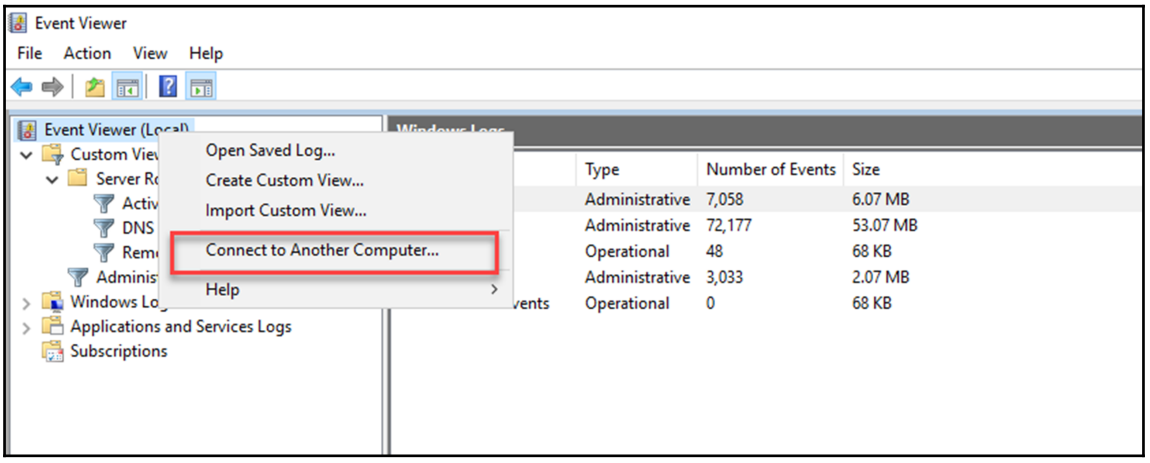

Active Directory Administrative Center ‣ therebeladmin (local) ‣ AADDC Users
Active Directory...
Overview
therebeladmin (local)
AADDC Users
Dynamic Access Control
Authentication
Global Search
AADDC Users (259)
Filter
Name
Type
Description
AAD DC Administrators Group Security group used to gra...
adadmin User
Adelinde Friedrichs User
Adolfa Leis User
ADSyncAdmins Group
ADSyncBrowse Group
ADSyncOperators Group
ADSyncPasswordSet Group
Albrecht Rohde User
Alla Siegel User
Altfried Neuberger User
Annalene Jentzsch User
Anneheide Emmert User
Annelen Hug User
Annelene Tillmann User
Anneliese Mühlbauer User
Annetrud Nguyen User
Anny Grewe User
Arnold Ziegler User
Arwid Saathoff User
Benedicta Leis User
Benjamin Ebner User
Berngard Saller User
Bernhard Bolte User
Bertl Thielemann User
Bianka Mogg User

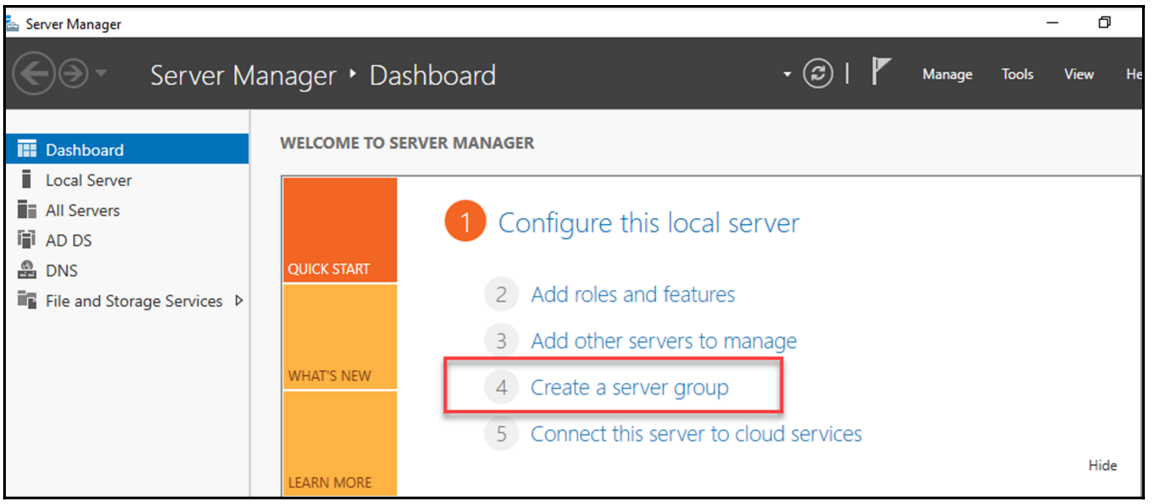
Chapter 18: Active Directory Audit and Monitoring

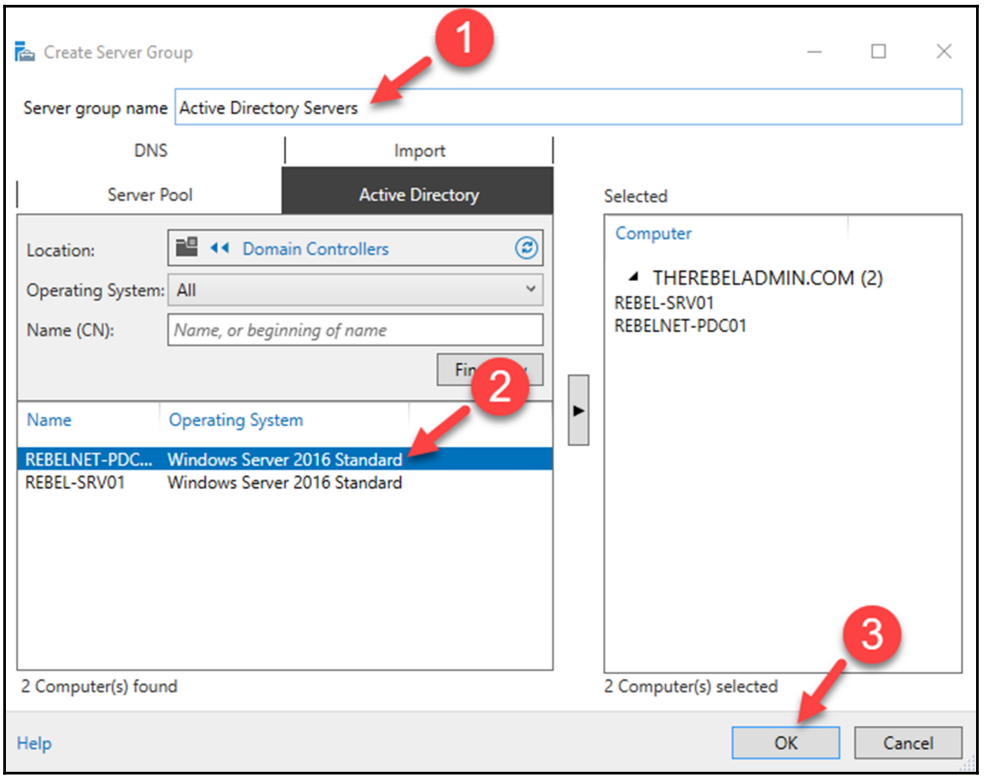


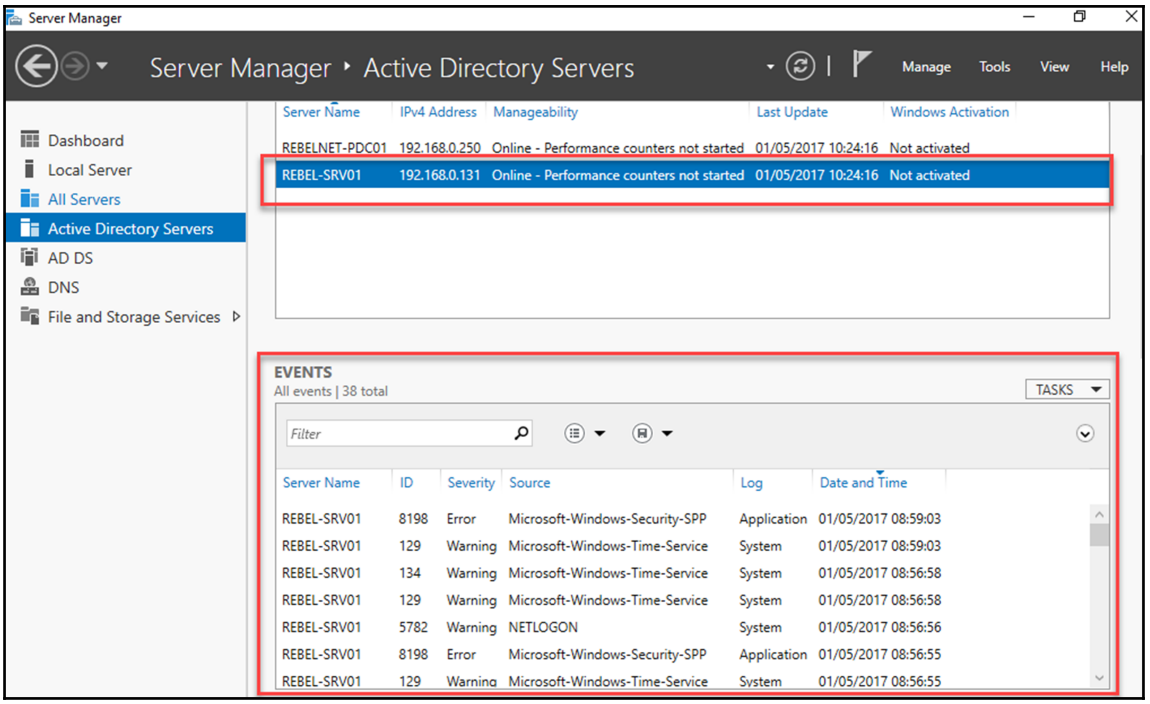


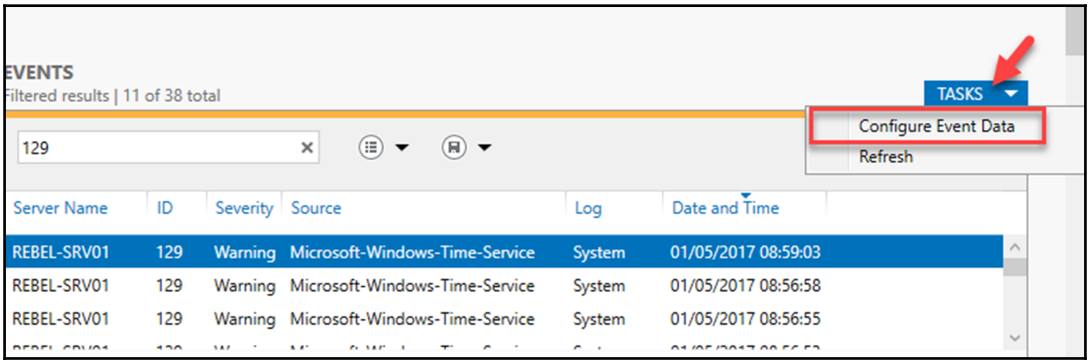

Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (THEREBELADM
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Advanced
Getting Started
Advanced Audit Policy Configuration settings can be used to provide detailed control over audit policies, identify attempted or successful attacks on your network and resources, and verify compliance with rules governing the management of critical organizational assets.
When Advanced Audit Policy Configuration settings are used, the "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" policy setting under Local Policies\Security Options must also be enabled.
More about
Which editions of
A summary
Categories
Configuration
Account Logon
Not configured
Account Management
Not configured
Detailed Tracking
Not configured
DS Access
Not configured
Logon/Logoff
Not configured
Object Access
Not configured
Policy Change
Not configured
Privilege Use
Not configured
System
Not configured
Global Object Access Auditing
Not configured

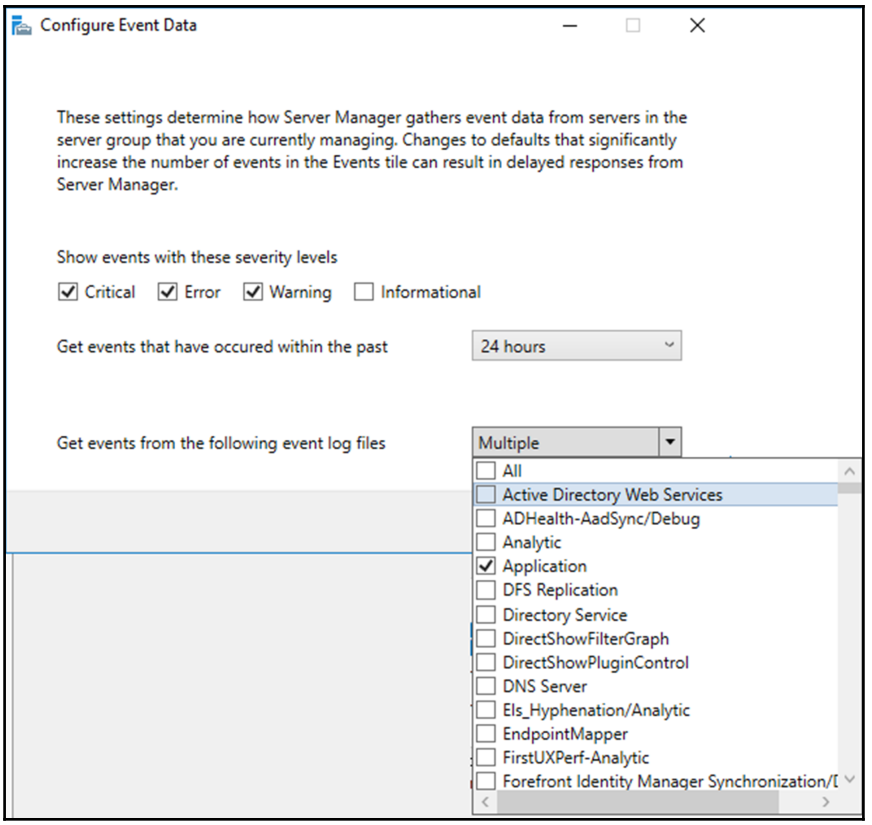

Event Viewer
File
Action
View
Help
Event Viewer (Local)
Custom Vie
Server Ro
Activ
DNS
Remo
Adminis
Windows Lo
Applications and Services Logs
Subscriptions
Open Saved Log...
Create Custom View...
Import Custom View...
Connect to Another Computer...
Help
Type
Number of Events
Size
Administrative
7,058
6.07 MB
Administrative
72,177
53.07 MB
Operational
48
68 KB
Administrative
3,033
2.07 MB
Operational
0
68 KB

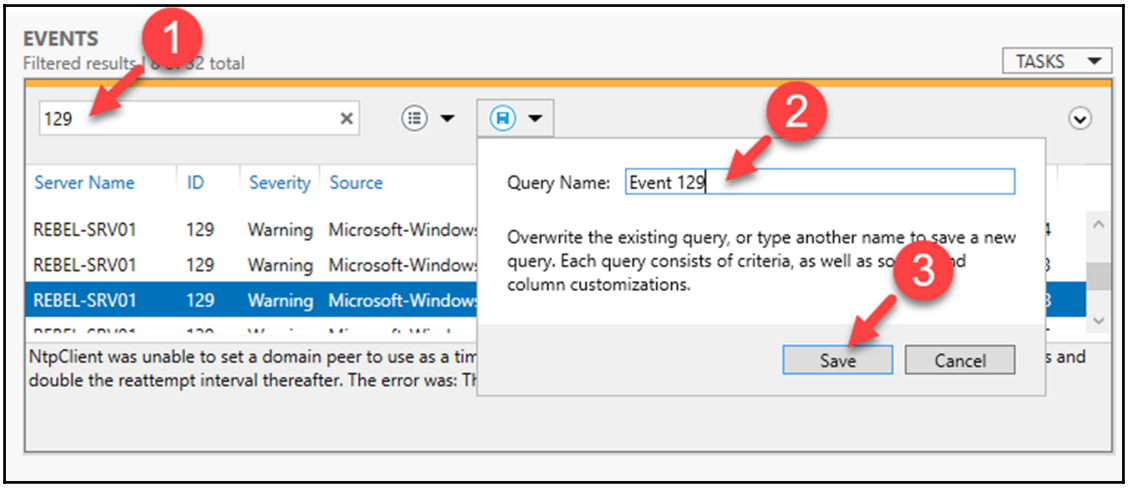

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide

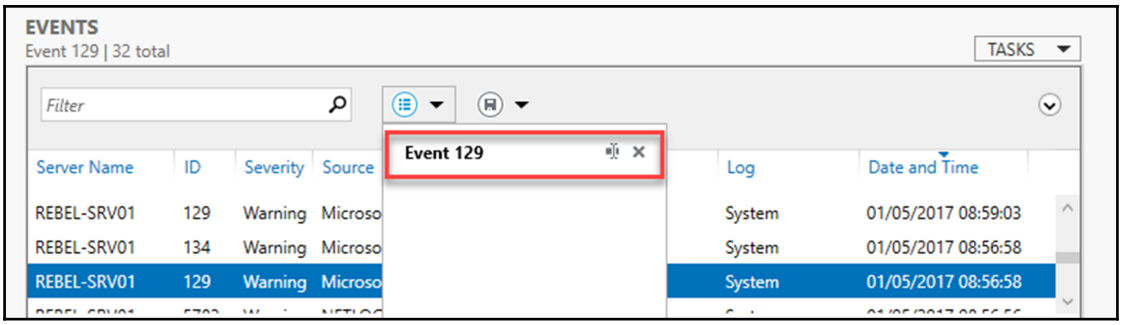

Create Server Group
1
Server group name
Active Directory Servers
DNS
Import
Server Pool
Active Directory
Location:
Domain Controllers
Operating System:
All
Name (CN):
Name, or beginning of name
Name
Operating System
REBELNET-PDC...
Windows Server 2016 Standard
REBEL-SRV01
Windows Server 2016 Standard
2
2 Computer(s) found
Selected
Computer
THEREBELADMIN.COM (2)
REBEL-SRV01
REBELNET-PDC01
3
2 Computer(s) selected
Help
OK
Cancel

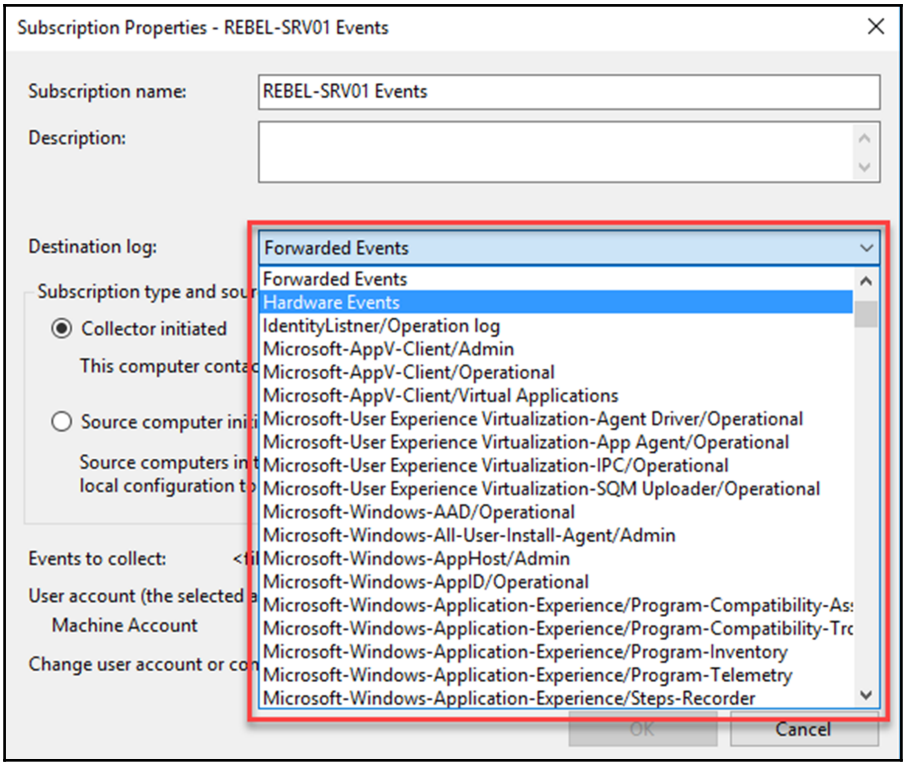

Server Manager
Server Manager ‣ Active Directory Servers
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
Active Directory Servers
AD DS
DNS
File and Storage Services
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
REBELNET-PDC01 192.168.0.250 Online - Performance counters not started 01/05/2017 10:24:16 Not activated
REBEL-SRV01 192.168.0.131 Online - Performance counters not started 01/05/2017 10:24:16 Not activated
EVENTS
All events | 38 total
TASKS
Filter
Server Name ID Severity Source Log Date and Time
REBEL-SRV01 8198 Error Microsoft-Windows-Security-SPP Application 01/05/2017 08:59:03
REBEL-SRV01 129 Warning Microsoft-Windows-Time-Service System 01/05/2017 08:59:03
REBEL-SRV01 134 Warning Microsoft-Windows-Time-Service System 01/05/2017 08:56:58
REBEL-SRV01 129 Warning Microsoft-Windows-Time-Service System 01/05/2017 08:56:58
REBEL-SRV01 5782 Warning NETLOGON System 01/05/2017 08:56:56
REBEL-SRV01 8198 Error Microsoft-Windows-Security-SPP Application 01/05/2017 08:56:55
REBEL-SRV01 129 Warning Microsoft-Windows-Time-Service System 01/05/2017 08:56:55

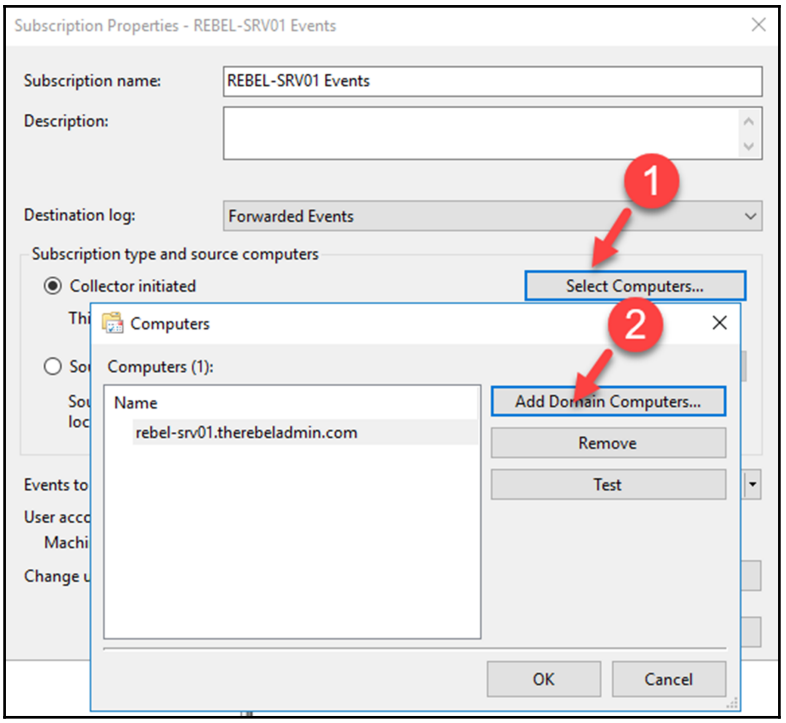

EVENTS
Filtered results | 11 of 38 total
TASKS
Configure Event Data
Refresh
129
Server Name ID Severity Source Log Date and Time
REBEL-SRV01 129 Warning Microsoft-Windows-Time-Service System 01/05/2017 08:59:03
REBEL-SRV01 129 Warning Microsoft-Windows-Time-Service System 01/05/2017 08:56:58
REBEL-SRV01 129 Warning Microsoft-Windows-Time-Service System 01/05/2017 08:56:55

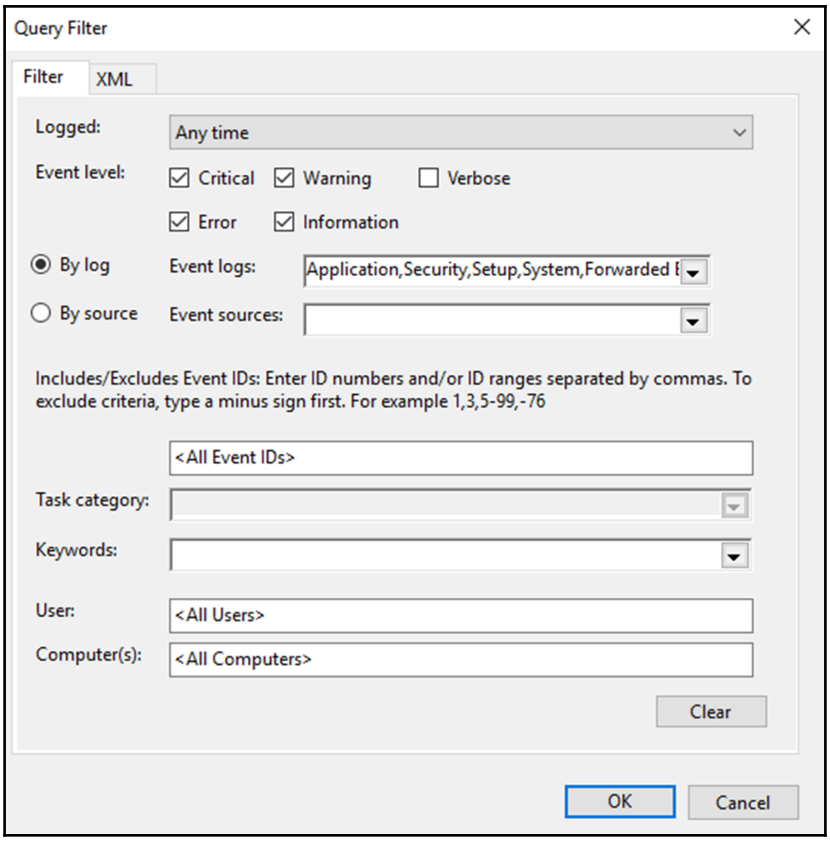

Configure Event Data
These settings determine how Server Manager gathers event data from servers in the server group that you are currently managing. Changes to defaults that significantly increase the number of events in the Events tile can result in delayed responses from Server Manager.
Show events with these severity levels
Critical
Error
Warning
Informational
Get events that have occured within the past
24 hours
Get events from the following event log files
Multiple
All
Active Directory Web Services
ADHealth-AadSync/Debug
Analytic
Application
DFS Replication
Directory Service
DirectShowFilterGraph
DirectShowPluginControl
DNS Server
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
Forefront Identity Manager Synchronization/I

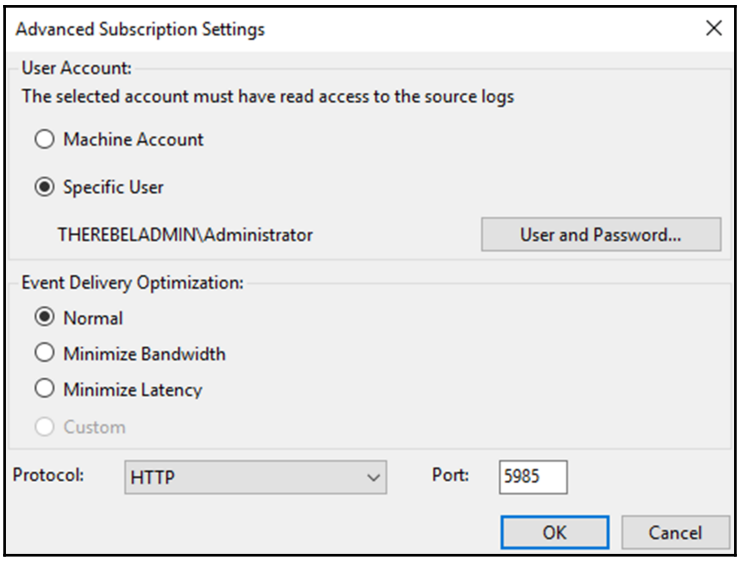

EVENTS
TASKS
1
129
2
Server Name
ID
Severity
Source
REBEL-SRV01
129
Warning
Microsoft-Windows
Query Name:
Event 129
Overwrite the existing query, or type another name to save a new query. Each query consists of criteria, as well as so
column customizations.
3
Save
Cancel
NtpClient was unable to set a domain peer to use as a tim
double the reattempt interval thereafter. The error was: Th

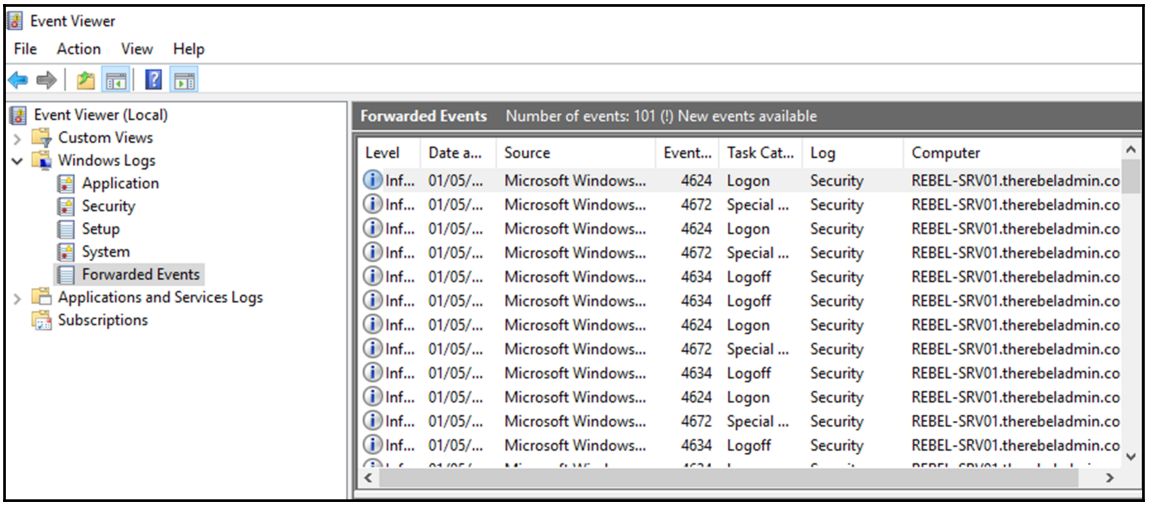

EVENTS
Event 129 | 32 total
TASKS
Filter
Event 129
Server Name
ID
Severity
Source
Log
Date and Time
REBEL-SRV01 129 Warning Microso System 01/05/2017 08:59:03
REBEL-SRV01 134 Warning Microso System 01/05/2017 08:56:58
REBEL-SRV01 129 Warning Microso System 01/05/2017 08:56:58

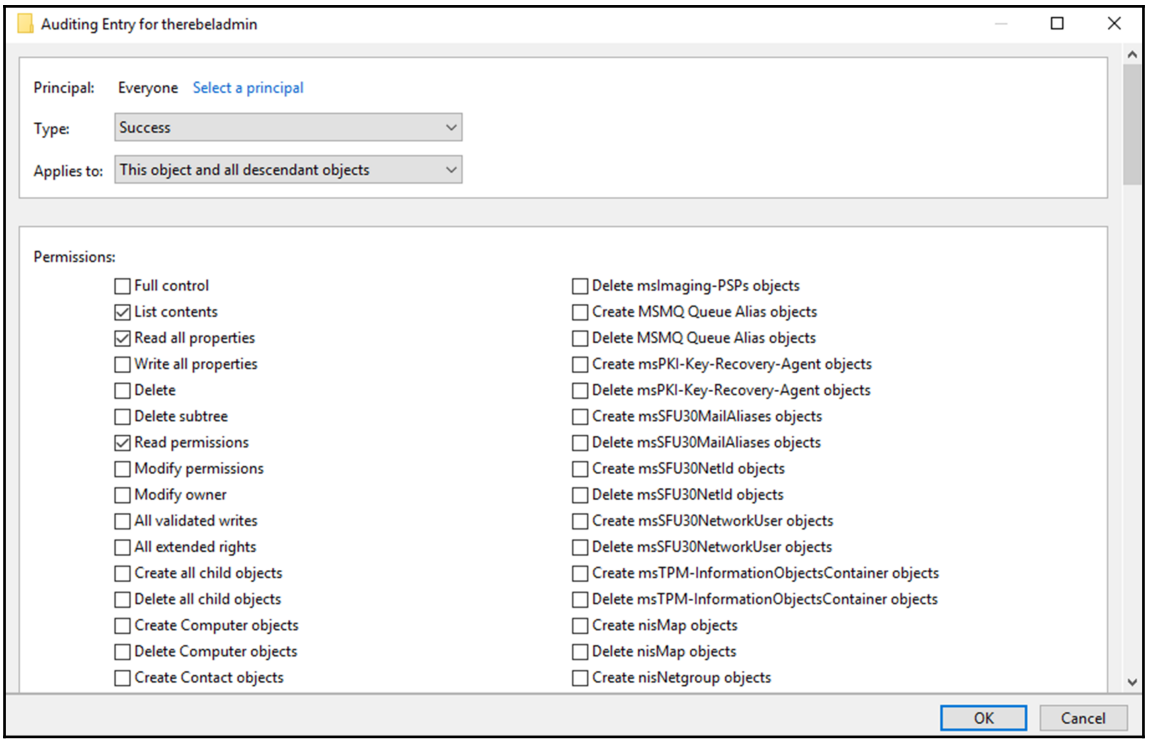

Subscription Properties - REBEL-SRV01 Events
Subscription name:
REBEL-SRV01 Events
Description:
Destination log:
Forwarded Events
Forwarded Events
Hardware Events
IdentityListner/Operation log
Microsoft-AppV-Client/Admin
Microsoft-AppV-Client/Operational
Microsoft-AppV-Client/Virtual Applications
Microsoft-User Experience Virtualization-Agent Driver/Operational
Microsoft-User Experience Virtualization-App Agent/Operational
Microsoft-User Experience Virtualization-IPC/Operational
Microsoft-User Experience Virtualization-SQM Uploader/Operational
Microsoft-Windows-AAD/Operational
Microsoft-Windows-All-User-Install-Agent/Admin
Microsoft-Windows-AppHost/Admin
Microsoft-Windows-AppID/Operational
Microsoft-Windows-Application-Experience/Program-Compatibility-As
Microsoft-Windows-Application-Experience/Program-Compatibility-Tr
Microsoft-Windows-Application-Experience/Program-Inventory
Microsoft-Windows-Application-Experience/Program-Telemetry
Microsoft-Windows-Application-Experience/Steps-Recorder
Subscription type and sou
Collector initiated
This computer conta
Source computer ini
Source computers in t
local configuration t
Events to collect:
User account (the selected
Machine Account
Change user account or co
OK
Cancel

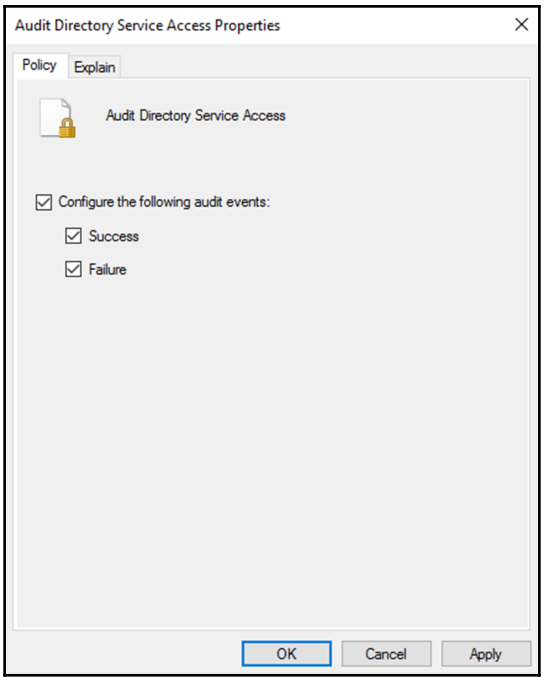

Subscription Properties - REBEL-SRV01 Events
Subscription name:
REBEL-SRV01 Events
Description:
Destination log:
Forwarded Events
Subscription type and source computers
Collector initiated
Select Computers...
1
2
Computers
Computers (1):
Name
rebel-srv01.therebeladmin.com
Add Domain Computers...
Remove
Test
OK
Cancel

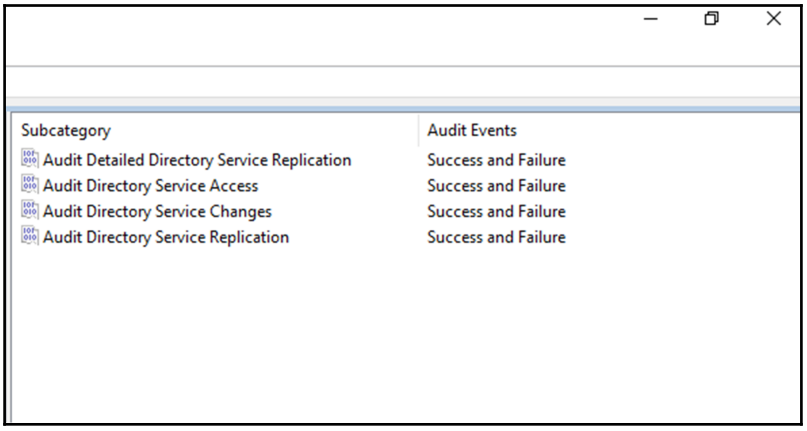

Query Filter
Filter
XML
Logged:
Any time
Event level:
Critical
Warning
Verbose
Error
Information
By log
Event logs:
Application,Security,Setup,System,Forwarded E
By source
Event sources:
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
<All Event IDs>
Task category:
Keywords:
User:
<All Users>
Computer(s):
<All Computers>
Clear
OK
Cancel


Advanced Subscription Settings
User Account:
The selected account must have read access to the source logs
Machine Account
Specific User
THEREBELADMIN\Administrator
User and Password...
Event Delivery Optimization:
Normal
Minimize Bandwidth
Minimize Latency
Custom
Protocol:
HTTP
Port:
5985
OK
Cancel


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Subscriptions
Forwarded Events
Number of events: 101 (!) New events available
Level Date a... Source Event... Task Cat... Log Computer
Inf... 01/05/... Microsoft Windows... 4624 Logon Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4672 Special ... Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4624 Logon Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4672 Special ... Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4634 Logoff Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4634 Logoff Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4624 Logon Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4672 Special ... Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4634 Logoff Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4624 Logon Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4672 Special ... Security REBEL-SRV01.therebeladmin.co
Inf... 01/05/... Microsoft Windows... 4634 Logoff Security REBEL-SRV01.therebeladmin.co


Auditing Entry for therebeladmin
Principal: Everyone Select a principal
Type: Success
Applies to: This object and all descendant objects
Permissions:
Full control
List contents
Read all properties
Write all properties
Delete
Delete subtree
Read permissions
Modify permissions
Modify owner
All validated writes
All extended rights
Create all child objects
Delete all child objects
Create Computer objects
Delete Computer objects
Create Contact objects
Delete msImaging-PSPs objects
Create MSMQ Queue Alias objects
Delete MSMQ Queue Alias objects
Create msPKI-Key-Recovery-Agent objects
Delete msPKI-Key-Recovery-Agent objects
Create msSFU30MailAliases objects
Delete msSFU30MailAliases objects
Create msSFU30NetId objects
Delete msSFU30NetId objects
Create msSFU30NetworkUser objects
Delete msSFU30NetworkUser objects
Create msTPM-InformationObjectsContainer objects
Delete msTPM-InformationObjectsContainer objects
Create nisMap objects
Delete nisMap objects
Create nisNetgroup objects
OK
Cancel


Audit Directory Service Access Properties
Policy
Explain
Audit Directory Service Access
Configure the following audit events:
Success
Failure
OK
Cancel
Apply


Subcategory
Audit Events
Audit Detailed Directory Service Replication
Success and Failure
Audit Directory Service Access
Success and Failure
Audit Directory Service Changes
Success and Failure
Audit Directory Service Replication
Success and Failure

```
PS C:\Users\Administrator> Get-EventLog -Newest 5 -LogName 'Directory Service' -ComputerName 'REBEL-SRV01' | fl -Propert
y *


EventID            : 1404
MachineName        : REBEL-SRV01.therebeladmin.com
Data               : {}
Index              : 79
Category           : Knowledge Consistency Checker
CategoryNumber     : 1
EntryType          : Information
Message            : This directory service is now the intersite topology generator and has assumed responsibility for
                     generating and maintaining intersite replication topologies for this site.
Source             : NTDS KCC
ReplacementStrings : {}
InstanceId         : 1073743228
TimeGenerated      : 02/05/2017 08:07:10
TimeWritten        : 02/05/2017 08:07:10
UserName           : NT AUTHORITY\ANONYMOUS LOGON
Site               :
Container          :

EventID            : 2405
MachineName        : REBEL-SRV01.therebeladmin.com
Data               : {}
Index              : 78
Category           : Internal Configuration
CategoryNumber     : 7
EntryType          : Information
Message            : This Active Directory Domain Services server does not support the "Recycle Bin Feature" optional
                     feature.
Source             : NTDS General
ReplacementStrings : {Recycle Bin Feature}
InstanceId         : 1073744229
TimeGenerated      : 02/05/2017 00:37:54
TimeWritten        : 02/05/2017 00:37:54
UserName           : NT AUTHORITY\ANONYMOUS LOGON
Site               :
Container          :
```

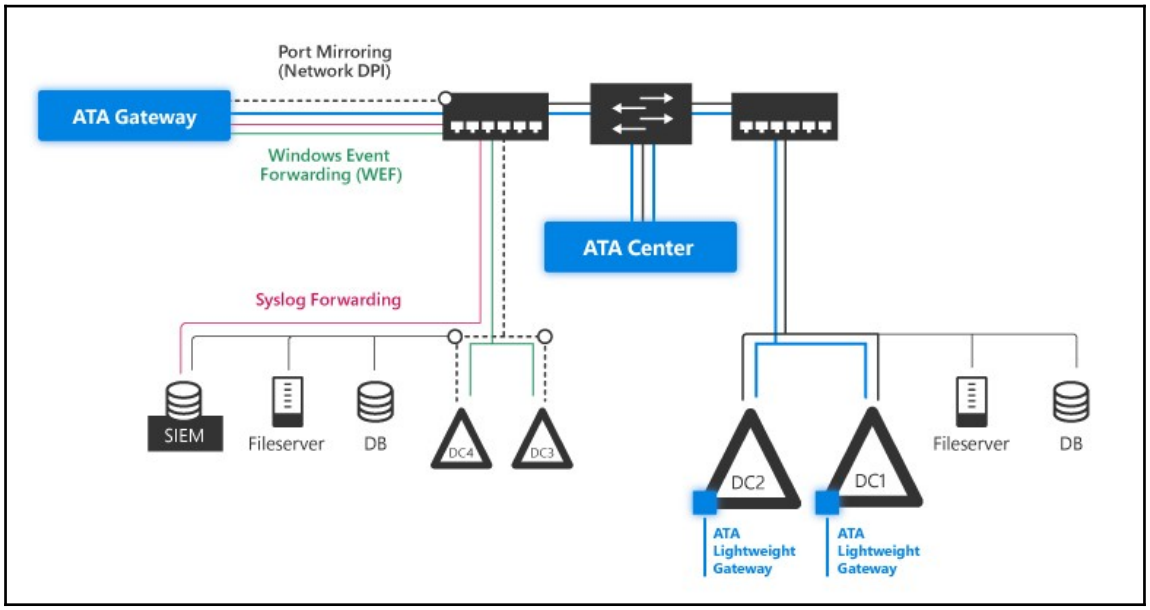
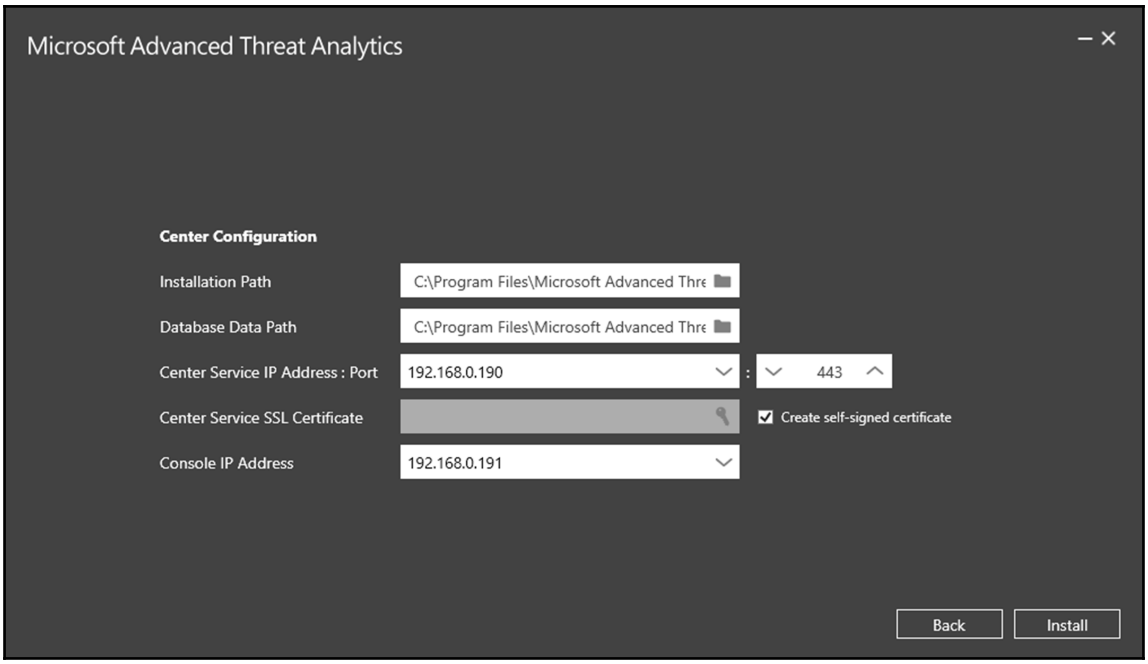
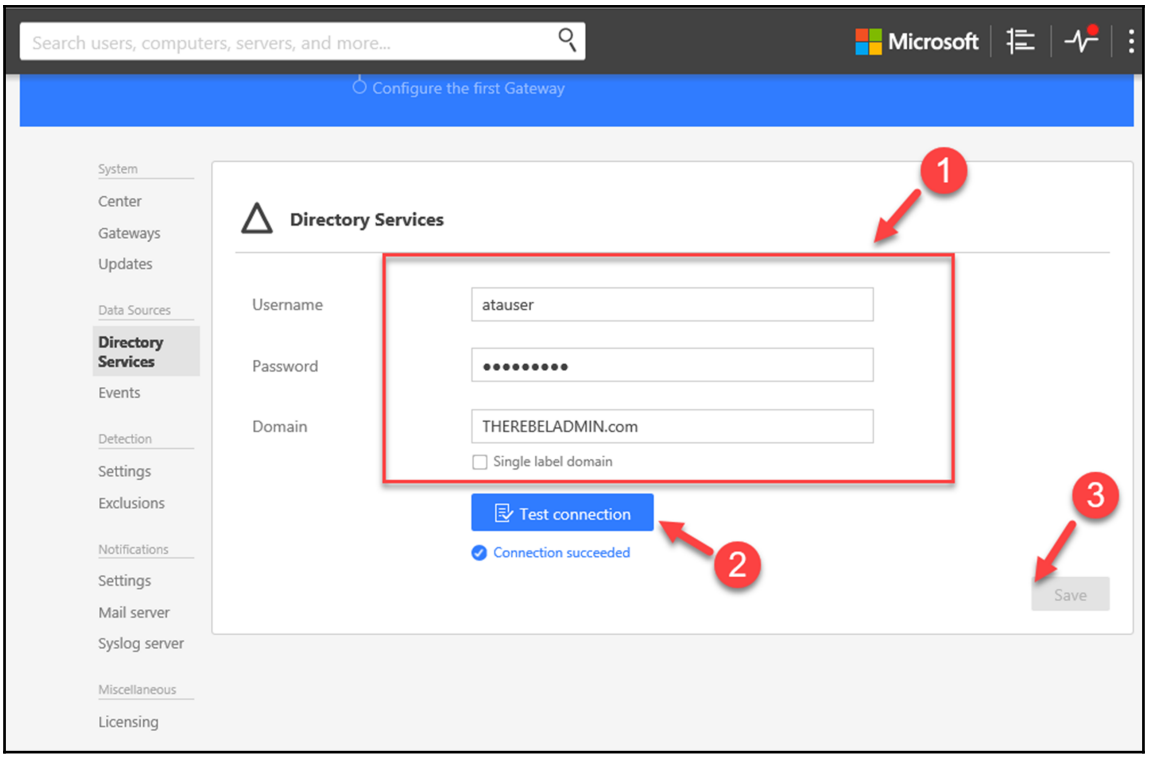
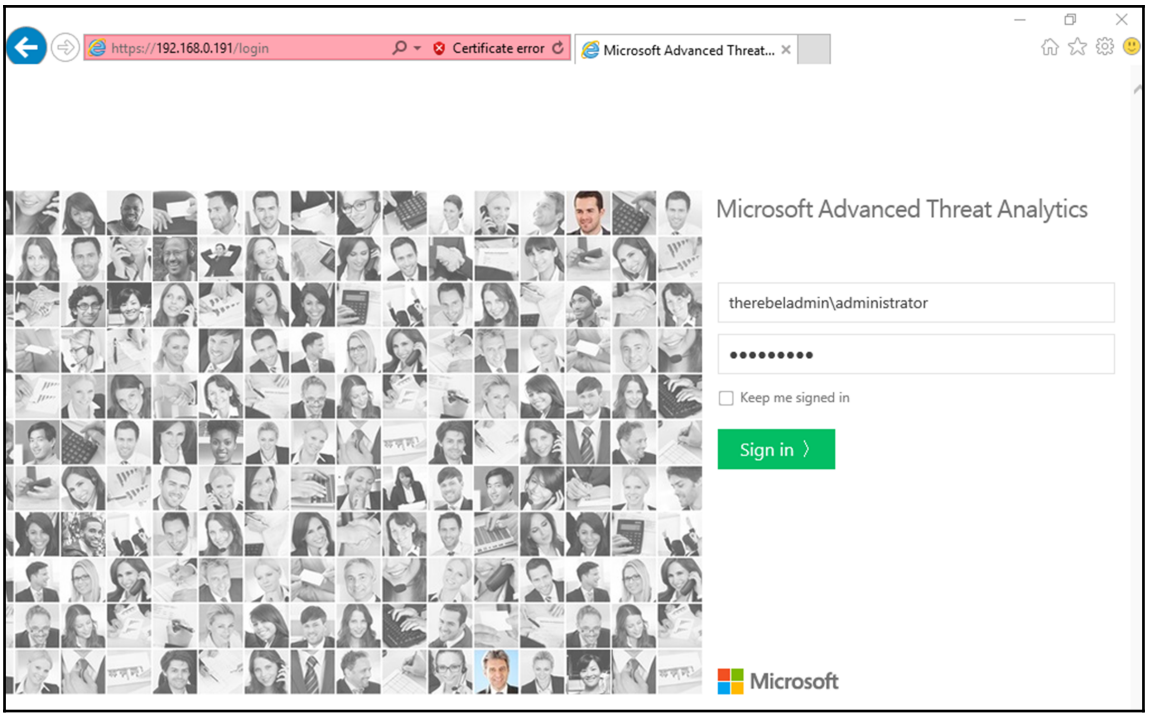
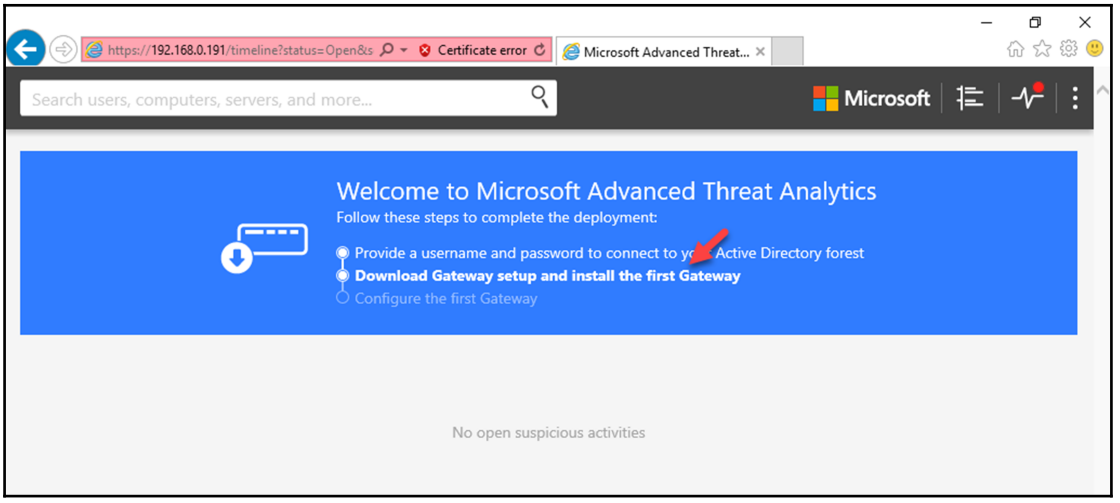


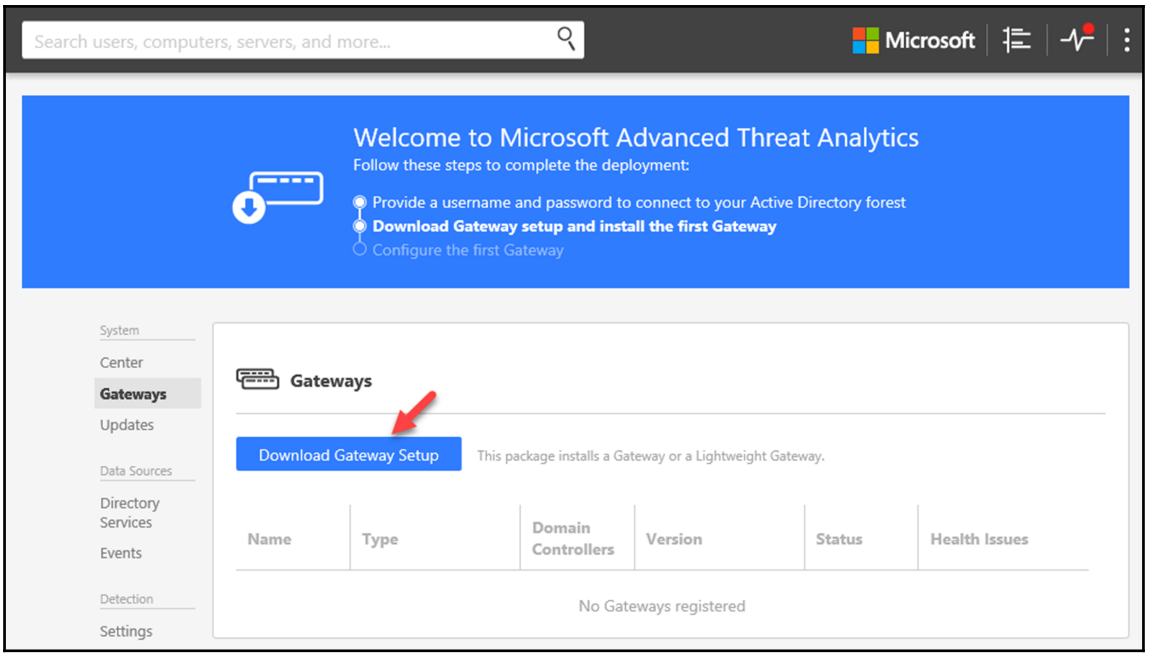
Image source: https://docs.microsoft.com/en-gb/advanced-threat-analytics/plan-design/media/ata-architecture-topology.jpg

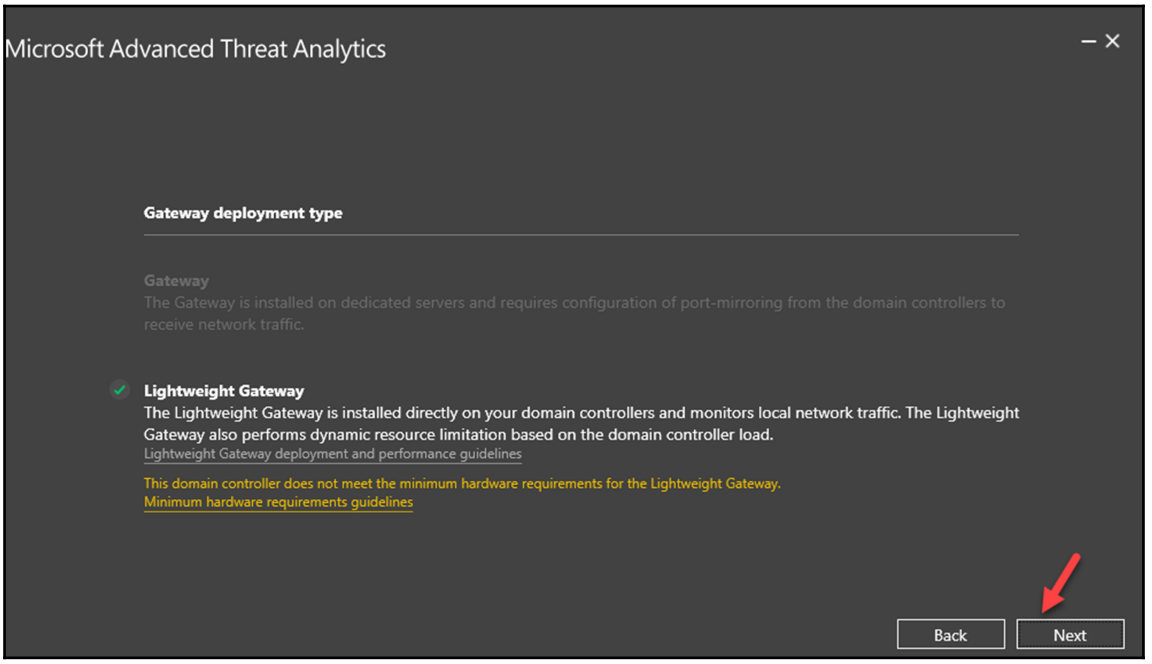

Microsoft Advanced Threat Analytics
Center Configuration
Installation Path
C:\Program Files\Microsoft Advanced Thre
Database Data Path
C:\Program Files\Microsoft Advanced Thre
Center Service IP Address : Port
192.168.0.190
443
Center Service SSL Certificate
Create self-signed certificate
Console IP Address
192.168.0.191
Back
Install

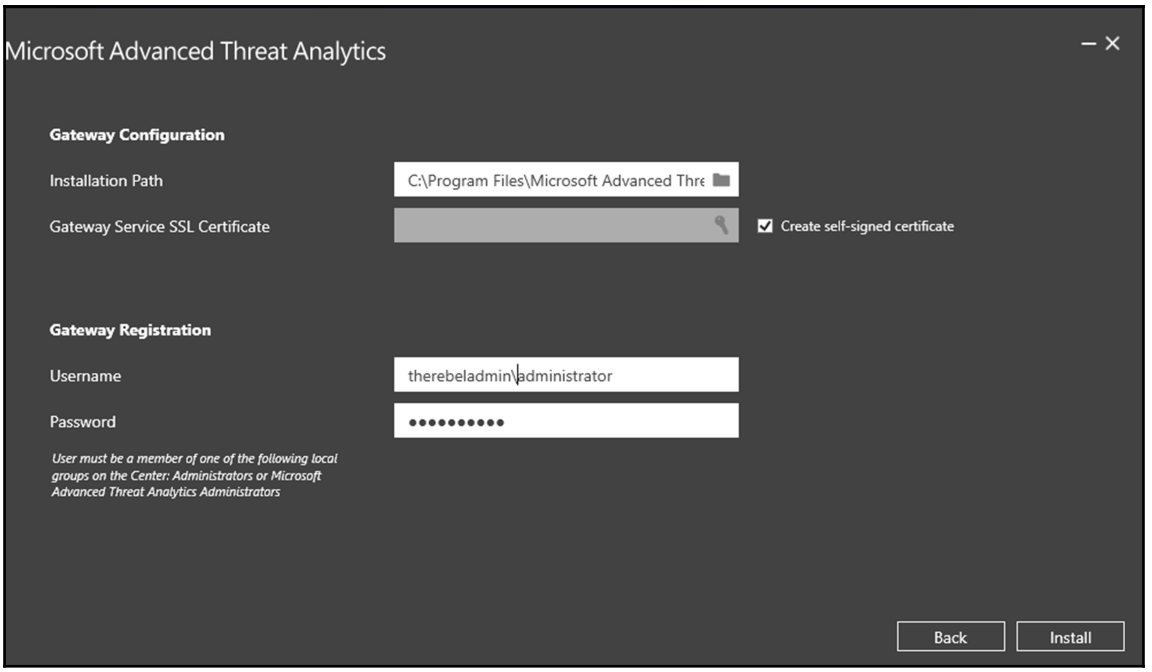

Search users, computers, servers, and more...
Microsoft
Configure the first Gateway
System
Center
Gateways
Updates
Data Sources
Directory Services
Events
Detection
Settings
Exclusions
Notifications
Settings
Mail server
Syslog server
Miscellaneous
Licensing
Directory Services
Username
atauser
Password
Domain
THEREBELADMIN.com
Single label domain
Test connection
Connection succeeded
Save
1
2
3

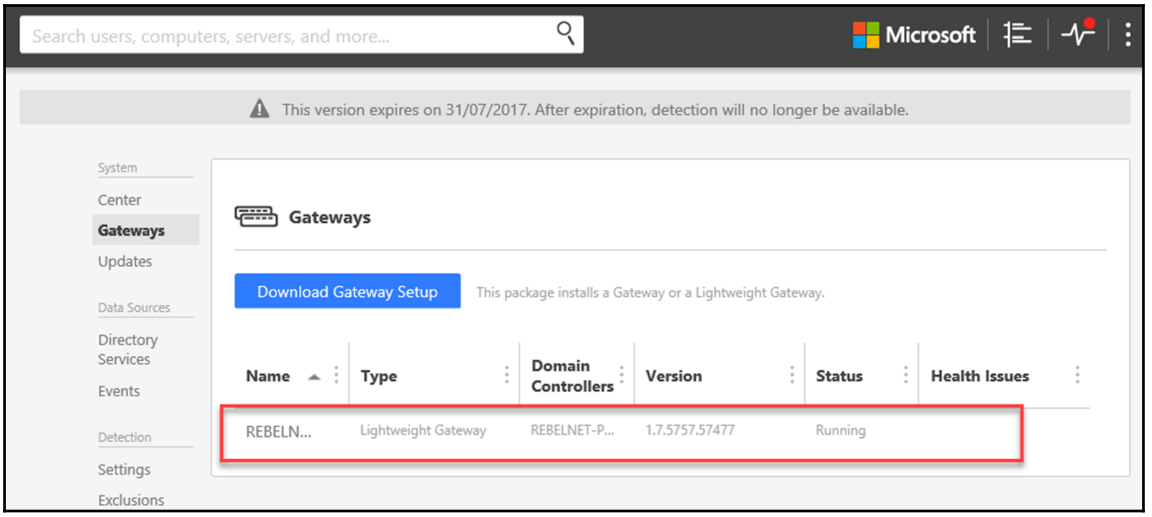

https://192.168.0.191/login
Certificate error
Microsoft Advanced Threat...
Microsoft Advanced Threat Analytics
therebeladmin\administrator
Keep me signed in
Sign in
Microsoft

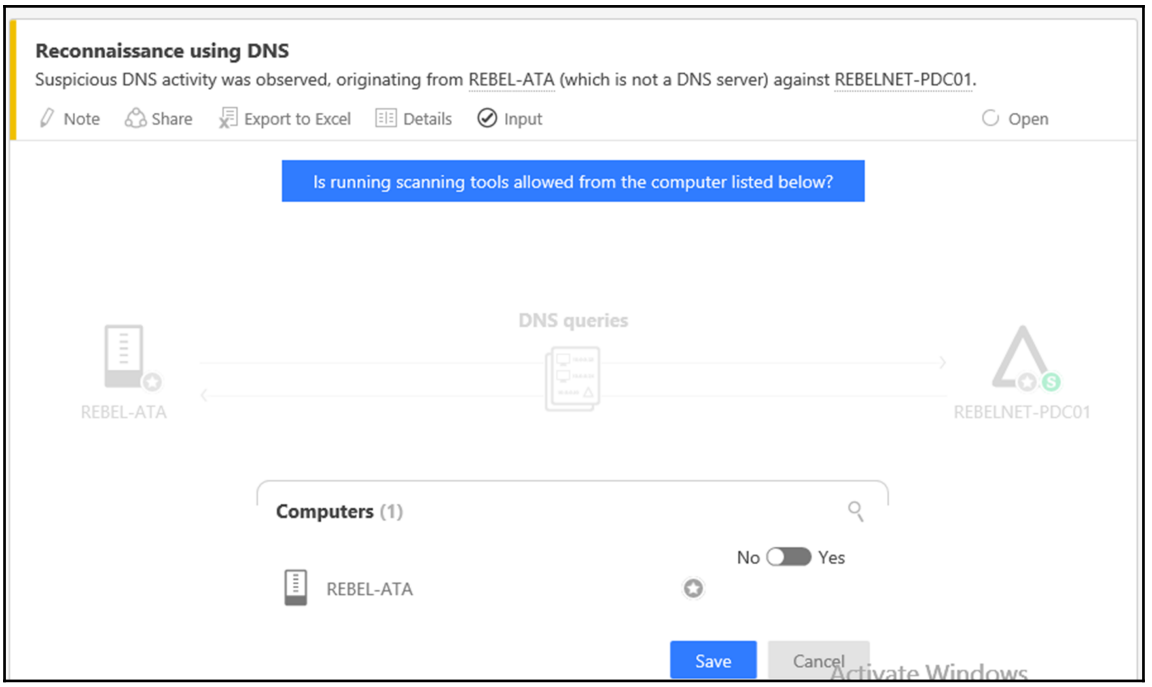

https://192.168.0.191/timeline?status=Open&s
Certificate error
Microsoft Advanced Threat...
Search users, computers, servers, and more...
Microsoft
Welcome to Microsoft Advanced Threat Analytics
Follow these steps to complete the deployment:
Provide a username and password to connect to y Active Directory forest
Download Gateway setup and install the first Gateway
Configure the first Gateway
No open suspicious activities

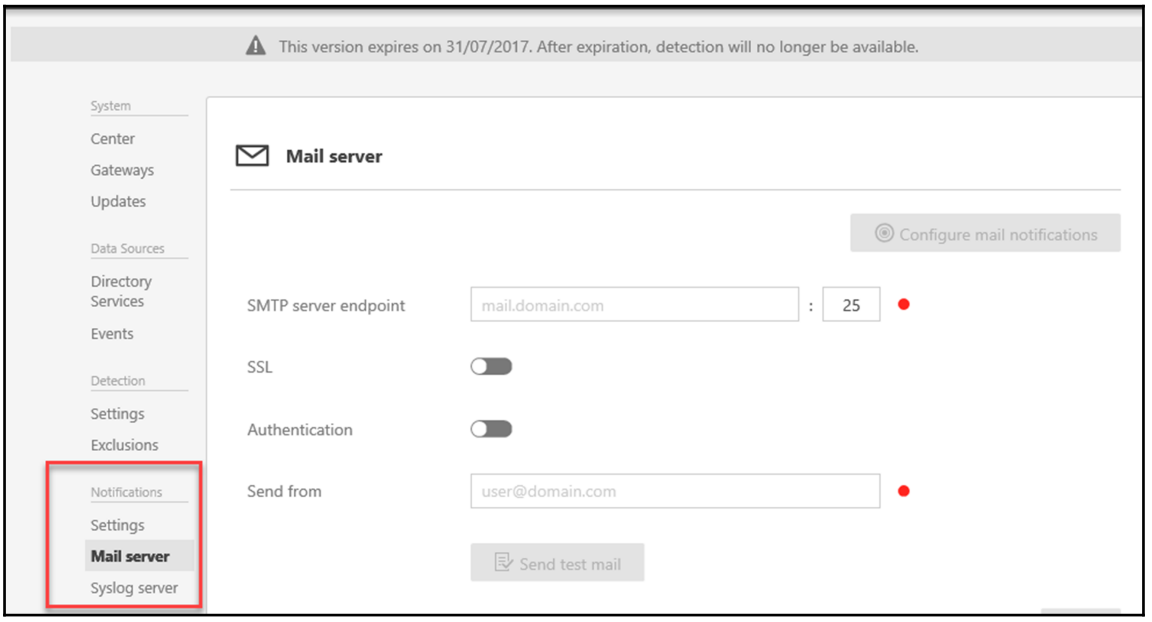

Search users, computers, servers, and more...
Microsoft
Welcome to Microsoft Advanced Threat Analytics
Follow these steps to complete the deployment:
Provide a username and password to connect to your Active Directory forest
Download Gateway setup and install the first Gateway
Configure the first Gateway
System
Center
Gateways
Updates
Data Sources
Directory Services
Events
Detection
Settings
Gateways
Download Gateway Setup
This package installs a Gateway or a Lightweight Gateway.
Name
Type
Domain Controllers
Version
Status
Health Issues
No Gateways registered

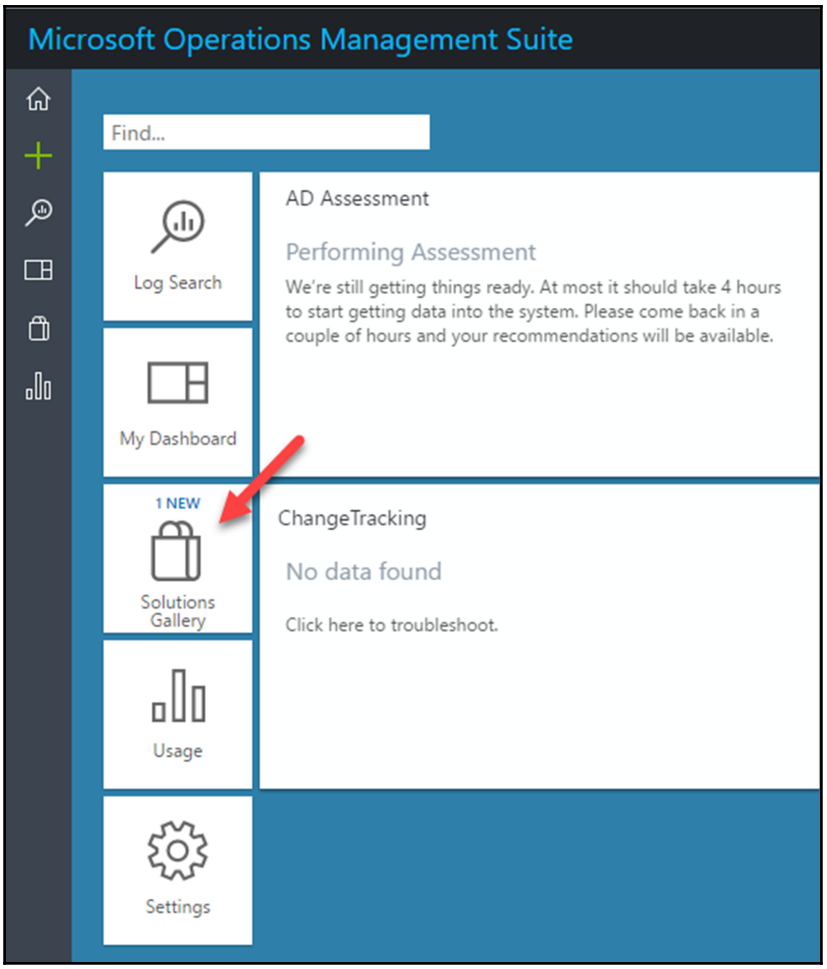

Microsoft Advanced Threat Analytics
Gateway deployment type
Gateway
The Gateway is installed on dedicated servers and requires configuration of port-mirroring from the domain controllers to receive network traffic.
Lightweight Gateway
The Lightweight Gateway is installed directly on your domain controllers and monitors local network traffic. The Lightweight Gateway also performs dynamic resource limitation based on the domain controller load.
Lightweight Gateway deployment and performance guidelines
This domain controller does not meet the minimum hardware requirements for the Lightweight Gateway.
Minimum hardware requirements guidelines
Back
Next

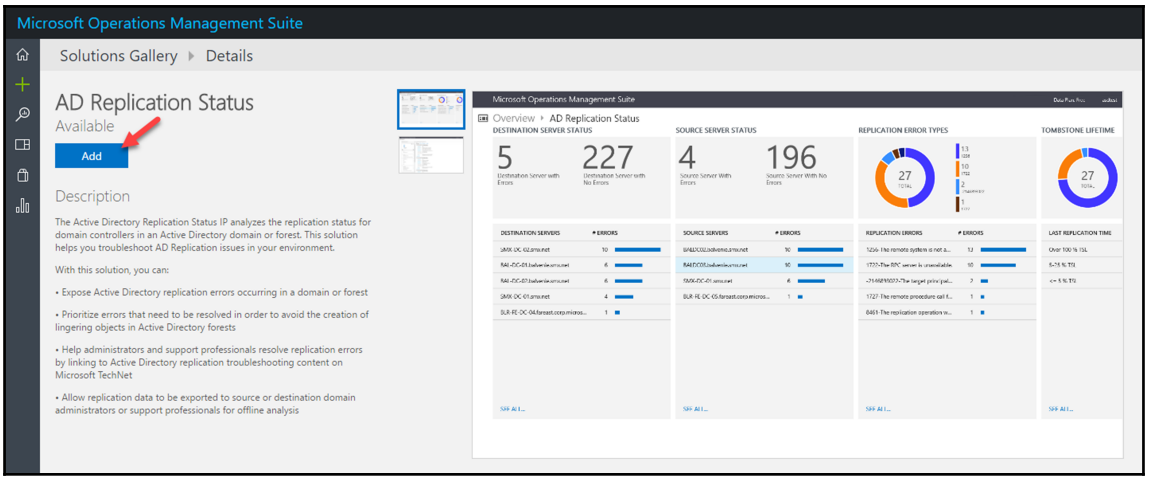

Microsoft Advanced Threat Analytics
Gateway Configuration
Installation Path
C:\Program Files\Microsoft Advanced Thre
Gateway Service SSL Certificate
Create self-signed certificate
Gateway Registration
Username
therebeladmin\administrator
Password
User must be a member of one of the following local groups on the Center: Administrators or Microsoft Advanced Threat Analytics Administrators
Back
Install

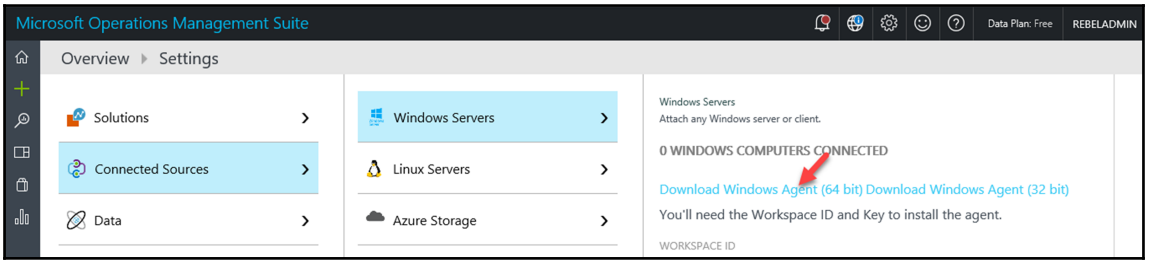

Search users, computers, servers, and more...
Microsoft
This version expires on 31/07/2017. After expiration, detection will no longer be available.
System
Center
Gateways
Updates
Data Sources
Directory Services
Events
Detection
Settings
Exclusions
Gateways
Download Gateway Setup
This package installs a Gateway or a Lightweight Gateway.
Name
Type
Domain Controllers
Version
Status
Health Issues
REBELN...
Lightweight Gateway
REBELNET-P...
1.7.5757.57477
Running

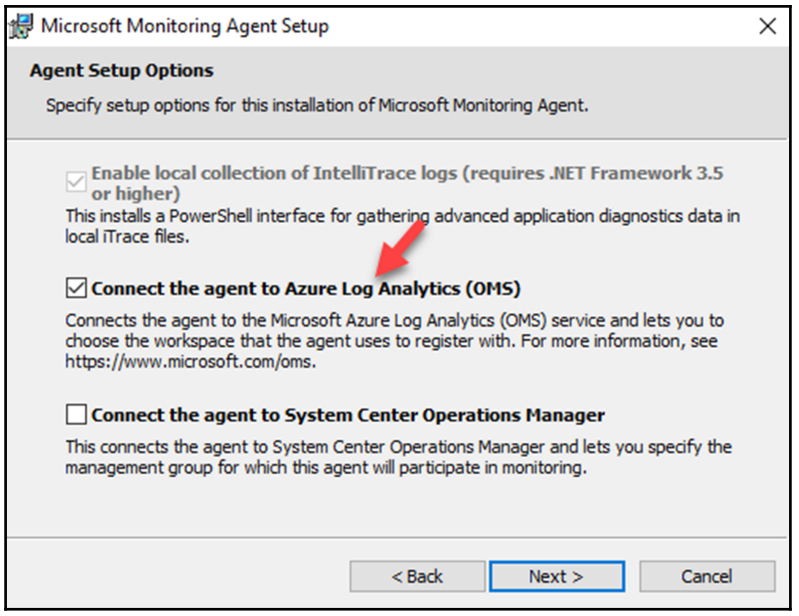

Reconnaissance using DNS
Suspicious DNS activity was observed, originating from REBEL-ATA (which is not a DNS server) against REBELNET-PDC01.
Note
Share
Export to Excel
Details
Input
Open
Is running scanning tools allowed from the computer listed below?
DNS queries
REBEL-ATA
REBELNET-PDC01
Computers (1)
No
Yes
REBEL-ATA
Save
Cancel
Activate Windows

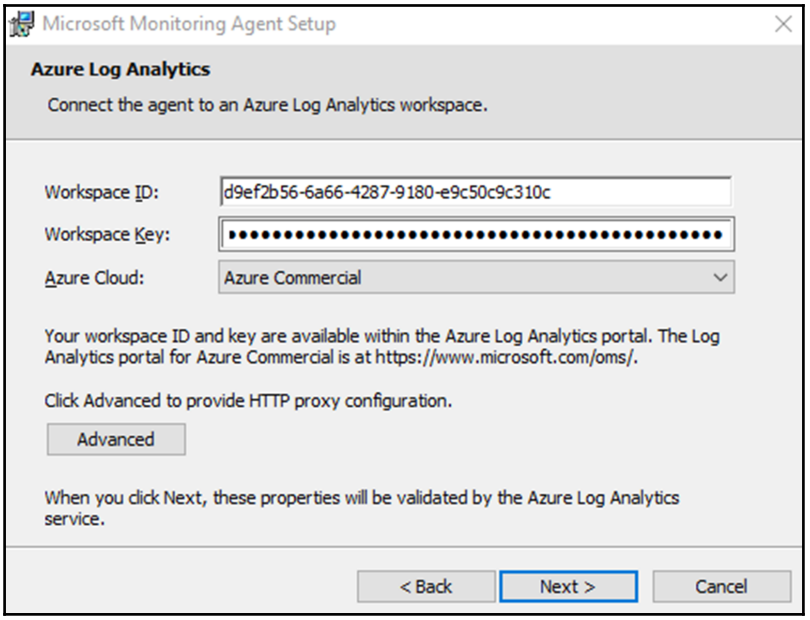

This version expires on 31/07/2017. After expiration, detection will no longer be available.
System
Center
Gateways
Updates
Data Sources
Directory Services
Events
Detection
Settings
Exclusions
Notifications
Settings
Mail server
Syslog server
Mail server
Configure mail notifications
SMTP server endpoint
mail.domain.com
25
SSL
Authentication
Send from
user@domain.com
Send test mail

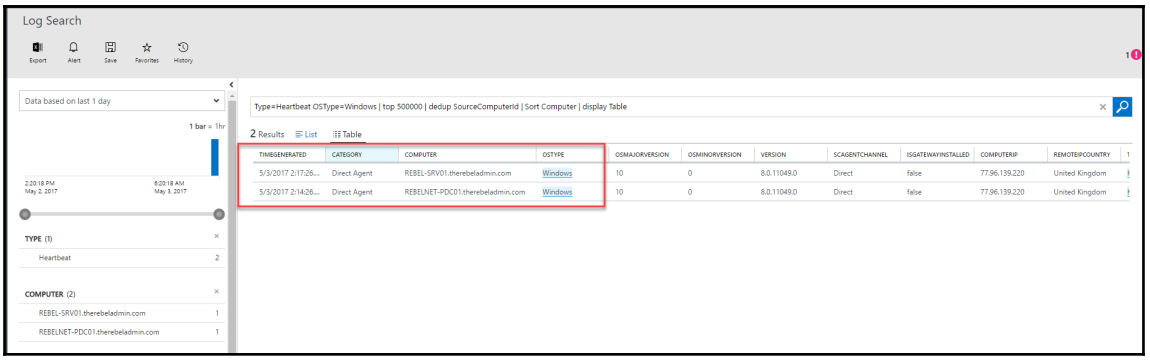

Microsoft Operations Management Suite
Find...
Log Search
AD Assessment
Performing Assessment
We're still getting things ready. At most it should take 4 hours to start getting data into the system. Please come back in a couple of hours and your recommendations will be available.
My Dashboard
1 NEW
Solutions Gallery
ChangeTracking
No data found
Click here to troubleshoot.
Usage
Settings

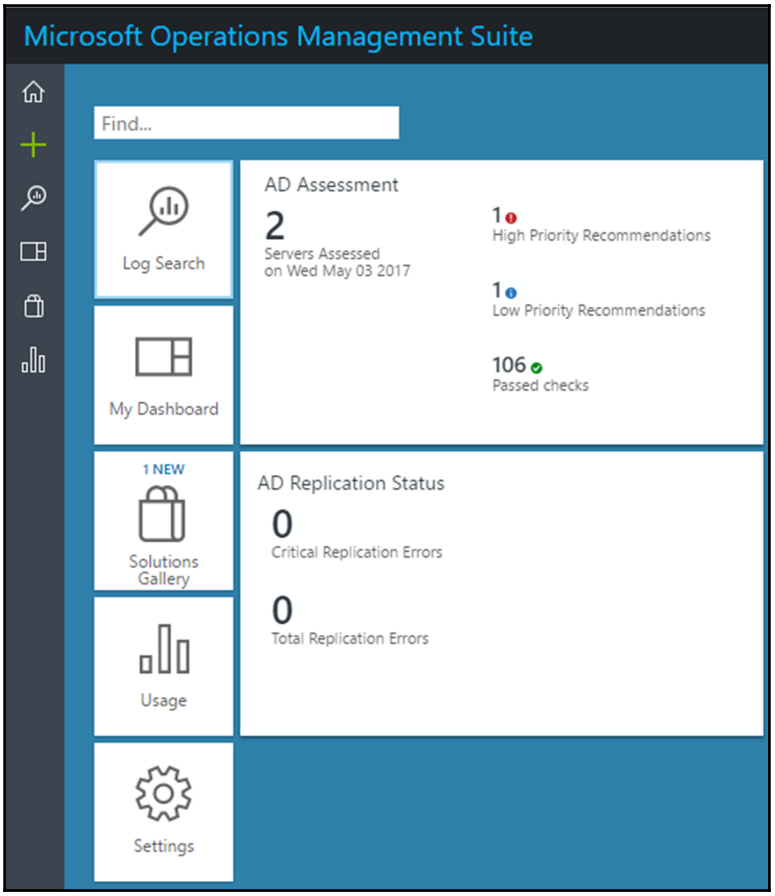

Microsoft Operations Management Suite
Solutions Gallery
Details
AD Replication Status
Available
Add
Description
The Active Directory Replication Status IP analyzes the replication status for domain controllers in an Active Directory domain or forest. This solution helps you troubleshoot AD Replication issues in your environment.
With this solution, you can:
• Expose Active Directory replication errors occurring in a domain or forest
• Prioritize errors that need to be resolved in order to avoid the creation of lingering objects in Active Directory forests
• Help administrators and support professionals resolve replication errors by linking to Active Directory replication troubleshooting content on Microsoft TechNet
• Allow replication data to be exported to source or destination domain administrators or support professionals for offline analysis
Overview
AD Replication Status
DESTINATION SERVER STATUS
5
227
SOURCE SERVER STATUS
4
196
REPLICATION ERROR TYPES
TOMBSTONE LIFETIME

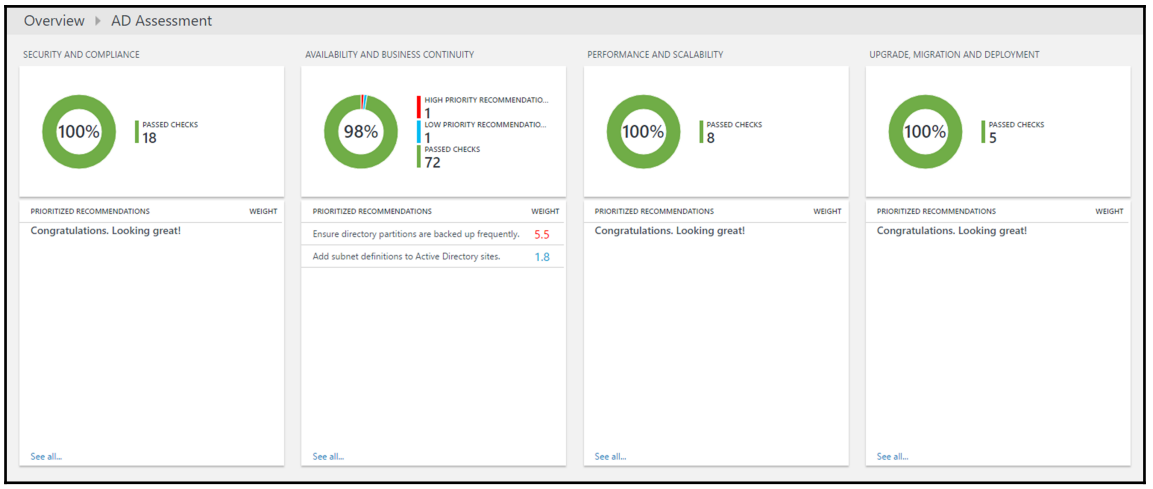

Microsoft Operations Management Suite
Data Plan: Free
REBELADMIN
Overview
Settings
Solutions
Connected Sources
Data
Windows Servers
Linux Servers
Azure Storage
Windows Servers
Attach any Windows server or client.
0 WINDOWS COMPUTERS CONNECTED
Download Windows Agent (64 bit) Download Windows Agent (32 bit)
You'll need the Workspace ID and Key to install the agent.
WORKSPACE ID

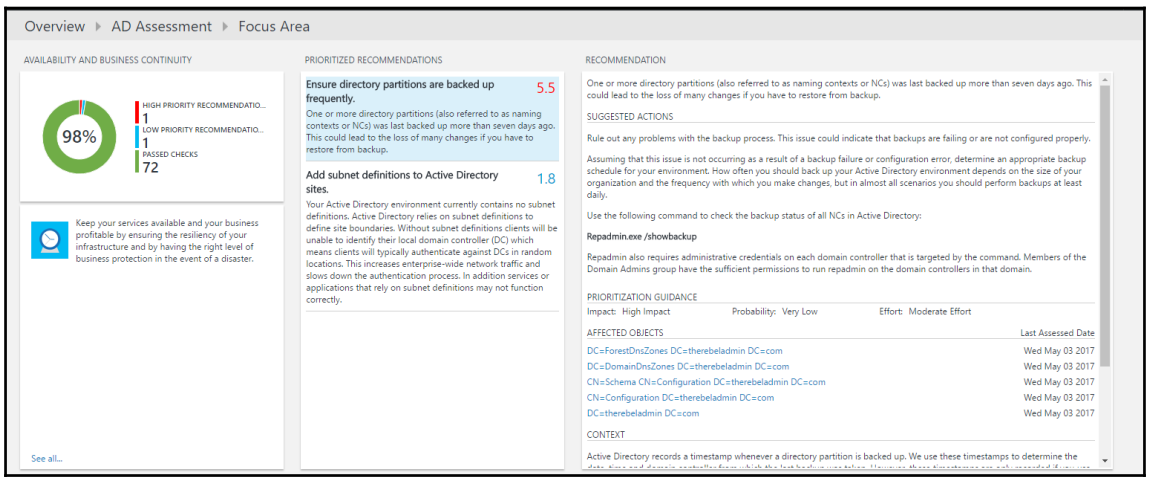

Microsoft Monitoring Agent Setup
Agent Setup Options
Specify setup options for this installation of Microsoft Monitoring Agent.
Enable local collection of IntelliTrace logs (requires .NET Framework 3.5 or higher)
This installs a PowerShell interface for gathering advanced application diagnostics data in local iTrace files.
Connect the agent to Azure Log Analytics (OMS)
Connects the agent to the Microsoft Azure Log Analytics (OMS) service and lets you to choose the workspace that the agent uses to register with. For more information, see https://www.microsoft.com/oms.
Connect the agent to System Center Operations Manager
This connects the agent to System Center Operations Manager and lets you specify the management group for which this agent will participate in monitoring.
< Back
Next >
Cancel

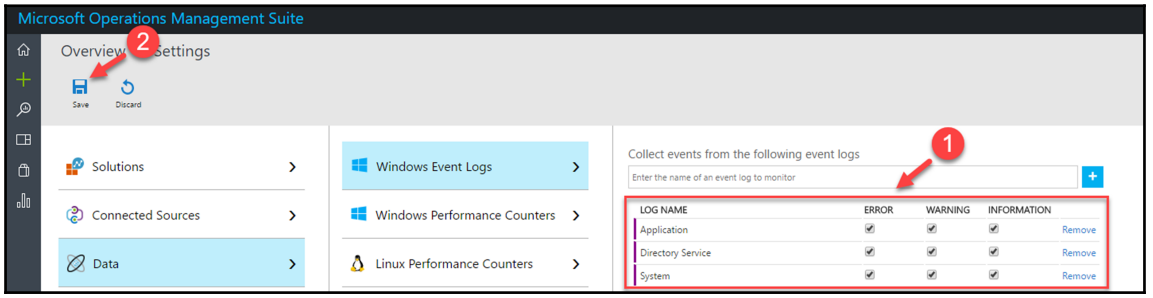

Microsoft Monitoring Agent Setup
Azure Log Analytics
Connect the agent to an Azure Log Analytics workspace.
Workspace ID:
d9ef2b56-6a66-4287-9180-e9c50c9c310c
Workspace Key:
Azure Cloud:
Azure Commercial
Your workspace ID and key are available within the Azure Log Analytics portal. The Log Analytics portal for Azure Commercial is at https://www.microsoft.com/oms/.
Click Advanced to provide HTTP proxy configuration.
Advanced
When you click Next, these properties will be validated by the Azure Log Analytics service.
< Back
Next >
Cancel

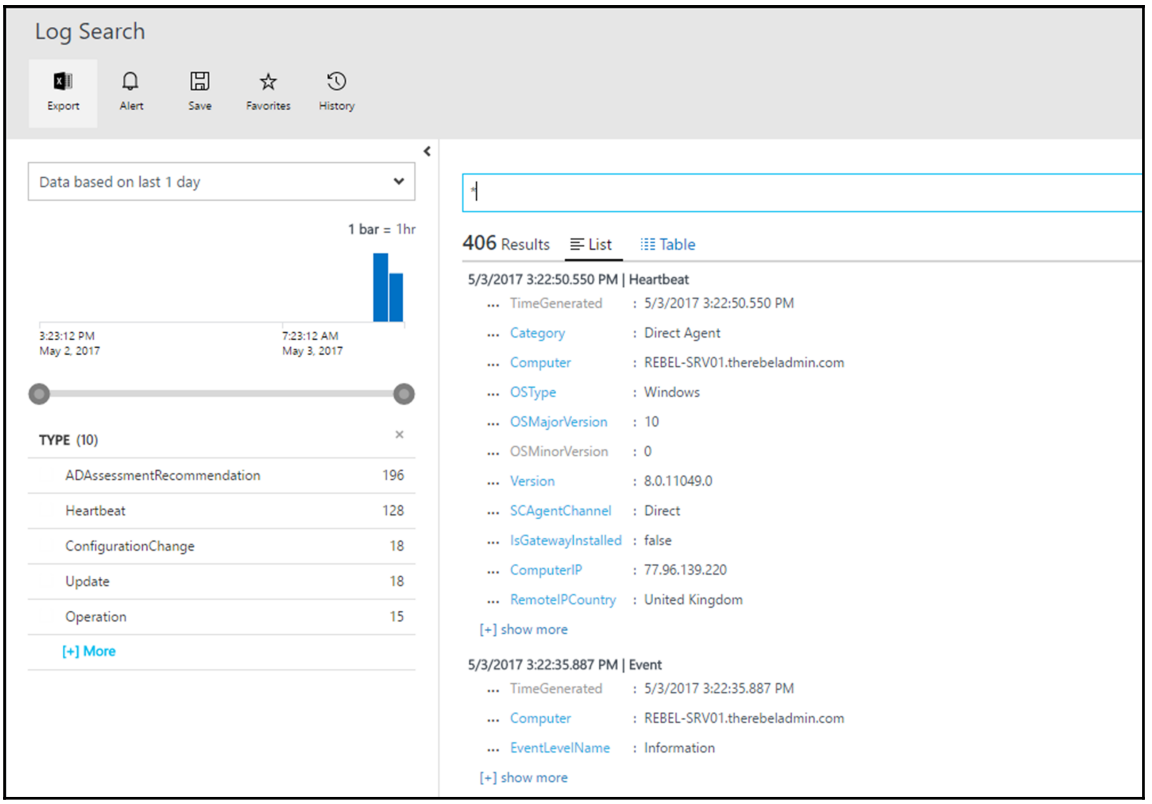

Log Search
Export
Alert
Save
Favorites
History
Data based on last 1 day
1 bar = 1hr
2:20:18 PM
May 2, 2017
6:20:18 AM
May 3, 2017
TYPE (1)
Heartbeat 2
COMPUTER (2)
REBEL-SRV01.therebeladmin.com 1
REBELNET-PDC01.therebeladmin.com 1
Type=Heartbeat OSType=Windows | top 500000 | dedup SourceComputerId | Sort Computer | display Table
2 Results
List
Table
TIMEGENERATED
CATEGORY
COMPUTER
OSTYPE
OSMAJORVERSION
OSMINORVERSION
VERSION
SCAGENTCHANNEL
ISGATEWAYINSTALLED
COMPUTERIP
REMOTEIPCOUNTRY
5/3/2017 2:17:26...
Direct Agent
REBEL-SRV01.therebeladmin.com
Windows
10
0
8.0.11049.0
Direct
false
77.96.139.220
United Kingdom
5/3/2017 2:14:26...
Direct Agent
REBELNET-PDC01.therebeladmin.com
Windows
10
0
8.0.11049.0
Direct
false
77.96.139.220
United Kingdom


Microsoft Operations Management Suite
Find...
Log Search
My Dashboard
1 NEW
Solutions Gallery
Usage
Settings
AD Assessment
2
Servers Assessed
on Wed May 03 2017
1
High Priority Recommendations
1
Low Priority Recommendations
106
Passed checks
AD Replication Status
0
Critical Replication Errors
0
Total Replication Errors


Overview ▸ AD Assessment
SECURITY AND COMPLIANCE
100%
PASSED CHECKS
18
PRIORITIZED RECOMMENDATIONS
WEIGHT
Congratulations. Looking great!
See all...
AVAILABILITY AND BUSINESS CONTINUITY
98%
HIGH PRIORITY RECOMMENDATIO...
1
LOW PRIORITY RECOMMENDATIO...
1
PASSED CHECKS
72
PRIORITIZED RECOMMENDATIONS
WEIGHT
Ensure directory partitions are backed up frequently.
5.5
Add subnet definitions to Active Directory sites.
1.8
See all...
PERFORMANCE AND SCALABILITY
100%
PASSED CHECKS
8
PRIORITIZED RECOMMENDATIONS
WEIGHT
Congratulations. Looking great!
See all...
UPGRADE, MIGRATION AND DEPLOYMENT
100%
PASSED CHECKS
5
PRIORITIZED RECOMMENDATIONS
WEIGHT
Congratulations. Looking great!
See all...


Overview ▸ AD Assessment ▸ Focus Area
AVAILABILITY AND BUSINESS CONTINUITY
98%
HIGH PRIORITY RECOMMENDATIO...
1
LOW PRIORITY RECOMMENDATIO...
1
PASSED CHECKS
72
Keep your services available and your business profitable by ensuring the resiliency of your infrastructure and by having the right level of business protection in the event of a disaster.
See all...
PRIORITIZED RECOMMENDATIONS
Ensure directory partitions are backed up frequently.
5.5
One or more directory partitions (also referred to as naming contexts or NCs) was last backed up more than seven days ago. This could lead to the loss of many changes if you have to restore from backup.
Add subnet definitions to Active Directory sites.
1.8
Your Active Directory environment currently contains no subnet definitions. Active Directory relies on subnet definitions to define site boundaries. Without subnet definitions clients will be unable to identify their local domain controller (DC) which means clients will typically authenticate against DCs in random locations. This increases enterprise-wide network traffic and slows down the authentication process. In addition services or applications that rely on subnet definitions may not function correctly.
RECOMMENDATION
One or more directory partitions (also referred to as naming contexts or NCs) was last backed up more than seven days ago. This could lead to the loss of many changes if you have to restore from backup.
SUGGESTED ACTIONS
Rule out any problems with the backup process. This issue could indicate that backups are failing or are not configured properly.
Assuming that this issue is not occurring as a result of a backup failure or configuration error, determine an appropriate backup schedule for your environment. How often you should back up your Active Directory environment depends on the size of your organization and the frequency with which you make changes, but in almost all scenarios you should perform backups at least daily.
Use the following command to check the backup status of all NCs in Active Directory:
Repadmin.exe /showbackup
Repadmin also requires administrative credentials on each domain controller that is targeted by the command. Members of the Domain Admins group have the sufficient permissions to run repadmin on the domain controllers in that domain.
PRIORITIZATION GUIDANCE
Impact: High Impact
Probability: Very Low
Effort: Moderate Effort
AFFECTED OBJECTS
Last Assessed Date
DC=ForestDnsZones DC=therebeladmin DC=com
Wed May 03 2017
DC=DomainDnsZones DC=therebeladmin DC=com
Wed May 03 2017
CN=Schema CN=Configuration DC=therebeladmin DC=com
Wed May 03 2017
CN=Configuration DC=therebeladmin DC=com
Wed May 03 2017
DC=therebeladmin DC=com
Wed May 03 2017
CONTEXT
Active Directory records a timestamp whenever a directory partition is backed up. We use these timestamps to determine the


Microsoft Operations Management Suite
Overview ▸ Settings
2
Save
Discard
Solutions
Connected Sources
Data
Windows Event Logs
Windows Performance Counters
Linux Performance Counters
Collect events from the following event logs
1
Enter the name of an event log to monitor
LOG NAME
ERROR
WARNING
INFORMATION
Application
Directory Service
System
Remove


Log Search
Export
Alert
Save
Favorites
History
Data based on last 1 day
1 bar = 1hr
3:23:12 PM
May 2, 2017
7:23:12 AM
May 3, 2017
TYPE (10)
ADAssessmentRecommendation 196
Heartbeat 128
ConfigurationChange 18
Update 18
Operation 15
[+] More
406 Results
List
Table
5/3/2017 3:22:50.550 PM | Heartbeat
TimeGenerated : 5/3/2017 3:22:50.550 PM
Category : Direct Agent
Computer : REBEL-SRV01.therebeladmin.com
OSType : Windows
OSMajorVersion : 10
OSMinorVersion : 0
Version : 8.0.11049.0
SCAgentChannel : Direct
IsGatewayInstalled : false
ComputerIP : 77.96.139.220
RemoteIPCountry : United Kingdom
[+] show more
5/3/2017 3:22:35.887 PM | Event
TimeGenerated : 5/3/2017 3:22:35.887 PM
Computer : REBEL-SRV01.therebeladmin.com
EventLevelName : Information
[+] show more

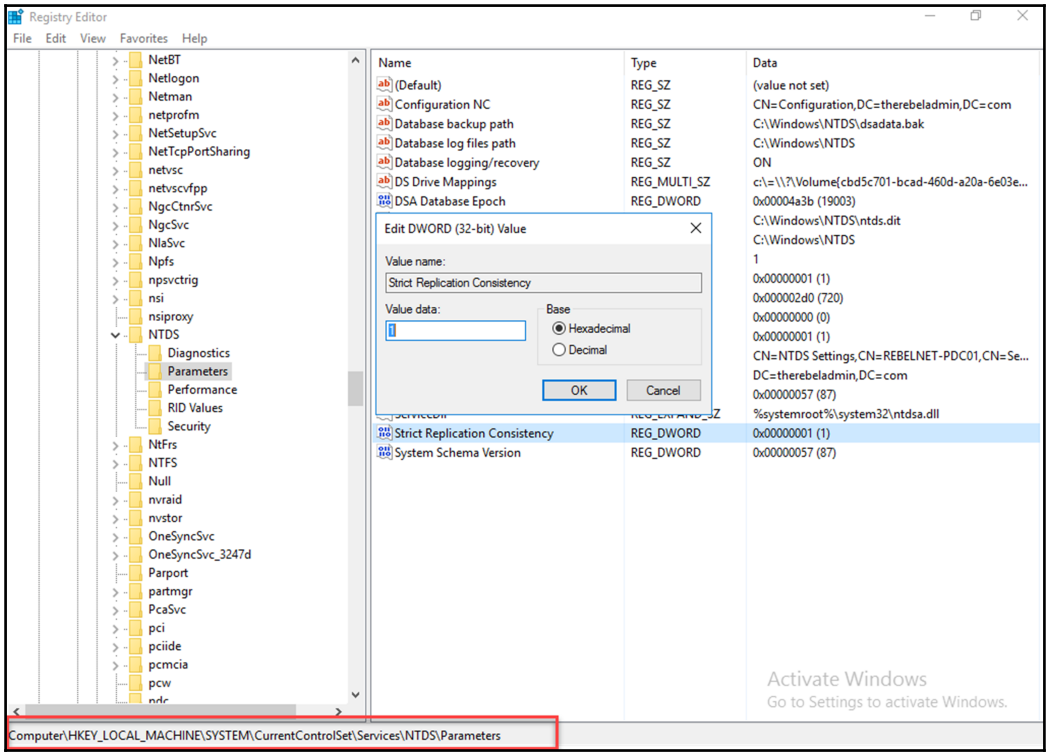
Chapter 19: Active Directory Audit and Monitoring

```
PS C:\Users\Administrator> repadmin /showrepl /csv
showrepl_COLUMNS,Destination DSA Site,Destination DSA,Naming Context,Source DSA Site,Source DSA,Transport Type,Number of Failures,Last Failure
 Time,Last Success Time,Last Failure Status
showrepl_INFO,Default-First-Site-Name,REBELNET-PDC01,"DC=therebeladmin,DC=com",Default-First-Site-Name,REBEL-SRV01,RPC,0,0,2017-05-05 10:54:43
,0
showrepl_INFO,Default-First-Site-Name,REBELNET-PDC01,"CN=Configuration,DC=therebeladmin,DC=com",Default-First-Site-Name,REBEL-SRV01,RPC,0,0,20
17-05-05 10:54:43,0
showrepl_INFO,Default-First-Site-Name,REBELNET-PDC01,"CN=Schema,CN=Configuration,DC=therebeladmin,DC=com",Default-First-Site-Name,REBEL-SRV01,
RPC,0,0,2017-05-05 10:54:43,0
showrepl_INFO,Default-First-Site-Name,REBELNET-PDC01,"DC=DomainDnsZones,DC=therebeladmin,DC=com",Default-First-Site-Name,REBEL-SRV01,RPC,0,0,2
017-05-05 10:54:43,0
showrepl_INFO,Default-First-Site-Name,REBELNET-PDC01,"DC=ForestDnsZones,DC=therebeladmin,DC=com",Default-First-Site-Name,REBEL-SRV01,RPC,0,0,2
017-05-05 10:54:43,0
```

```
PS C:\Users\Administrator> repadmin /syncall REBEL-SRV01 dc=therebeladmin,dc=com
Syncing partition: dc=therebeladmin,dc=com
CALLBACK MESSAGE: The following replication is in progress:
    From: e05aa0a0-dfdc-4964-9ae2-da7667fcce87._msdcs.therebeladmin.com
    To  : d3f89917-5fff-40a8-acc2-b148b60d9309._msdcs.therebeladmin.com
CALLBACK MESSAGE: The following replication completed successfully:
    From: e05aa0a0-dfdc-4964-9ae2-da7667fcce87._msdcs.therebeladmin.com
    To  : d3f89917-5fff-40a8-acc2-b148b60d9309._msdcs.therebeladmin.com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

```
PS C:\Users\Administrator> repadmin /showchanges REBELNET-PDC01 d3f89917-5fff-40a8-acc2-b148b60d9309 dc=therebeladmin,dc=com
Building starting position from destination server REBELNET-PDC01
Source Neighbor:
dc=therebeladmin,dc=com
pszDsa = d3f89917-5fff-40a8-acc2-b148b60d9309._msdcs.therebeladmin.com
==== INBOUND NEIGHBORS ======================================

dc=therebeladmin,dc=com
    Default-First-Site-Name\REBEL-SRV01 via RPC
        DSA object GUID: d3f89917-5fff-40a8-acc2-b148b60d9309
        Address: d3f89917-5fff-40a8-acc2-b148b60d9309._msdcs.therebeladmin.com
        DSA invocationID: 833e9bd7-4598-4acc-bf7b-6981b54e907e
        SYNC_ON_STARTUP DO_SCHEDULED_SYNCS WRITEABLE
        USNs: 30522/OU, 30522/PU
        Last attempt @ 2017-05-05 11:25:27 was successful.
Destination's up-to-date vector:
833e9bd7-4598-4acc-bf7b-6981b54e907e @ USN 30571
e05aa0a0-dfdc-4964-9ae2-da7667fcce87 @ USN 28944
==== SOURCE DSA: (null) ====
No Changes
```

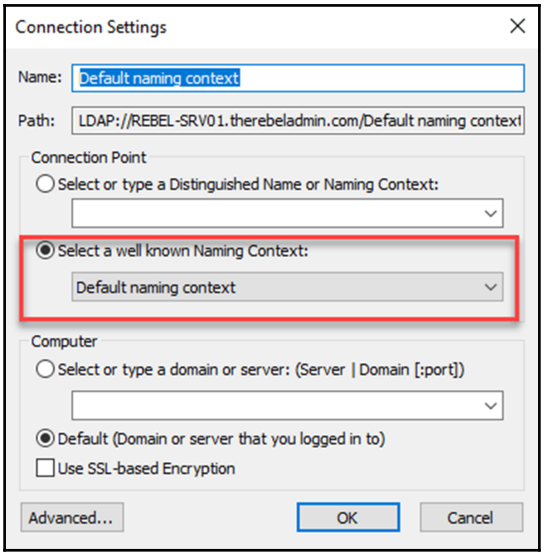
```
PS C:\Users\Administrator> Get-ADReplicationConnection -Filter *


AutoGenerated                       : True
DistinguishedName                   : CN=1364adb7-76d4-46ec-83fa-21a4060d0538,CN=NTDS Settings,CN=REBELNET-PDC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=therebeladmin,DC=com
InterSiteTransportProtocol          :
Name                                : 1364adb7-76d4-46ec-83fa-21a4060d0538
ObjectClass                         : nTDSConnection
ObjectGUID                          : c449cede-d8df-43f6-bf4d-c9d9e5d533da
PartiallyReplicatedNamingContexts   : {}
ReplicatedNamingContexts            : {DC=ForestDnsZones,DC=therebeladmin,DC=com, DC=DomainDnsZones,DC=therebeladmin,DC=com,
                                      CN=Schema,CN=Configuration,DC=therebeladmin,DC=com, CN=Configuration,DC=therebeladmin,DC=com...}
ReplicateFromDirectoryServer        : CN=NTDS Settings,CN=REBEL-SRV01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=therebeladmin,DC=com
ReplicateToDirectoryServer          : CN=REBELNET-PDC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=therebeladmin,DC=com
ReplicationSchedule                 : System.DirectoryServices.ActiveDirectory.ActiveDirectorySchedule

AutoGenerated                       : True
DistinguishedName                   : CN=ca959ad0-bf91-4c33-ade1-1182060474c2,CN=NTDS Settings,CN=REBEL-SRV01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=therebeladmin,DC=com
InterSiteTransportProtocol          :
Name                                : ca959ad0-bf91-4c33-ade1-1182060474c2
ObjectClass                         : nTDSConnection
ObjectGUID                          : 0490d8a6-db8c-467e-8734-37a026346a40
PartiallyReplicatedNamingContexts   : {}
ReplicatedNamingContexts            : {DC=ForestDnsZones,DC=therebeladmin,DC=com, DC=DomainDnsZones,DC=therebeladmin,DC=com,
                                      CN=Schema,CN=Configuration,DC=therebeladmin,DC=com, CN=Configuration,DC=therebeladmin,DC=com...}
ReplicateFromDirectoryServer        : CN=NTDS Settings,CN=REBELNET-PDC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=therebeladmin,DC=com
ReplicateToDirectoryServer          : CN=REBEL-SRV01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=therebeladmin,DC=com
ReplicationSchedule                 : System.DirectoryServices.ActiveDirectory.ActiveDirectorySchedule
```

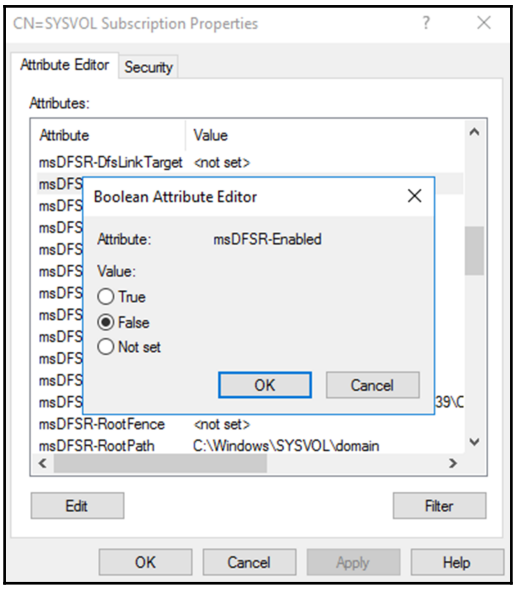


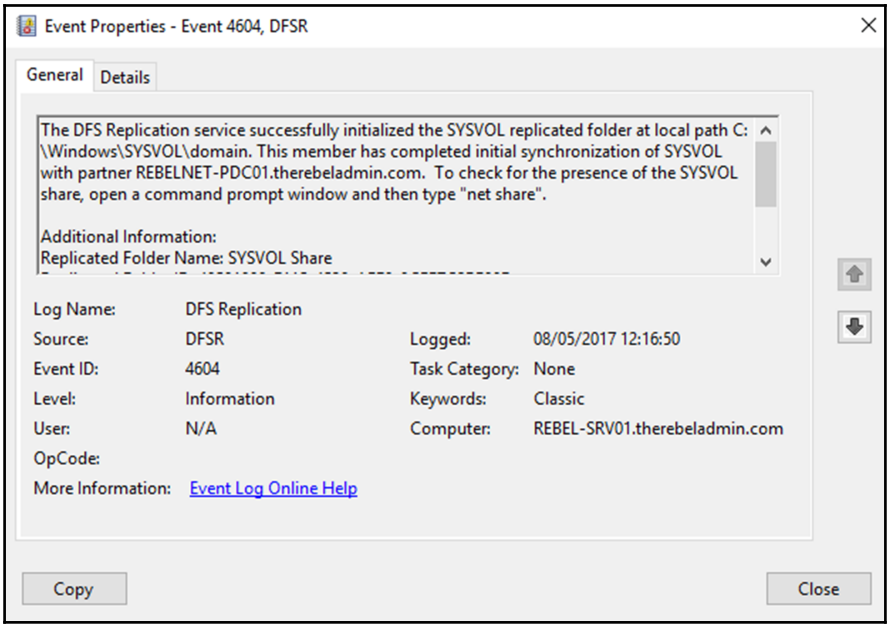
```
C:\Windows\system32>For /f %s IN ('dsquery server -o rdn') do @echo %s && @(net view \\%s | find "SYSVOL") & echo
REBELNET-PDC01
SYSVOL      Disk           Logon server share
ECHO is on.
REBEL-SRV01
SYSVOL      Disk           Logon server share
ECHO is on.
```

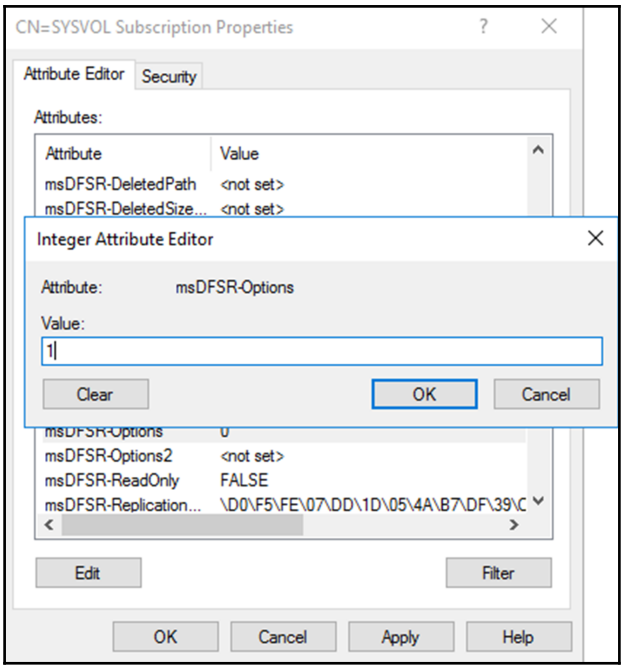
```
C:\Windows\system32>For /f %r IN ('dsquery server -o rdn') do @echo %i && @wmic /node:"%r" /namespace:\\root\microsoftdfs pat
h dfsrreplicatedfolderinfo WHERE replicatedfoldername='SYSVOL share' get replicatedfoldername,state
%i
ReplicatedFolderName  State
SYSVOL Share          4

%i
ReplicatedFolderName  State
SYSVOL Share          4
```

```
C:\Windows\system32>For /f %m IN ('dsquery server -o rdn') do @echo %m && @wmic /node:"%m" /namespace:\\root\microsoftdfs pat
h DfsrMachineConfig get MaxOfflineTimeInDays
REBELNET-PDC01
MaxOfflineTimeInDays
60

REBEL-SRV01
MaxOfflineTimeInDays
60
```



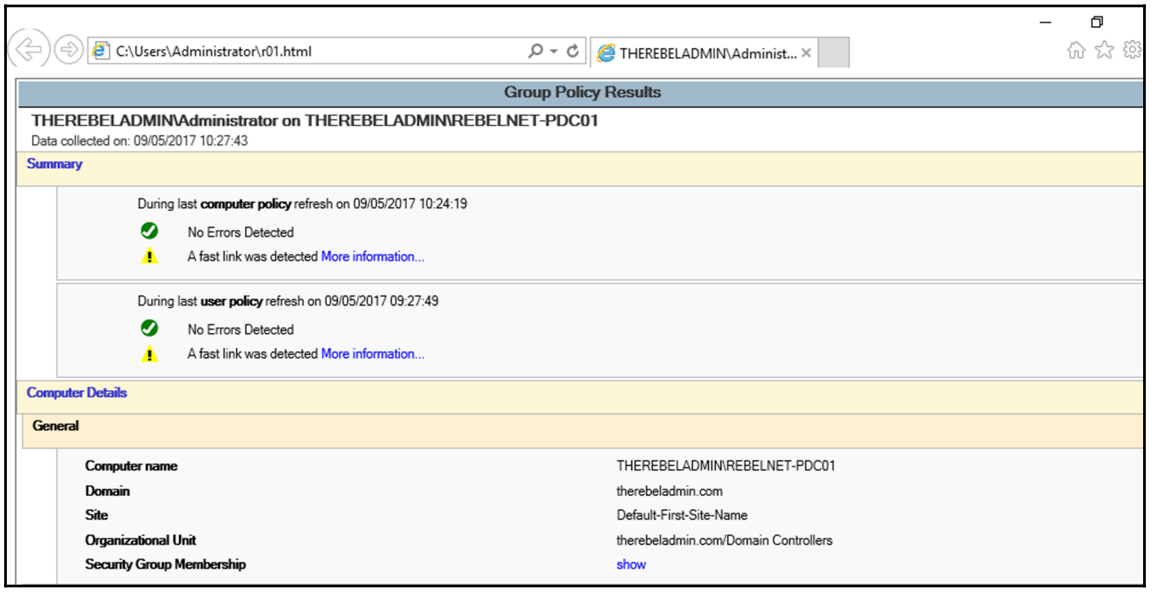

CN=SYSVOL Subscription Properties
Attribute Editor
Security
Attributes:
Attribute
Value
msDFSR-DfsLinkTarget
<not set>
Boolean Attribute Editor
Attribute:
msDFSR-Enabled
Value:
True
False
Not set
OK
Cancel
msDFSR-RootFence
<not set>
msDFSR-RootPath
C:\Windows\SYSVOL\domain
Edit
Filter
OK
Cancel
Apply
Help

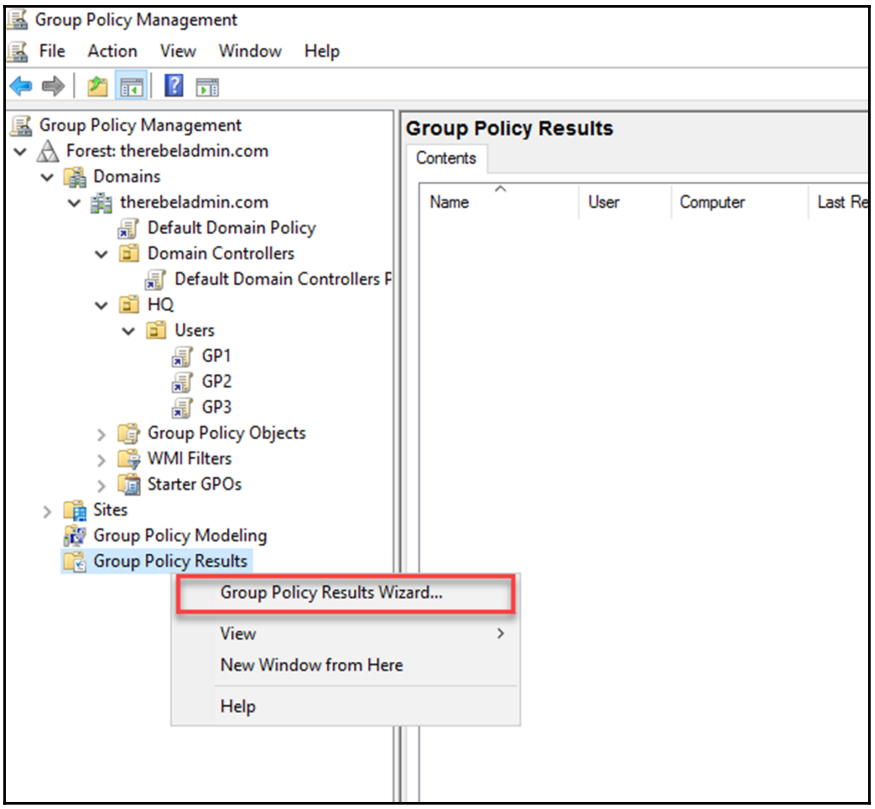

Event Properties - Event 4604, DFSR
General
Details
The DFS Replication service successfully initialized the SYSVOL replicated folder at local path C:\Windows\SYSVOL\domain. This member has completed initial synchronization of SYSVOL with partner REBELNET-PDC01.therebeladmin.com. To check for the presence of the SYSVOL share, open a command prompt window and then type "net share".
Additional Information:
Replicated Folder Name: SYSVOL Share
Log Name: DFS Replication
Source: DFSR
Logged: 08/05/2017 12:16:50
Event ID: 4604
Task Category: None
Level: Information
Keywords: Classic
User: N/A
Computer: REBEL-SRV01.therebeladmin.com
OpCode:
More Information: Event Log Online Help
Copy
Close

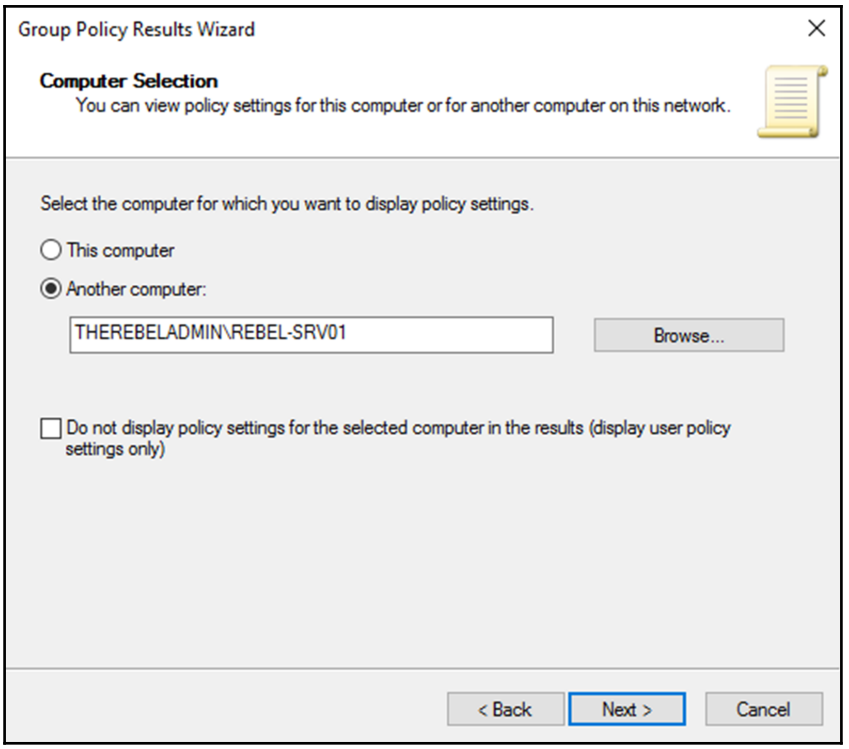

CN=SYSVOL Subscription Properties
Attribute Editor
Security
Attributes:
Attribute
Value
msDFSR-DeletedPath
<not set>
msDFSR-DeletedSize...
<not set>
Integer Attribute Editor
Attribute:
msDFSR-Options
Value:
1
Clear
OK
Cancel
msDFSR-Options
0
msDFSR-Options2
<not set>
msDFSR-ReadOnly
FALSE
msDFSR-Replication...
\D0\F5\FE\07\DD\1D\05\4A\B7\DF\39\C
Edit
Filter
OK
Cancel
Apply
Help

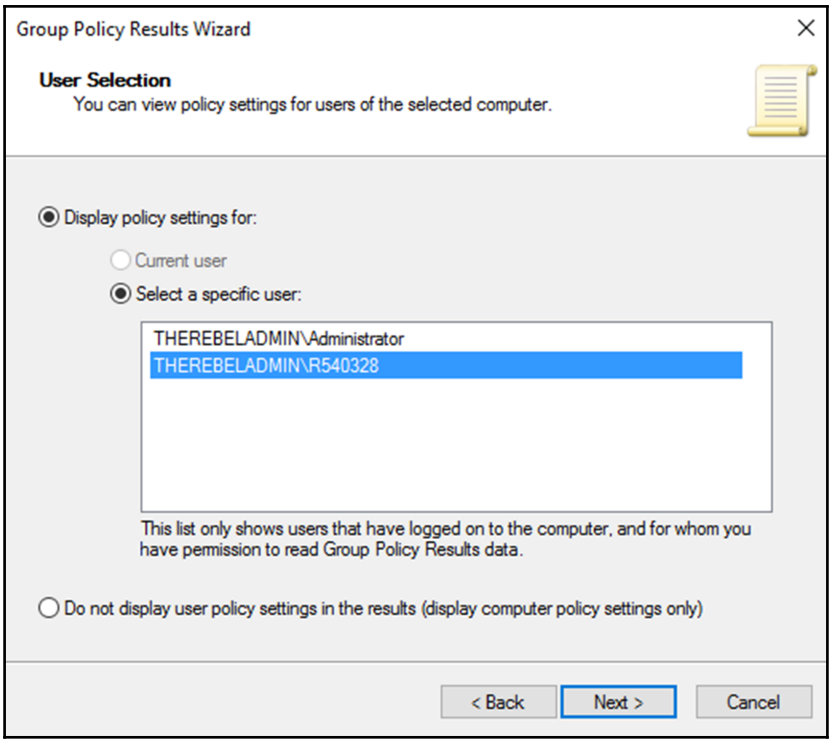
```
PS C:\Users\Administrator> gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2016 Microsoft Corporation. All rights reserved.

Created on 09/05/2017 at 09:49:13


RSOP data for THEREBELADMIN\Administrator on REBELNET-PDC01 : Logging Mode
------------------------------------------------------------------------------

OS Configuration:            Primary Domain Controller
OS Version:                  10.0.14393
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\Administrator
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=REBELNET-PDC01,OU=Domain Controllers,DC=therebeladmin,DC=com
    Last time Group Policy was applied: 09/05/2017 at 09:44:13
    Group Policy was applied from:      REBELNET-PDC01.therebeladmin.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        THEREBELADMIN
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        Default Domain Controllers Policy
        Default Domain Policy

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The computer is a part of the following security groups
    -------------------------------------------------------
        BUILTIN\Administrators
        Everyone
        BUILTIN\Pre-Windows 2000 Compatible Access
        BUILTIN\Users
        Windows Authorization Access Group
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users
        This Organization
        REBELNET-PDC01$
        Domain Controllers
        NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
        Authentication authority asserted identity
        Denied RODC Password Replication Group
        System Mandatory Level
```

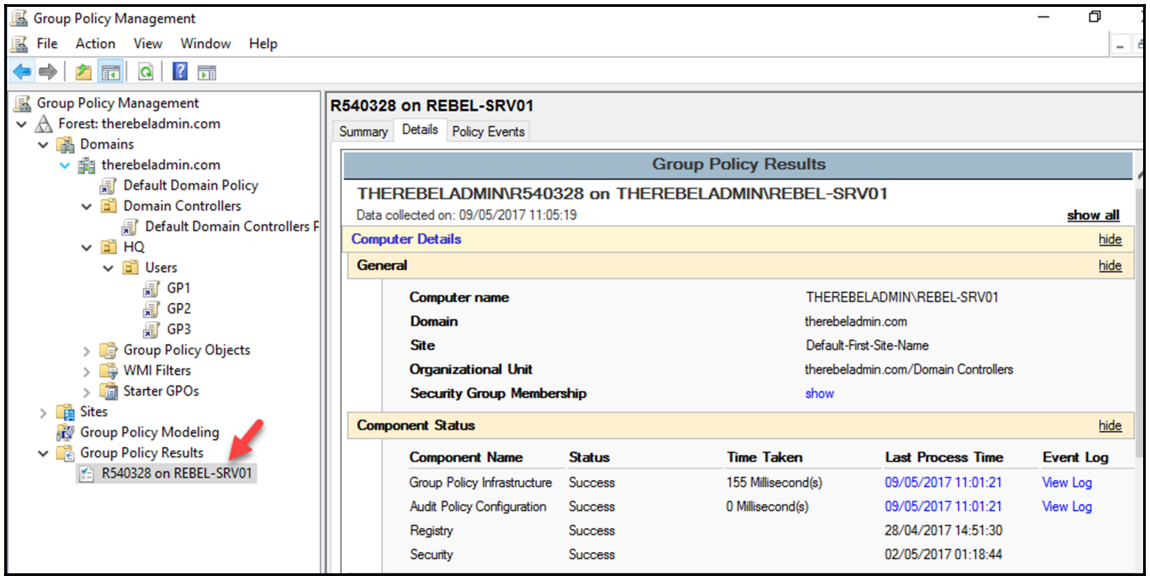
```
PS C:\Users\Administrator> gpresult /s REBEL-SRV01 /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2016 Microsoft Corporation. All rights reserved.

Created on 09/05/2017 at 10:04:35


RSOP data for THEREBELADMIN\Administrator on REBEL-SRV01 : Logging Mode
------------------------------------------------------------------------

OS Configuration:            Additional/Backup Domain Controller
OS Version:                  10.0.14393
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\administrator.THEREBELADMIN
Connected over a slow link?: Yes


COMPUTER SETTINGS
------------------

    Last time Group Policy was applied: 09/05/2017 at 10:01:18
    Group Policy was applied from:      REBEL-SRV01.therebeladmin.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        THEREBELADMIN
    Domain Type:                        Windows 2008 or later
```

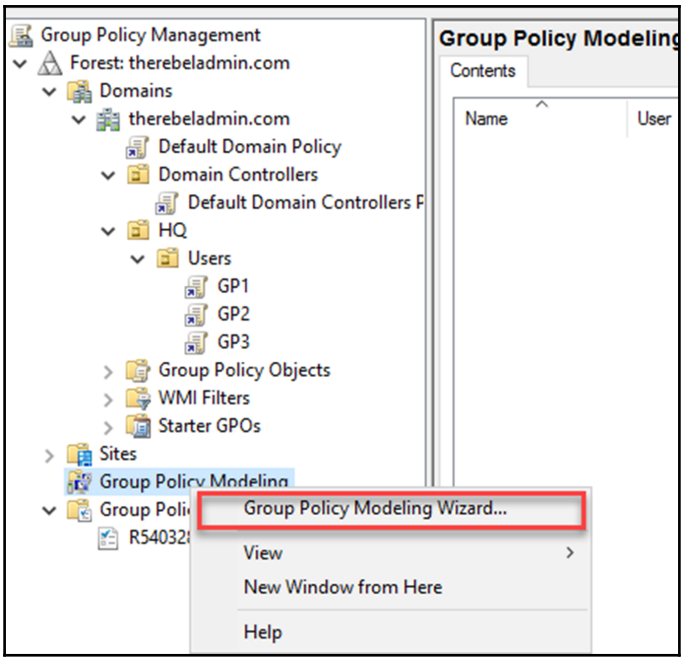


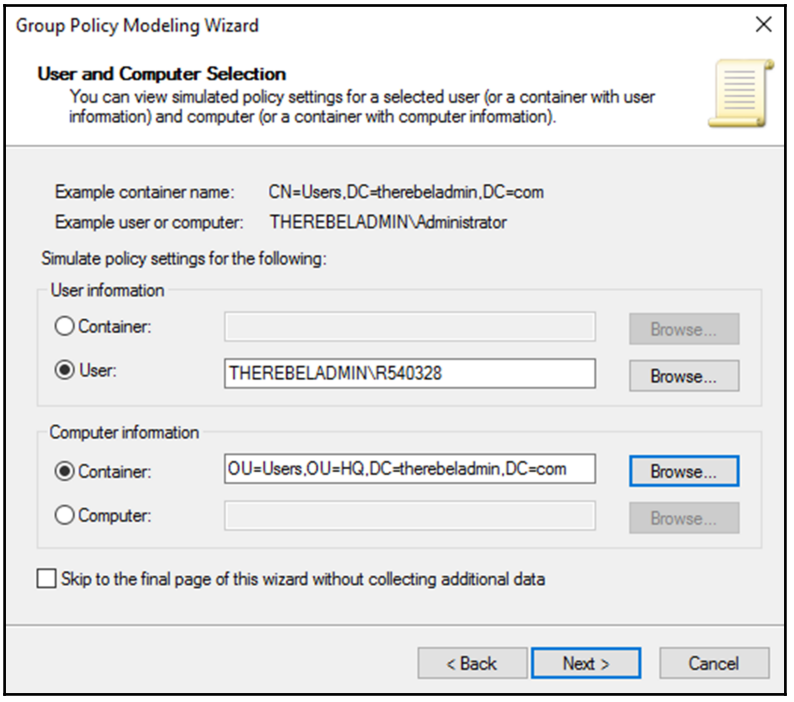

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: therebeladmin.com
Domains
therebeladmin.com
Default Domain Policy
Domain Controllers
Default Domain Controllers P
HQ
Users
GP1
GP2
GP3
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Results Wizard...
View
New Window from Here
Help
Group Policy Results
Contents
Name
User
Computer
Last Re

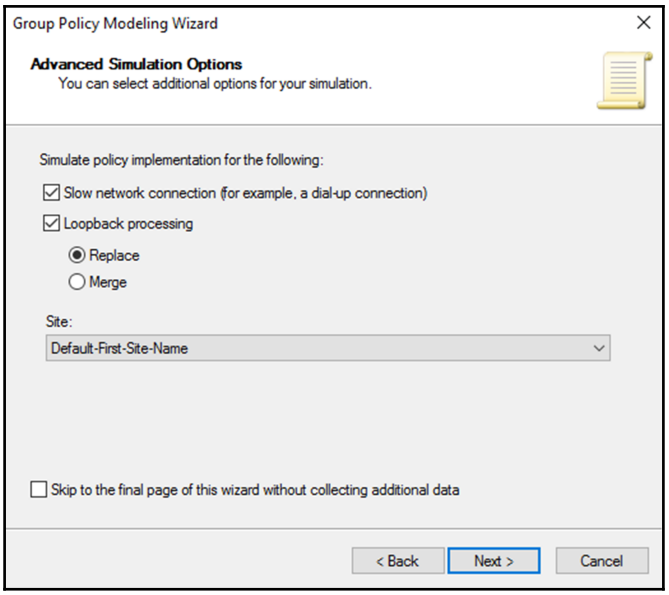

Group Policy Results Wizard
Computer Selection
You can view policy settings for this computer or for another computer on this network.
Select the computer for which you want to display policy settings.
This computer
Another computer:
THEREBELADMIN\REBEL-SRV01
Browse...
Do not display policy settings for the selected computer in the results (display user policy settings only)
< Back
Next >
Cancel

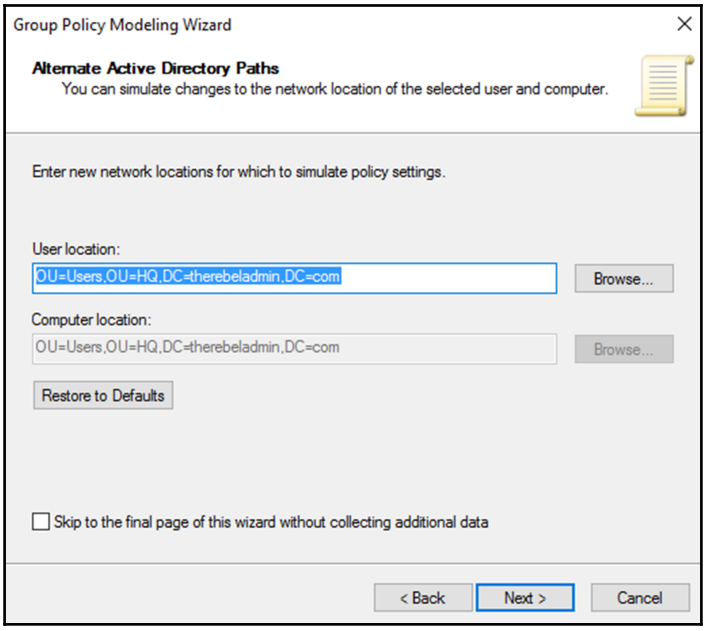

Group Policy Results Wizard
User Selection
You can view policy settings for users of the selected computer.
Display policy settings for:
Current user
Select a specific user:
THEREBELADMIN\Administrator
THEREBELADMIN\R540328
This list only shows users that have logged on to the computer, and for whom you have permission to read Group Policy Results data.
Do not display user policy settings in the results (display computer policy settings only)
< Back
Next >
Cancel

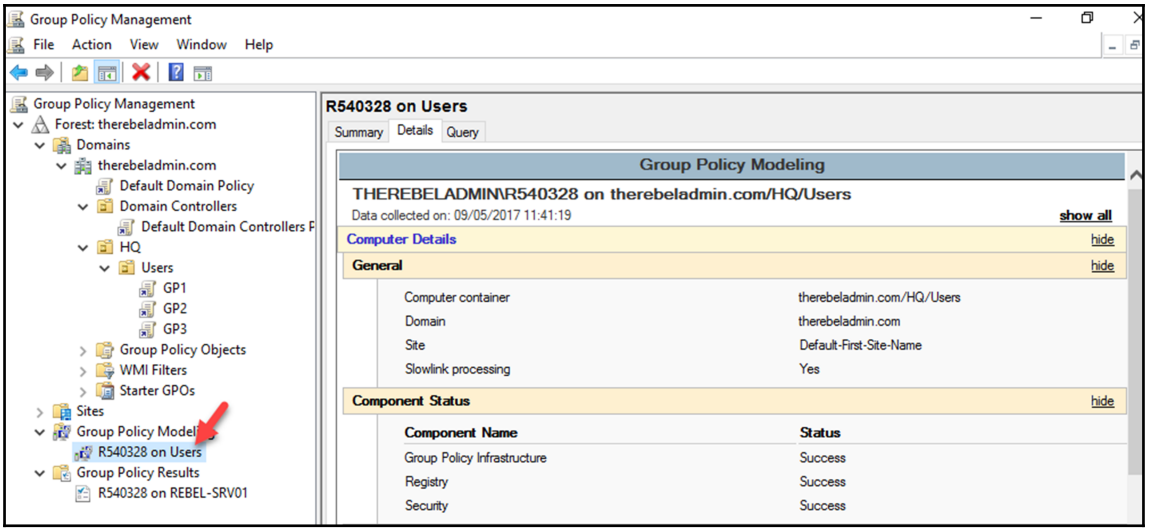

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: therebeladmin.com
Domains
therebeladmin.com
Default Domain Policy
Domain Controllers
Default Domain Controllers P
HQ
Users
GP1
GP2
GP3
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
R540328 on REBEL-SRV01
R540328 on REBEL-SRV01
Summary
Details
Policy Events
Group Policy Results
THEREBELADMIN\R540328 on THEREBELADMIN\REBEL-SRV01
Data collected on: 09/05/2017 11:05:19
show all
Computer Details
hide
General
hide
Computer name
THEREBELADMIN\REBEL-SRV01
Domain
therebeladmin.com
Site
Default-First-Site-Name
Organizational Unit
therebeladmin.com/Domain Controllers
Security Group Membership
show
Component Status
hide
Component Name
Status
Time Taken
Last Process Time
Event Log
Group Policy Infrastructure
Success
155 Millisecond(s)
09/05/2017 11:01:21
View Log
Audit Policy Configuration
Success
0 Millisecond(s)
09/05/2017 11:01:21
View Log
Registry
Success
28/04/2017 14:51:30
Security
Success
02/05/2017 01:18:44

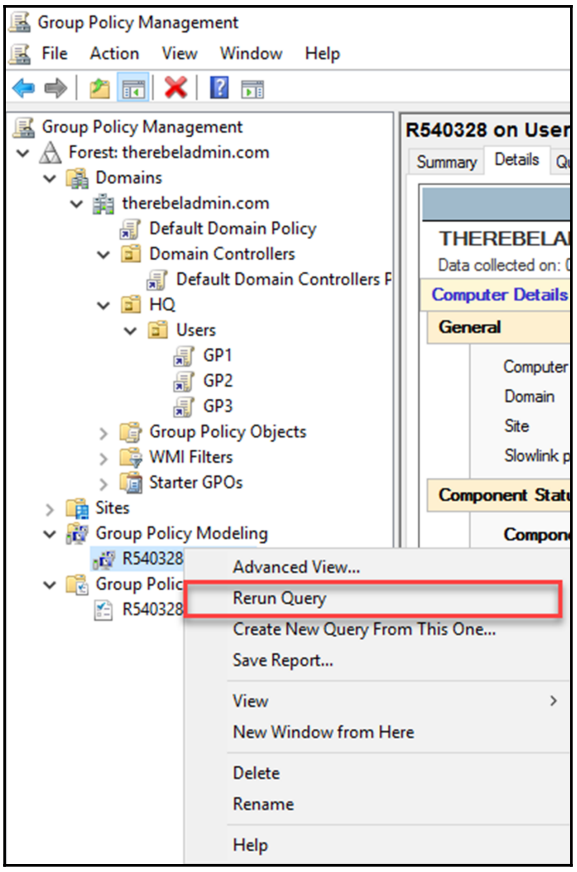

Group Policy Management
Forest: therebeladmin.com
Domains
therebeladmin.com
Default Domain Policy
Domain Controllers
Default Domain Controllers P
HQ
Users
GP1
GP2
GP3
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Poli
R540328
Group Policy Modeling
Contents
Name
User
Group Policy Modeling Wizard...
View
New Window from Here
Help


Group Policy Modeling Wizard
User and Computer Selection
You can view simulated policy settings for a selected user (or a container with user information) and computer (or a container with computer information).
Example container name: CN=Users,DC=therebeladmin,DC=com
Example user or computer: THEREBELADMIN\Administrator
Simulate policy settings for the following:
User information
Container:
User:
THEREBELADMIN\R540328
Browse...
Computer information
Container:
OU=Users,OU=HQ,DC=therebeladmin,DC=com
Computer:
Skip to the final page of this wizard without collecting additional data
< Back
Next >
Cancel

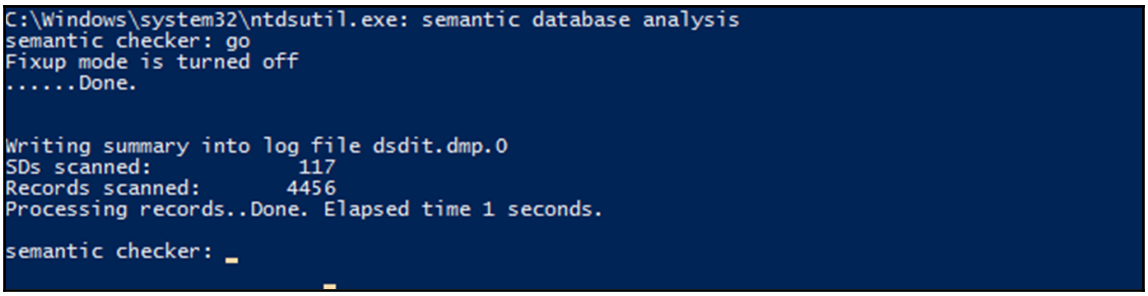

Group Policy Modeling Wizard
Advanced Simulation Options
You can select additional options for your simulation.
Simulate policy implementation for the following:
Slow network connection (for example, a dial-up connection)
Loopback processing
Replace
Merge
Site:
Default-First-Site-Name
Skip to the final page of this wizard without collecting additional data
< Back
Next >
Cancel


Group Policy Modeling Wizard
Alternate Active Directory Paths
You can simulate changes to the network location of the selected user and computer.
Enter new network locations for which to simulate policy settings.
User location:
OU=Users,OU=HQ,DC=therebeladmin,DC=com
Browse...
Computer location:
OU=Users,OU=HQ,DC=therebeladmin,DC=com
Browse...
Restore to Defaults
Skip to the final page of this wizard without collecting additional data
< Back
Next >
Cancel


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: therebeladmin.com
Domains
therebeladmin.com
Default Domain Policy
Domain Controllers
Default Domain Controllers P
HQ
Users
GP1
GP2
GP3
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
R540328 on Users
Group Policy Results
R540328 on REBEL-SRV01
R540328 on Users
Summary
Details
Query
Group Policy Modeling
THEREBELADMIN\R540328 on therebeladmin.com/HQ/Users
Data collected on: 09/05/2017 11:41:19
show all
Computer Details
hide
General
hide
Computer container
therebeladmin.com/HQ/Users
Domain
therebeladmin.com
Site
Default-First-Site-Name
Slowlink processing
Yes
Component Status
hide
Component Name
Status
Group Policy Infrastructure
Success
Registry
Success
Security
Success




```
file maintenance: integrity
Doing Integrity Check for db: C:\Windows\NTDS\ntds.dit.

Checking database integrity.

                    Scanning  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................


Integrity check successful.

It is recommended you run semantic database analysis
to ensure semantic database consistency as well.
```


C:\Windows\system32\ntdsutil.exe: semantic database analysis
semantic checker: go
Fixup mode is turned off
......Done.
Writing summary into log file dsdit.dmp.0
SDs scanned: 117
Records scanned: 4456
Processing records..Done. Elapsed time 1 seconds.
semantic checker: