

# Active Directory Domain Report

demo2012r2.int



# Table of Contents

General Information	
Operations Masters	6
Groups	
Access Control Assistance Operators	9
Account Operators	9
Administrators	9
Backup Operators	10
Certificate Service DCOM Access	10
Cryptographic Operators	10
Distributed COM Users	11
Event Log Readers	11
Guests	11
Hyper-V Administrators	12
IIS_IUSRS	12
Incoming Forest Trust Builders	12
Network Configuration Operators	13
Performance Log Users	13
Performance Monitor Users	13
Pre-Windows 2000 Compatible Access	14
Print Operators	14
RDS Endpoint Servers	14
RDS Management Servers	15
RDS Remote Access Servers	15
Remote Desktop Users	15
Remote Management Users	16
Replicator	16
Server Operators	16
Terminal Server License Servers	17
Users	17
Windows Authorization Access Group	17

Schema Configuration	
Schema Classes	19
Group Policy Objects	
Default Domain Controllers Policy	28
Default Domain Policy	29
Sample GPO	30
Trusts	
Purchasing.demo2012r2.int	32
MANUFACTURING	33
contoso.com	34
Inter-Site Transports	
IP	36
DEFAULTIPSITELINK	37
Remote Site Links	38
Sample Bridge	39
SMTP	40
Sample Bridge	41
Sample SMTP link 2	42
SMTPTest	43
Sample SMTP bridge	44
Subnets	
Sites	
ContosoHQ	47
Domain Controllers	49
DEMO-2012R2-DC4	50
<automatically generated>	52
<automatically generated>	53
HQ	54
Domain Controllers	56
DEMO-2012R2-DC1	57
<automatically generated>	59
454d2609-2ca3-4f69-8147-709ce24ebf47	60
Purchasing	61

Domain Controllers	63
DEMO-2012R2-DC3	64
<automatically generated>	66
<automatically generated>	67
SalesOffice	68
Domain Controllers	70
DEMO-2012R2-DC2	71
DEMO-2012R2-DC1	74
RODC Connection (SYSVOL)	75
Version History	

# General Information

Active Directory is a centralized authentication and directory service based around standards such as the Lightweight Directory Access Protocol (LDAP) and Kerberos. It stores information about user accounts, groups, distribution lists as well as information for directory enabled applications such as Microsoft Exchange Server.

The forest acts as a security boundary for an organization and defines the scope of authority for administrators. By default, a forest contains a single domain, which is known as the forest root domain however additional domains can be created in the forest.

## General Information

Domain Name	demo2012r2.int
NetBIOS Name	DEMO2012R2
Domain SID	S-1-5-21-2086088546-3111580926-4218423029
Domain Functional Level	Windows Server 2012 R2
Forest Functional Level	Windows Server 2012 R2 Forest
Forest Name	demo2012r2.int
Root Domain SID	S-1-5-21-2086088546-3111580926-4218423029

## Active Directory Recycle Bin






Enabled	False
---------	-------

## Builtin Administrators Group

Name	Administrators
SAM Account Name	Administrators
Canonical Name	demo2012r2.int/Builtin/Administrators
Description	Administrators have complete and unrestricted access to the computer/domain
Group Scope	Built-In
Group Type	Security
GUID	efb24cf6-3d69-4fe8-aac7-9d70a5b0effb
SID	S-1-5-32-544
Members	DEMO2012R2\Domain Admins DEMO2012R2\Enterprise Admins DEMO2012R2\Administrator

# Operations Masters






Active Directory is a multi-master system where each domain controller has autonomy for read and write operations there are however five special Flexible Single Master Operation Roles (FSMO) which must be assigned to specific domain controllers. All roles can be assigned to a single domain controller or can be distributed between domain controllers.










Role	Server	Scope	Description
 PDC Emulator	DEMO-2012R2-DC1	Domain	The PDC emulator performs many roles including handling logon authentication failures on other domain controllers, account lockout and time synchronization with other domain controllers in the domain.
 Infrastructure Master	DEMO-2012R2-DC1	Domain	The infrastructure master ensures that cross-domain object references are correctly updated. When the Recycle Bin optional feature is enabled, every domain controller is responsible for updating its cross-domain object references in the event that the referenced object is moved, renamed, or deleted. In this case, there are no tasks associated with the infrastructure master role, and it is not important which domain controller owns the infrastructure master role.
 RID Master	DEMO-2012R2-DC1	Domain	The RID master role owner is the single domain controller responsible for processing relative ID (RID) pool requests from all DCs within a given domain. RIDs are used to ensure that each object's security identifier (SID) is unique within the domain. The RID master is also responsible for moving an object from one domain to another during an inter-domain object move.
 Domain Naming Master	DEMO-2012R2-DC1	Forest	The Domain Naming master role owner is the domain controller responsible for making changes to the forest-wide domain name space for example adding a child domain to the forest root.
 Schema Master	DEMO-2012R2-DC1	Forest	The Schema Master FSMO role owner is the domain controller responsible for and the only server in the forest capable of, performing updates to the directory schema.

# Groups

A group is a collection of user and computer accounts, contacts and other groups that can be managed as a single unit. Users and computers that belong to a particular group are referred to as group members. Using groups can simplify administration by assigning a common set of permissions and rights to many accounts at once, rather than assigning permissions and rights to each account individually.

Only built-in security groups were scanned.

Name	Type	Description
 Access Control Assistance Operators	Built-In Security Group	Members of this group can remotely query authorization attributes and permissions for resources on this computer.
 Account Operators	Built-In Security Group	Members can administer domain user and group accounts
 Administrators	Built-In Security Group	Administrators have complete and unrestricted access to the computer/domain
 Backup Operators	Built-In Security Group	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
 Certificate Service DCOM Access	Built-In Security Group	Members of this group are allowed to connect to Certification Authorities in the enterprise
 Cryptographic Operators	Built-In Security Group	Members are authorized to perform cryptographic operations.
 Distributed COM Users	Built-In Security Group	Members are allowed to launch, activate and use Distributed COM objects on this machine.
 Event Log Readers	Built-In Security Group	Members of this group can read event logs from local machine
 Guests	Built-In Security Group	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
 Hyper-V Administrators	Built-In Security Group	Members of this group have complete and unrestricted access to all features of Hyper-V.
 IIS_IUSRS	Built-In Security Group	Built-in group used by Internet Information Services.
 Incoming Forest Trust Builders	Built-In Security Group	Members of this group can create incoming, one-way trusts to this forest
 Network Configuration Operators	Built-In Security Group	Members in this group can have some administrative privileges to manage configuration of networking features
 Performance Log Users	Built-In Security Group	Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer
 Performance Monitor Users	Built-In Security Group	Members of this group can access performance counter data locally and remotely
 Pre-Windows 2000 Compatible Access	Built-In Security Group	A backward compatibility group which allows read access on all users and groups in the domain
 Print Operators	Built-In Security Group	Members can administer printers installed on domain controllers
 RDS Endpoint Servers	Built-In Security Group	Servers in this group run virtual machines and host sessions where users RemoteApp programs and personal virtual desktops run. This group needs to be

		populated on servers running RD Connection Broker. RD Session Host servers and RD Virtualization Host servers used in the deployment need to be in this group.
 RDS Management Servers	Built-In Security Group	Servers in this group can perform routine administrative actions on servers running Remote Desktop Services. This group needs to be populated on all servers in a Remote Desktop Services deployment. The servers running the RDS Central Management service must be included in this group.
 RDS Remote Access Servers	Built-In Security Group	Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. In Internet-facing deployments, these servers are typically deployed in an edge network. This group needs to be populated on servers running RD Connection Broker, RD Gateway servers and RD Web Access servers used in the deployment need to be in this group.
 Remote Desktop Users	Built-In Security Group	Members in this group are granted the right to logon remotely
 Remote Management Users	Built-In Security Group	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.
 Replicator	Built-In Security Group	Supports file replication in a domain
 Server Operators	Built-In Security Group	Members can administer domain servers
 Terminal Server License Servers	Built-In Security Group	Members of this group can update user accounts in Active Directory with information about license issuance, for the purpose of tracking and reporting TS Per User CAL usage
 Users	Built-In Security Group	Users are prevented from making accidental or intentional system-wide changes and can run most applications
 Windows Authorization Access Group	Built-In Security Group	Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects



# Access Control Assistance Operators

## Group Details

Name	Access Control Assistance Operators
SAM Account Name	Access Control Assistance Operators
Canonical Name	demo2012r2.int/Builtin/Access Control Assistance Operators
Description	Members of this group can remotely query authorization attributes and permissions for resources on this computer.
Group Scope	Built-In
Group Type	Security
GUID	362658ad-43ab-452f-b4ae-951807664c4b
SID	S-1-5-32-579
Members	

# Account Operators

## Group Details

Name	Account Operators
SAM Account Name	Account Operators
Canonical Name	demo2012r2.int/Builtin/Account Operators
Description	Members can administer domain user and group accounts
Group Scope	Built-In
Group Type	Security
GUID	3eb2723f-471b-4de9-af04-ea0a10a45a20
SID	S-1-5-32-548
Members	

# Administrators

## Group Details

Name	Administrators
SAM Account Name	Administrators
Canonical Name	demo2012r2.int/Builtin/Administrators
Description	Administrators have complete and unrestricted access to the computer/domain
Group Scope	Built-In
Group Type	Security
GUID	efb24cf6-3d69-4fe8-aac7-9d70a5b0effb
SID	S-1-5-32-544
Members	DEMO2012R2\Domain Admins DEMO2012R2\Enterprise Admins DEMO2012R2\Administrator

# Backup Operators

## Group Details

Name	Backup Operators
SAM Account Name	Backup Operators
Canonical Name	demo2012r2.int/Builtin/Backup Operators
Description	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Group Scope	Built-In
Group Type	Security
GUID	df0dacf1-84df-42b3-97c3-ac72ba77e7ae
SID	S-1-5-32-551
Members	

# Certificate Service DCOM Access

## Group Details

Name	Certificate Service DCOM Access
SAM Account Name	Certificate Service DCOM Access
Canonical Name	demo2012r2.int/Builtin/Certificate Service DCOM Access
Description	Members of this group are allowed to connect to Certification Authorities in the enterprise
Group Scope	Built-In
Group Type	Security
GUID	80085e87-0446-4b33-8ffa-c8a7b205c7ad
SID	S-1-5-32-574
Members	

# Cryptographic Operators

## Group Details

Name	Cryptographic Operators
SAM Account Name	Cryptographic Operators
Canonical Name	demo2012r2.int/Builtin/Cryptographic Operators
Description	Members are authorized to perform cryptographic operations.
Group Scope	Built-In
Group Type	Security
GUID	bf5ebb18-50a3-44bd-bc91-7ef0d2aa6877
SID	S-1-5-32-569
Members	

## Distributed COM Users

### Group Details

Name	Distributed COM Users
SAM Account Name	Distributed COM Users
Canonical Name	demo2012r2.int/Builtin/Distributed COM Users
Description	Members are allowed to launch, activate and use Distributed COM objects on this machine.
Group Scope	Built-In
Group Type	Security
GUID	093ca397-4b0a-4cad-86e3-ba22305e99df
SID	S-1-5-32-562
Members	

## Event Log Readers

### Group Details

Name	Event Log Readers
SAM Account Name	Event Log Readers
Canonical Name	demo2012r2.int/Builtin/Event Log Readers
Description	Members of this group can read event logs from local machine
Group Scope	Built-In
Group Type	Security
GUID	8fe1fb76-f606-4cee-8afe-a878656e97c6
SID	S-1-5-32-573
Members	

## Guests

### Group Details

Name	Guests
SAM Account Name	Guests
Canonical Name	demo2012r2.int/Builtin/Guests
Description	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
Group Scope	Built-In
Group Type	Security
GUID	df40742b-64f0-4bc5-bfd9-004289021db2
SID	S-1-5-32-546
Members	DEMO2012R2\Domain Guests DEMO2012R2\Guest

# Hyper-V Administrators

## Group Details

Name	Hyper-V Administrators
SAM Account Name	Hyper-V Administrators
Canonical Name	demo2012r2.int/Builtin/Hyper-V Administrators
Description	Members of this group have complete and unrestricted access to all features of Hyper-V.
Group Scope	Built-In
Group Type	Security
GUID	c2fd337d-7579-4f87-a651-560d4101c95b
SID	S-1-5-32-578
Members	

# IIS\_IUSRS

## Group Details

Name	IIS_IUSRS
SAM Account Name	IIS_IUSRS
Canonical Name	demo2012r2.int/Builtin/IIS_IUSRS
Description	Built-in group used by Internet Information Services.
Group Scope	Built-In
Group Type	Security
GUID	3b2a5f92-140c-48ca-a358-792cdb5c11e
SID	S-1-5-32-568
Members	NT AUTHORITY\IUSR

# Incoming Forest Trust Builders

## Group Details

Name	Incoming Forest Trust Builders
SAM Account Name	Incoming Forest Trust Builders
Canonical Name	demo2012r2.int/Builtin/Incoming Forest Trust Builders
Description	Members of this group can create incoming, one-way trusts to this forest
Group Scope	Built-In
Group Type	Security
GUID	9503fca5-6f04-4744-b14b-d6ab221d89c7
SID	S-1-5-32-557
Members	

# Network Configuration Operators

## Group Details

Name	Network Configuration Operators
SAM Account Name	Network Configuration Operators
Canonical Name	demo2012r2.int/Builtin/Network Configuration Operators
Description	Members in this group can have some administrative privileges to manage configuration of networking features
Group Scope	Built-In
Group Type	Security
GUID	a7dfc41b-5ef8-4cc2-b3eb-ccc2f5459b8a
SID	S-1-5-32-556
Members	

# Performance Log Users

## Group Details

Name	Performance Log Users
SAM Account Name	Performance Log Users
Canonical Name	demo2012r2.int/Builtin/Performance Log Users
Description	Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer
Group Scope	Built-In
Group Type	Security
GUID	01e10ceb-85e2-4ede-a3e2-10fe2195a4c9
SID	S-1-5-32-559
Members	

# Performance Monitor Users

## Group Details

Name	Performance Monitor Users
SAM Account Name	Performance Monitor Users
Canonical Name	demo2012r2.int/Builtin/Performance Monitor Users
Description	Members of this group can access performance counter data locally and remotely
Group Scope	Built-In
Group Type	Security
GUID	283ec0df-e1ef-4cce-b1aa-10aee0f337ac
SID	S-1-5-32-558
Members	

# Pre-Windows 2000 Compatible Access

## Group Details

Name	Pre-Windows 2000 Compatible Access
SAM Account Name	Pre-Windows 2000 Compatible Access
Canonical Name	demo2012r2.int/Builtin/Pre-Windows 2000 Compatible Access
Description	A backward compatibility group which allows read access on all users and groups in the domain
Group Scope	Built-In
Group Type	Security
GUID	dfd72f7e-44cb-4f99-ba62-e18d1277c833
SID	S-1-5-32-554
Members	NT AUTHORITY\Authenticated Users

# Print Operators

## Group Details

Name	Print Operators
SAM Account Name	Print Operators
Canonical Name	demo2012r2.int/Builtin/Print Operators
Description	Members can administer printers installed on domain controllers
Group Scope	Built-In
Group Type	Security
GUID	2dfae24c-dc19-4aa8-8aac-bee98e39e3dd
SID	S-1-5-32-550
Members	

# RDS Endpoint Servers

## Group Details

Name	RDS Endpoint Servers
SAM Account Name	RDS Endpoint Servers
Canonical Name	demo2012r2.int/Builtin/RDS Endpoint Servers
Description	Servers in this group run virtual machines and host sessions where users RemoteApp programs and personal virtual desktops run. This group needs to be populated on servers running RD Connection Broker. RD Session Host servers and RD Virtualization Host servers used in the deployment need to be in this group.
Group Scope	Built-In
Group Type	Security
GUID	1cfa747d-1305-4c8f-8d76-85ae27ea745e
SID	S-1-5-32-576
Members	

## RDS Management Servers

### Group Details

Name	RDS Management Servers
SAM Account Name	RDS Management Servers
Canonical Name	demo2012r2.int/BuiltIn/RDS Management Servers
Description	Servers in this group can perform routine administrative actions on servers running Remote Desktop Services. This group needs to be populated on all servers in a Remote Desktop Services deployment. The servers running the RDS Central Management service must be included in this group.
Group Scope	Built-In
Group Type	Security
GUID	9488c645-4c26-4ea9-b451-b0c53790eaa7
SID	S-1-5-32-577
Members	

## RDS Remote Access Servers

### Group Details

Name	RDS Remote Access Servers
SAM Account Name	RDS Remote Access Servers
Canonical Name	demo2012r2.int/BuiltIn/RDS Remote Access Servers
Description	Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. In Internet-facing deployments, these servers are typically deployed in an edge network. This group needs to be populated on servers running RD Connection Broker. RD Gateway servers and RD Web Access servers used in the deployment need to be in this group.
Group Scope	Built-In
Group Type	Security
GUID	d822512b-f2d0-4fab-8d9d-983435f133e3
SID	S-1-5-32-575
Members	

## Remote Desktop Users

### Group Details

Name	Remote Desktop Users
SAM Account Name	Remote Desktop Users
Canonical Name	demo2012r2.int/BuiltIn/Remote Desktop Users
Description	Members in this group are granted the right to logon remotely
Group Scope	Built-In
Group Type	Security
GUID	7e2d4748-070a-483b-8153-9707ebaf5b6b
SID	S-1-5-32-555
Members	

# Remote Management Users

## Group Details

Name	Remote Management Users
SAM Account Name	Remote Management Users
Canonical Name	demo2012r2.int/Builtin/Remote Management Users
Description	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.
Group Scope	Built-In
Group Type	Security
GUID	57e643eb-538e-4fe4-b0c2-a10141fdde02
SID	S-1-5-32-580
Members	

# Replicator

## Group Details

Name	Replicator
SAM Account Name	Replicator
Canonical Name	demo2012r2.int/Builtin/Replicator
Description	Supports file replication in a domain
Group Scope	Built-In
Group Type	Security
GUID	f13da6fe-b81a-4d81-9a76-b0e1fe441145
SID	S-1-5-32-552
Members	

# Server Operators

## Group Details

Name	Server Operators
SAM Account Name	Server Operators
Canonical Name	demo2012r2.int/Builtin/Server Operators
Description	Members can administer domain servers
Group Scope	Built-In
Group Type	Security
GUID	1d823a7d-2552-45dd-962f-c289c3a3030e
SID	S-1-5-32-549
Members	



# Terminal Server License Servers

## Group Details

Name	Terminal Server License Servers
SAM Account Name	Terminal Server License Servers
Canonical Name	demo2012r2.int/Builtin/Terminal Server License Servers
Description	Members of this group can update user accounts in Active Directory with information about license issuance, for the purpose of tracking and reporting TS Per User CAL usage
Group Scope	Built-In
Group Type	Security
GUID	133f20e9-9205-471e-8f4e-19802975235a
SID	S-1-5-32-561
Members	

# Users

## Group Details

Name	Users
SAM Account Name	Users
Canonical Name	demo2012r2.int/Builtin/Users
Description	Users are prevented from making accidental or intentional system-wide changes and can run most applications
Group Scope	Built-In
Group Type	Security
GUID	1d677a1e-2b17-4595-b6ca-967c06d75216
SID	S-1-5-32-545
Members	DEMO2012R2\Domain Users NT AUTHORITY\Authenticated Users NT AUTHORITY\INTERACTIVE

# Windows Authorization Access Group

## Group Details

Name	Windows Authorization Access Group
SAM Account Name	Windows Authorization Access Group
Canonical Name	demo2012r2.int/Builtin/Windows Authorization Access Group
Description	Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects
Group Scope	Built-In
Group Type	Security
GUID	b9a5d448-744b-47a1-9ed4-8dfa642cede2
SID	S-1-5-32-560
Members	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

# Schema Configuration

The Active Directory schema defines all of the objects and attributes that the directory service uses to store data. It is replicated to all domain controllers in all domains in the forest.



## Schema Configuration

Distinguished Name	CN=Schema,CN=Configuration,DC=demo2012r2,DC=int
Schema Version	69
Schema Master	DEMO-2012R2-DC1

# Schema Classes




Each object in Active Directory is (for example a computer object) an instance of an object class defined in the schema. The class contains attributes (such as description) which determine what information can be stored within it.

Name	Type	Status	Description
 account	Structural	Active	The account object class is used to define entries representing computer accounts.
 aCSPolicy	Structural	Active	ACS-Policy
 aCSResourceLimits	Structural	Active	ACS-Resource-Limits
 aCSSubnet	Structural	Active	ACS-Subnet
 addressBookContainer	Structural	Active	Address-Book-Container
 addressTemplate	Structural	Active	Address-Template
 applicationEntity	Structural	Active	Application-Entity
 applicationProcess	Structural	Active	Application-Process
 applicationSettings	Abstract	Active	Application-Settings
 applicationSiteSettings	Abstract	Active	Application-Site-Settings
 applicationVersion	Structural	Active	Stores versioning information for an application and its schema.
 attributeSchema	Structural	Active	Attribute-Schema
 bootableDevice	Auxiliary	Active	A device with boot parameters
 builtinDomain	Structural	Active	Builtin-Domain
 categoryRegistration	Structural	Active	Category-Registration
 certificationAuthority	Type 88	Active	Certification-Authority
 classRegistration	Structural	Active	Class-Registration
 classSchema	Structural	Active	Class-Schema
 classStore	Structural	Active	Class-Store
 comConnectionPoint	Structural	Active	Com-Connection-Point
 computer	Structural	Active	Computer
 configuration	Structural	Active	Configuration
 connectionPoint	Abstract	Active	Connection-Point
 contact	Structural	Active	Contact
 container	Structural	Active	Container
 controlAccessRight	Structural	Active	Control-Access-Right
 country	Type 88	Active	Country
 cRLDistributionPoint	Structural	Active	CRL-Distribution-Point
 crossRef	Structural	Active	Cross-Ref
 crossRefContainer	Structural	Active	Cross-Ref-Container
 device	Type 88	Active	Device
 dfsConfiguration	Structural	Active	Dfs-Configuration

 dHCPClass	Structural	Active	DHCP-Class
 displaySpecifier	Structural	Active	Display-Specifier
 displayTemplate	Structural	Active	Display-Template
 dMD	Structural	Active	DMD
 dnsNode	Structural	Active	Dns-Node
 dnsZone	Structural	Active	Dns-Zone
 document	Structural	Active	The document object class is used to define entries which represent documents.
 documentSeries	Structural	Active	The documentSeries object class is used to define an entry which represents a series of documents.
 domain	Abstract	Active	Domain
 domainDNS	Structural	Active	Domain-DNS
 domainPolicy	Structural	Active	Domain-Policy
 domainRelatedObject	Auxiliary	Active	The domainRelatedObject object class is used to define an entry which represents a series of documents.
 dSA	Structural	Active	DSA
 dSUISettings	Structural	Active	DS-UI-Settings
 dynamicObject	Auxiliary	Active	Dynamic-Object
 fileLinkTracking	Structural	Active	File-Link-Tracking
 fileLinkTrackingEntry	Structural	Active	File-Link-Tracking-Entry
 foreignSecurityPrincipal	Structural	Active	Foreign-Security-Principal
 friendlyCountry	Structural	Active	The friendlyCountry object class is used to define country entries in the DIT.
 fTDfs	Structural	Active	FT-Dfs
 group	Structural	Active	Group
 groupOfNames	Type 88	Active	Group-Of-Names
 groupOfUniqueNames	Structural	Active	Defines the entries for a group of unique names.
 groupPolicyContainer	Structural	Active	Group-Policy-Container
 ieee802Device	Auxiliary	Active	A device with a MAC address
 indexServerCatalog	Structural	Active	Index-Server-Catalog
 inetOrgPerson	Structural	Active	Represents people who are associated with an organization in some way.
 infrastructureUpdate	Structural	Active	Infrastructure-Update
 intellimirrorGroup	Structural	Active	Intellimirror-Group
 intellimirrorSCP	Structural	Active	Intellimirror-SCP
 interSiteTransport	Structural	Active	Inter-Site-Transport
 interSiteTransportContainer	Structural	Active	Inter-Site-Transport-Container
 ipHost	Auxiliary	Active	Abstraction of a host, an IP device.
 ipNetwork	Structural	Active	Abstraction of a network. The distinguished value of the cn attribute denotes the network's canonical name
 ipProtocol	Structural	Active	Abstraction of an IP protocol
 ipsecBase	Abstract	Active	Ipsec-Base
 ipsecFilter	Structural	Active	Ipsec-Filter

 ipsecISAKMPPolicy	Structural	Active	Ipssec-ISAKMP-Policy
 ipsecNegotiationPolicy	Structural	Active	Ipssec-Negotiation-Policy
 ipsecNFA	Structural	Active	Ipssec-NFA
 ipsecPolicy	Structural	Active	Ipssec-Policy
 ipService	Structural	Active	Abstraction of an Internet Protocol service.
 leaf	Abstract	Active	Leaf
 licensingSiteSettings	Structural	Active	Licensing-Site-Settings
 linkTrackObjectMoveTable	Structural	Active	Link-Track-Object-Move-Table
 linkTrackOMTEntry	Structural	Active	Link-Track-OMT-Entry
 linkTrackVolEntry	Structural	Active	Link-Track-Vol-Entry
 linkTrackVolumeTable	Structural	Active	Link-Track-Volume-Table
 locality	Structural	Active	Locality
 lostAndFound	Structural	Active	Lost-And-Found
 mailRecipient	Auxiliary	Active	Mail-Recipient
 meeting	Structural	Active	Meeting
 msAuthz-CentralAccessPolicies	Structural	Active	A container of this class can contain Central Access Policy objects.
 msAuthz-CentralAccessPolicy	Structural	Active	A class that defines Central Access Policy objects.
 msAuthz-CentralAccessRule	Structural	Active	A class that defines Central Access Rules used to construct a central access policy.
 msAuthz-CentralAccessRules	Structural	Active	A container of this class can contain Central Access Policy Entry objects.
 msCOM-Partition	Structural	Active	Partition class. Default = adminDisplayName
 msCOM-PartitionSet	Structural	Active	PartitionSet class. Default = adminDisplayName
 msDFS-DeletedLinkv2	Structural	Active	Deleted DFS Link in DFS namespace
 msDFS-Linkv2	Structural	Active	DFS Link in DFS namespace
 msDFS-NamespaceAnchor	Structural	Active	DFS namespace anchor
 msDFS-Namespavev2	Structural	Active	DFS namespace
 msDFSR-Connection	Structural	Active	Directional connection between two members
 msDFSR-Content	Structural	Active	Container for DFRS-ContentSet objects
 msDFSR-ContentSet	Structural	Active	DFSR Content Set
 msDFSR-GlobalSettings	Structural	Active	Global settings applicable to all replication group members
 msDFSR-LocalSettings	Structural	Active	DFSR settings applicable to local computer
 msDFSR-Member	Structural	Active	Replication group member
 msDFSR-ReplicationGroup	Structural	Active	Replication Group container
 msDFSR-Subscriber	Structural	Active	Represents local computer membership of a replication group
 msDFSR-Subscription	Structural	Active	Represents local computer participation of a content set
 msDFSR-Topology	Structural	Active	Container for objects that form the replication topology
 msDNS-ServerSettings	Structural	Active	A container for storing DNS server settings.
 msDS-App-Configuration	Structural	Active	Stores configuration parameters for an application.
 msDS-AppData	Structural	Active	Stores data that is to be used by an object. For example, profile information for a user object.














 msDS-AuthNPolicies	Structural	Active	A container of this class can contain authentication policy objects.
 msDS-AuthNPolicy	Structural	Active	An instance of this class defines authentication policy behaviors for assigned principals.
 msDS-AuthNPolicySilo	Structural	Active	An instance of this class defines authentication policies and related behaviors for assigned users, computers, and services.
 msDS-AuthNPolicySilos	Structural	Active	A container of this class can contain authentication policy silo objects.
 msDS-AzAdminManager	Structural	Active	Root of Authorization Policy store instance
 msDS-AzApplication	Structural	Active	Defines an installed instance of an application bound to a particular policy store.
 msDS-AzOperation	Structural	Active	Describes a particular operation supported by an application
 msDS-AzRole	Structural	Active	Defines a set of operations that can be performed by a particular set of users within a particular scope
 msDS-AzScope	Structural	Active	Describes a set of objects managed by an application
 msDS-AzTask	Structural	Active	Describes a set of operations
 msDS-ClaimsTransformationPolicies	Structural	Active	An object of this class holds the one set of Claims Transformation Policy for Cross-Forest Claims Transformation.
 msDS-ClaimsTransformationPolicyType	Structural	Active	An object of this class holds the one set of Claims Transformation Policy for Cross-Forest Claims Transformation.
 msDS-ClaimType	Structural	Active	An instance of this class holds the definition of a claim type that can be defined on security principals.
 msDS-ClaimTypePropertyBase	Abstract	Active	An abstract class that defines the base class for claim type or resource property classes.
 msDS-ClaimTypes	Structural	Active	A container of this class can contain claim type objects.
 msDS-CloudExtensions	Auxiliary	Active	A collection of attributes used to house arbitrary cloud-relevant strings.
 msDS-Device	Structural	Active	An object of this type represents a registered device.
 msDS-DeviceContainer	Structural	Active	A class for the container used to hold device objects.
 msDS-DeviceRegistrationService	Structural	Active	An object of this class holds the registration service configuration used for devices.
 msDS-DeviceRegistrationServiceContainer	Structural	Active	A class for the container used to house all enrollment services used for device registrations.
 msDS-GroupManagedServiceAccount	Structural	Active	The group managed service account class is used to create an account which can be shared by different computers to run Windows services.
 msDS-ManagedServiceAccount	Structural	Active	Service account class is used to create accounts that are used for running Windows services.
 msDS-OptionalFeature	Structural	Active	Configuration for an optional DS feature.
 msDS-PasswordSettings	Structural	Active	Password settings object for accounts
 msDS-PasswordSettingsContainer	Structural	Active	Container for password settings objects
 msDS-QuotaContainer	Structural	Active	A special container that holds all quota specifications for the directory database.
 msDS-QuotaControl	Structural	Active	A class used to represent quota specifications for the directory database.
 msDS-ResourceProperties	Structural	Active	A container of this class can contain resource properties.
 msDS-ResourceProperty	Structural	Active	An instance of this class holds the definition of a property on resources.
 msDS-ResourcePropertyList	Structural	Active	An object of this class contains a list of resource properties.
 msDS-ValueType	Structural	Active	An value type object holds value type information for a resource property.

 msExchConfigurationContainer	Structural	Active	ms-Exch-Configuration-Container
 msFVE-RecoveryInformation	Structural	Active	This class contains BitLocker recovery information including GUIDs, recovery passwords, and keys. Full Volume Encryption (FVE) was the pre-release name for BitLocker Drive Encryption.
 msieee80211-Policy	Structural	Active	class to store Wireless Network Policy Object
 msImaging-PostScanProcess	Structural	Active	Enterprise Scan Post Scan Process object.
 msImaging-PSPs	Structural	Active	Container for all Enterprise Scan Post Scan Process objects.
 msKds-ProvRootKey	Structural	Active	Root keys for the Group Key Distribution Service.
 msKds-ProvServerConfiguration	Structural	Active	Configuration for the Group Key Distribution Service.
 mSMQConfiguration	Structural	Active	MSMQ-Configuration
 msMQ-Custom-Recipient	Structural	Active	MSMQ-Custom-Recipient
 mSMQEnterpriseSettings	Structural	Active	MSMQ-Enterprise-Settings
 msMQ-Group	Structural	Active	MSMQ-Group
 mSMQMigratedUser	Structural	Active	MSMQ-Migrated-User
 mSMQQueue	Structural	Active	MSMQ-Queue
 mSMQSettings	Structural	Active	MSMQ-Settings
 mSMQSiteLink	Structural	Active	MSMQ-Site-Link
 ms-net-ieee-80211-GroupPolicy	Structural	Active	This class represents an 802.11 wireless network group policy object. This class contains identifiers and configuration data relevant to an 802.11 wireless network.
 ms-net-ieee-8023-GroupPolicy	Structural	Active	This class represents an 802.3 wired network group policy object. This class contains identifiers and configuration data relevant to an 802.3 wired network.
 msPKI-Enterprise-Oid	Structural	Active	ms-PKI-Enterprise-Oid
 msPKI-Key-Recovery-Agent	Structural	Active	ms-PKI-Key-Recovery-Agent
 msPKI-PrivateKeyRecoveryAgent	Structural	Active	ms-PKI-Private-Key-Recovery-Agent
 msPrint-ConnectionPolicy	Structural	Active	Pushed Printer Connection Policy1
 msSFU30DomainInfo	Structural	Active	Represents an internal data structure used by Server for NIS.
 msSFU30MailAliases	Structural	Active	represents UNIX mail file data
 msSFU30NetId	Structural	Active	stores the network ID
 msSFU30NetworkUser	Structural	Active	represents network file data
 msSFU30NISMapConfig	Structural	Active	represents an internal Data Structure used by Server for NIS
 msSPP-ActivationObject	Structural	Active	Activation Object used in Active Directory based activation
 msSPP-ActivationObjectsContainer	Structural	Active	Container for Activation Objects used by Active Directory based activation
 mS-SQL-OLAPCube	Structural	Active	MS-SQL-OLAPCube
 mS-SQL-OLAPDatabase	Structural	Active	MS-SQL-OLAPDatabase
 mS-SQL-OLAPServer	Structural	Active	MS-SQL-OLAPServer
 mS-SQL-SQLDatabase	Structural	Active	MS-SQL-SQLDatabase
 mS-SQL-SQLPublication	Structural	Active	MS-SQL-SQLPublication
 mS-SQL-SQLRepository	Structural	Active	MS-SQL-SQLRepository
 mS-SQL-SQLServer	Structural	Active	MS-SQL-SQLServer
 msTAPI-RtConference	Structural	Active	msTAPI-RtConference

 msTAPI-RtPerson	Structural	Active	msTAPI-RtPerson
 msTPM-InformationObject	Structural	Active	This class contains recovery information for a Trusted Platform Module (TPM) device.
 msTPM-InformationObjectsContainer	Structural	Active	Container for TPM objects.
 msWMI-IntRangeParam	Structural	Active	ms-WMI-IntRangeParam
 msWMI-IntSetParam	Structural	Active	ms-WMI-IntSetParam
 msWMI-MergeablePolicyTemplate	Structural	Active	ms-WMI-MergeablePolicyTemplate
 msWMI-ObjectEncoding	Structural	Active	ms-WMI-ObjectEncoding
 msWMI-PolicyTemplate	Structural	Active	ms-WMI-PolicyTemplate
 msWMI-PolicyType	Structural	Active	ms-WMI-PolicyType
 msWMI-RangeParam	Structural	Active	ms-WMI-RangeParam
 msWMI-RealRangeParam	Structural	Active	ms-WMI-RealRangeParam
 msWMI-Rule	Structural	Active	ms-WMI-Rule
 msWMI-ShadowObject	Structural	Active	ms-WMI-ShadowObject
 msWMI-SimplePolicyTemplate	Structural	Active	ms-WMI-SimplePolicyTemplate
 msWMI-Som	Structural	Active	ms-WMI-Som
 msWMI-StringSetParam	Structural	Active	ms-WMI-StringSetParam
 msWMI-UintRangeParam	Structural	Active	ms-WMI-UintRangeParam
 msWMI-UintSetParam	Structural	Active	ms-WMI-UintSetParam
 msWMI-UnknownRangeParam	Structural	Active	ms-WMI-UnknownRangeParam
 msWMI-WMIGPO	Structural	Active	ms-WMI-WMIGPO
 nisMap	Structural	Active	A generic abstraction of a nis map
 nisNetgroup	Structural	Active	Abstraction of a netgroup. May refer to other netgroups
 nisObject	Structural	Active	An entry in a NIS map
 nTDSConnection	Structural	Active	NTDS-Connection
 nTDSDSA	Structural	Active	NTDS-DSA
 nTDSDSARO	Structural	Active	A subclass of Directory Service Agent which is distinguished by its reduced privilege level.
 nTDSService	Structural	Active	NTDS-Service
 nTDSSiteSettings	Structural	Active	NTDS-Site-Settings
 nTFRSMember	Structural	Active	NTFRS-Member
 nTFRSReplicaSet	Structural	Active	NTFRS-Replica-Set
 nTFRSSettings	Structural	Active	NTFRS-Settings
 nTFRSSubscriber	Structural	Active	NTFRS-Subscriber
 nTFRSSubscriptions	Structural	Active	NTFRS-Subscriptions
 oncRpc	Structural	Active	Abstraction of an Open Network Computing (ONC) [RFC1057] Remote Procedure Call (RPC) binding
 organization	Structural	Active	Organization
 organizationalPerson	Type 88	Active	Organizational-Person
 organizationalRole	Structural	Active	Organizational-Role
 organizationalUnit	Structural	Active	Organizational-Unit






 packageRegistration	Structural	Active	Package-Registration
 person	Type 88	Active	Person
 physicalLocation	Structural	Active	Physical-Location
 pKICertificateTemplate	Structural	Active	PKI-Certificate-Template
 pKIEnrollmentService	Structural	Active	PKI-Enrollment-Service
 posixAccount	Auxiliary	Active	Abstraction of an account with posix attributes
 posixGroup	Auxiliary	Active	Abstraction of a group of accounts
 printQueue	Structural	Active	Print-Queue
 queryPolicy	Structural	Active	Query-Policy
 remoteMailRecipient	Structural	Active	Remote-Mail-Recipient
 remoteStorageServicePoint	Structural	Active	Remote-Storage-Service-Point
 residentialPerson	Structural	Active	Residential-Person
 rFC822LocalPart	Structural	Active	The rFC822LocalPart object class is used to define entries which represent the local part of mail addresses.
 rIDManager	Structural	Active	RID-Manager
 rIDSet	Structural	Active	RID-Set
 room	Structural	Active	The room object class is used to define entries representing rooms.
 rpcContainer	Structural	Active	Rpc-Container
 rpcEntry	Abstract	Active	rpc-Entry
 rpcGroup	Structural	Active	rpc-Group
 rpcProfile	Structural	Active	rpc-Profile
 rpcProfileElement	Structural	Active	rpc-Profile-Element
 rpcServer	Structural	Active	rpc-Server
 rpcServerElement	Structural	Active	rpc-Server-Element
 rRASAdministrationConnectionPoint	Structural	Active	RRAS-Administration-Connection-Point
 rRASAdministrationDictionary	Structural	Active	RRAS-Administration-Dictionary
 samDomain	Auxiliary	Active	Sam-Domain
 samDomainBase	Auxiliary	Active	Sam-Domain-Base
 samServer	Structural	Active	Sam-Server
 secret	Structural	Active	Secret
 securityObject	Abstract	Active	Security-Object
 securityPrincipal	Auxiliary	Active	Security-Principal
 server	Structural	Active	Server
 serversContainer	Structural	Active	Servers-Container
 serviceAdministrationPoint	Structural	Active	Service-Administration-Point
 serviceClass	Structural	Active	Service-Class
 serviceConnectionPoint	Structural	Active	Service-Connection-Point
 serviceInstance	Structural	Active	Service-Instance
 shadowAccount	Auxiliary	Active	Additional attributes for shadow passwords
 simpleSecurityObject	Auxiliary	Active	The simpleSecurityObject object class is used to allow an entry to

			have a userPassword attribute when an entry's principal object classes do not allow userPassword as an attribute type.
 site	Structural	Active	Site
 siteLink	Structural	Active	Site-Link
 siteLinkBridge	Structural	Active	Site-Link-Bridge
 sitesContainer	Structural	Active	Sites-Container
 storage	Structural	Active	Storage
 subnet	Structural	Active	Subnet
 subnetContainer	Structural	Active	Subnet-Container
 subSchema	Structural	Active	SubSchema
 top	Abstract	Active	Top
 trustedDomain	Structural	Active	Trusted-Domain
 typeLibrary	Structural	Active	Type-Library
 user	Structural	Active	User
 volume	Structural	Active	Volume

# Group Policy Objects

Group Policy is a technology incorporated into Active Directory that allows for centralized management of settings and simplistic software distribution to client computers and servers joined to the domain.

Settings are grouped into objects called Group Policy Objects (GPOs). GPOs are linked to an Active Directory domain, organizational units (OUs) and sites.

Name	Status	WMI Filter	Modified
 Default Domain Controllers Policy	Enabled	None	19/09/2013 17:36:14
 Default Domain Policy	Enabled	None	19/09/2013 17:40:10
 Sample GPO	Enabled	None	06/02/2014 10:22:16

# Default Domain Controllers Policy


## Default Domain Controllers Policy

Creation Time	19/09/2013 17:36:15
ID	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Modification Time	19/09/2013 17:36:14
Security Filtering	NT AUTHORITY\Authenticated Users
Status	Enabled
Computer Version	1 AD, 1 SYSVOL
User Version	0 AD, 0 SYSVOL
WMI Filter	None







## Linked Locations

Name	Enforced	Enabled
 demo2012r2.int/Domain Controllers	False	True

## Security

 Owner	DEMO2012R2\Domain Admins
--	--------------------------

## Permissions

Type	Principal	Access
 Allow	CREATOR OWNER	Create all child objects, Delete all child objects, Read, Write
 Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read
 Allow	NT AUTHORITY\Authenticated Users	Apply group policy, Read
 Allow	NT AUTHORITY\SYSTEM	Create all child objects, Delete all child objects, Read, Write
 Allow	DEMO2012R2\Domain Admins	Create all child objects, Delete all child objects, Read, Write
 Allow	DEMO2012R2\Enterprise Admins	Create all child objects, Delete all child objects, Read, Write

# Default Domain Policy


## Default Domain Policy

Creation Time	19/09/2013 17:36:15
ID	{31B2F340-016D-11D2-945F-00C04FB984F9}
Modification Time	19/09/2013 17:40:10
Security Filtering	NT AUTHORITY\Authenticated Users
Status	Enabled
Computer Version	3 AD, 3 SYSVOL
User Version	0 AD, 0 SYSVOL
WMI Filter	None







## Linked Locations

Name	Enforced	Enabled
 demo2012r2.int/	False	True

## Security

 Owner	DEMO2012R2\Domain Admins
--	--------------------------

## Permissions

Type	Principal	Access
 Allow	CREATOR OWNER	Create all child objects, Delete all child objects, Read, Write
 Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read
 Allow	NT AUTHORITY\Authenticated Users	Apply group policy, Read
 Allow	NT AUTHORITY\SYSTEM	Create all child objects, Delete all child objects, Read, Write
 Allow	DEMO2012R2\Domain Admins	Create all child objects, Delete all child objects, Read, Write
 Allow	DEMO2012R2\Enterprise Admins	Create all child objects, Delete all child objects, Read, Write

# Sample GPO


## Sample GPO

Creation Time	06/02/2014 09:21:26
ID	{7A760EFD-404B-40E6-96C9-FE6E0281528A}
Modification Time	06/02/2014 10:22:16
Security Filtering	NT AUTHORITY\Authenticated Users
Status	Enabled
Computer Version	2 AD, 2 SYSVOL
User Version	0 AD, 0 SYSVOL
WMI Filter	None







## Linked Locations

Name	Enforced	Enabled
 demo2012r2.int/Management	False	True

## Security

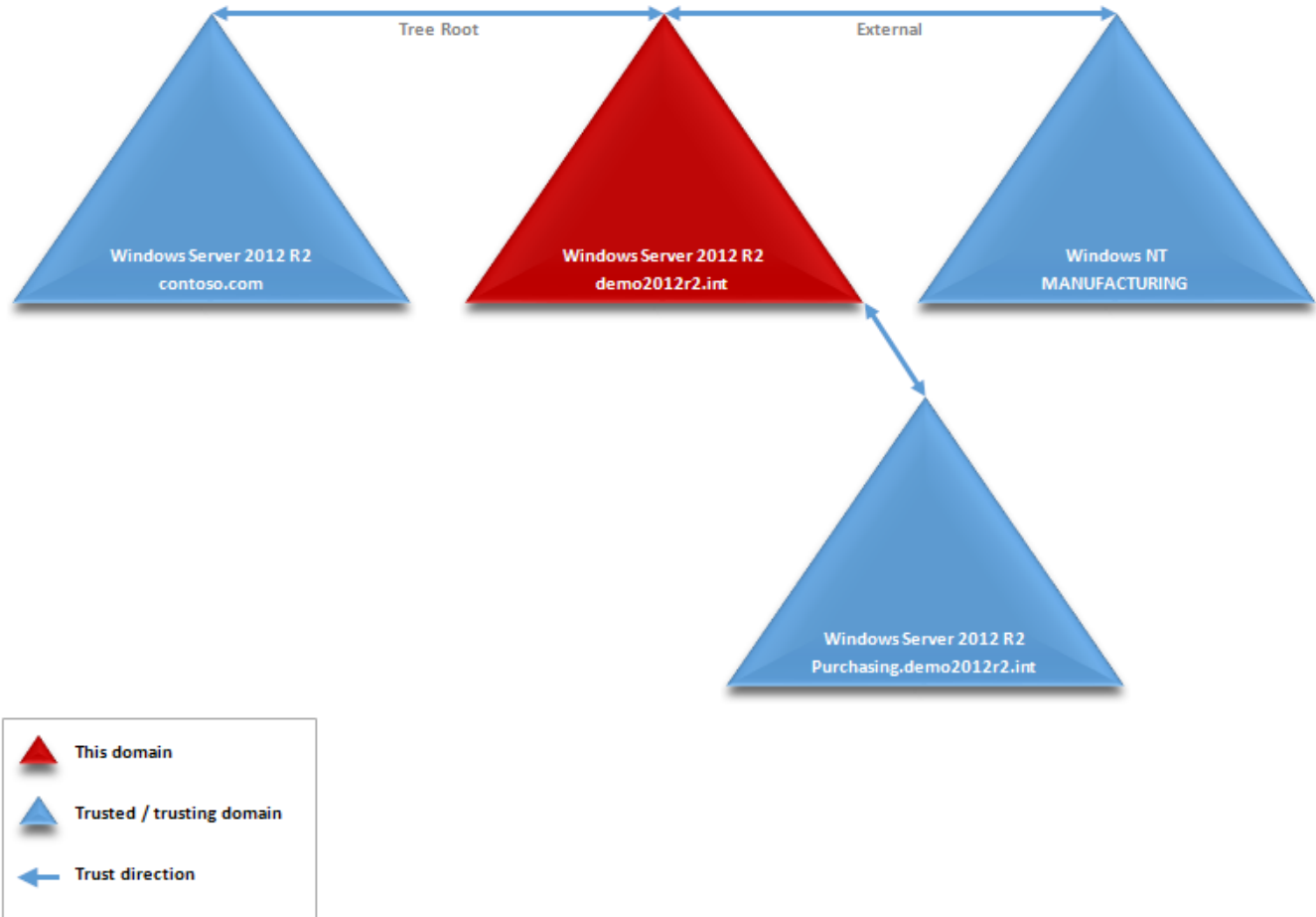
 Owner	DEMO2012R2\Domain Admins
--	--------------------------

## Permissions

Type	Principal	Access
 Allow	CREATOR OWNER	Create all child objects, Delete all child objects, Read, Write
 Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read
 Allow	NT AUTHORITY\Authenticated Users	Apply group policy, Read
 Allow	NT AUTHORITY\SYSTEM	Create all child objects, Delete all child objects, Read, Write
 Allow	DEMO2012R2\Domain Admins	Create all child objects, Delete all child objects, Read, Write
 Allow	DEMO2012R2\Enterprise Admins	Create all child objects, Delete all child objects, Read, Write

# Trusts

A trust is a relationship established between domains that enables users in one domain to be authenticated by a domain controller in the other domain.



## Trusts

Name	Type	Domain Functional Level	Transitive
Purchasing.demo2012r2.int	Child	Windows Server 2012 R2	True
MANUFACTURING	External	Windows NT	False
contoso.com	Tree Root	Windows Server 2012 R2	True

# Purchasing.demo2012r2.int

A parent and child trust is established when a new child domain is added to an existing domain tree. Authentication requests made from subordinate domains flow upward through their parent to the trusting domain.

---

## Purchasing.demo2012r2.int

Direction	Bidirectional
SID Filtering	False
Target Domain Mode	Windows Server 2012 R2
Target GUID	322e0a2d-fc8a-4254-98a8-3634075ebcdf
Target NetBIOS Name	PURCHASING
Target SID	S-1-5-21-1127135236-1044031741-4284996504
Transitive	True
Trust Type	Child



# MANUFACTURING

External trusts provide access to resources located on a Windows NT 4.0 domain or a domain located in a separate forest that is not joined by a forest trust.

---

## MANUFACTURING

Direction	Bidirectional
Selective Authentication	False
SID Filtering	True
Target Domain Mode	Windows NT
Target NetBIOS Name	MANUFACTURING
Target SID	S-1-5-21-1769940461-1463053390-309592939
Transitive	False
Trust Type	External

## contoso.com

A tree root trust relationship exists between root domains in the same forest. The root domains do not have a common DNS namespace. This trust relationship is established when a new tree root domain is added to a forest.

---

### contoso.com

Direction	Bidirectional
SID Filtering	False
Target Domain Mode	Windows Server 2012 R2
Target GUID	6c785c6c-2816-494b-a96e-75f8974ef53b
Target NetBIOS Name	CONTOSO
Target SID	S-1-5-21-3250448538-3074636085-3671305210
Transitive	True
Trust Type	Tree Root

# Inter-Site Transports




Inter-site transports all replication between sites using remote procedure call (RPC) over either the IP transport or the Simple Mail Transfer Protocol (SMTP) transport.

Name	Description
📁 IP	IP settings
📁 SMTP	

 IP

Description	IP settings
Bridge All Site Links	False
Ignore Schedules	False

 Site Links

Name	Type	Description	Cost	Replication Interval
 DEFAULTSITE LINK	Site Link	This is the default site link	101	210
 Remote Site Links	Site Link	This is used for remote sites	98	120
 Sample Bridge	Site Link Bridge	Sample site link bridge		

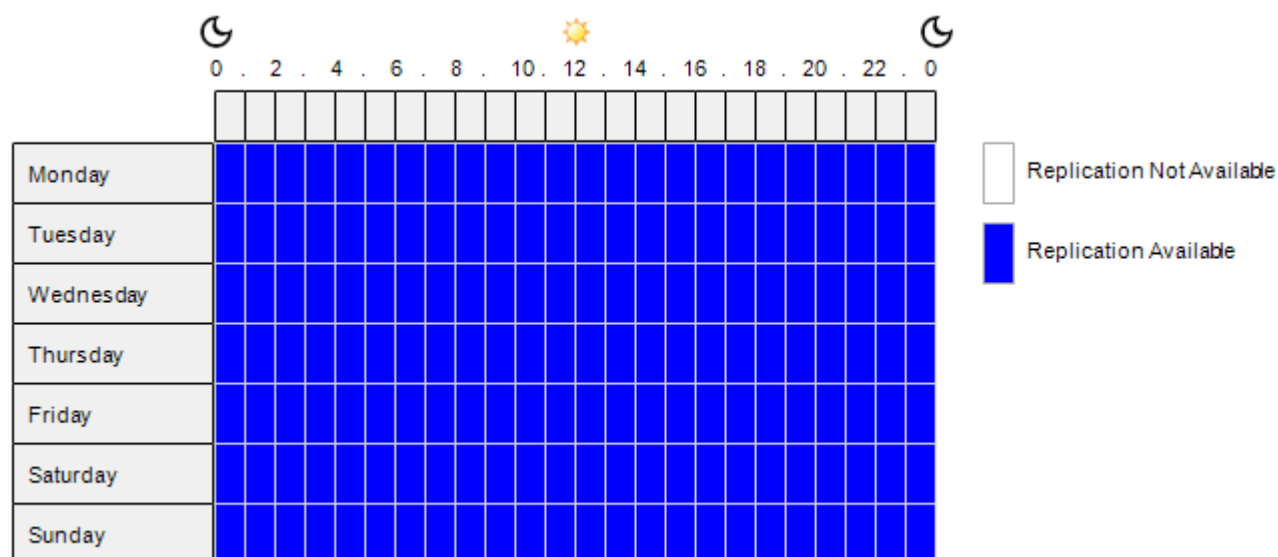
## DEFAULTIPSITELINK

Site links represent logical paths that the knowledge consistency checker (KCC) uses to establish a connection for Active Directory replication. A site link object represents a set of sites that can communicate at uniform cost through a specified inter-site transport.

### DEFAULTIPSITELINK

Description	This is the default site link
Transport Type	IP
Sites in link	ContosoHQ Purchasing SalesOffice HQ
Cost	101
Replication Interval	210

### Schedule



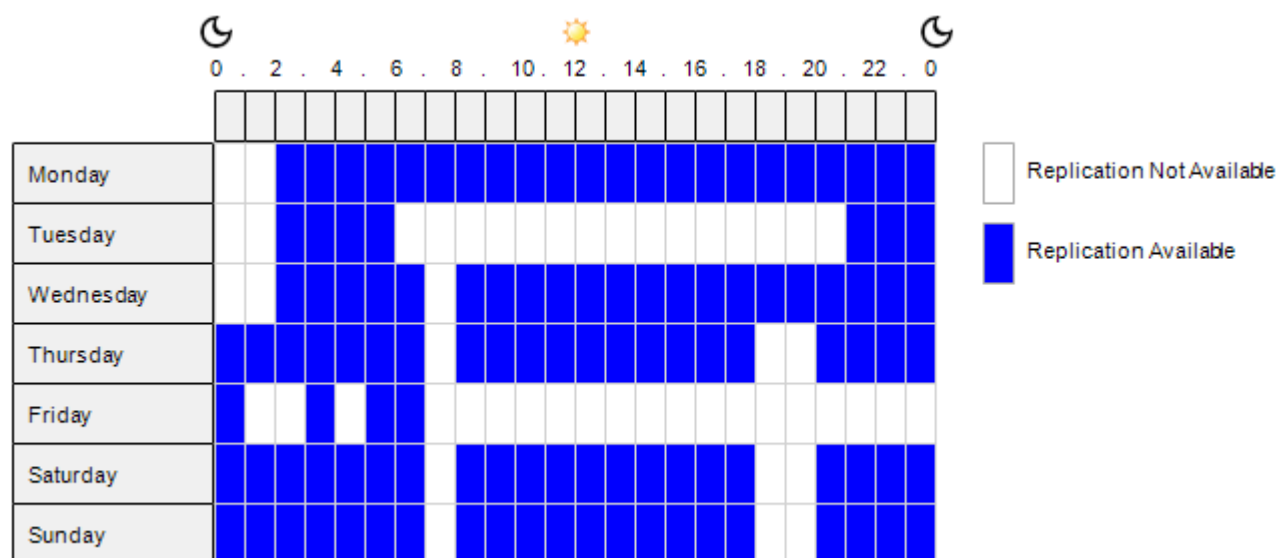
## Remote Site Links

Site links represent logical paths that the knowledge consistency checker (KCC) uses to establish a connection for Active Directory replication. A site link object represents a set of sites that can communicate at uniform cost through a specified inter-site transport.

### Remote Site Links

Description	This is used for remote sites
Transport Type	IP
Sites in link	SalesOffice HQ
Cost	98
Replication Interval	120

### Schedule



## Sample Bridge

A site link bridge represents a set of site links, all of whose sites can communicate by using a common transport. Site link bridges enable domain controllers that are not directly connected by means of a communication link to replicate with each other.

---

### **Sample Bridge**





Description	Sample site link bridge
Site Links	Remote Site Links DEFAULTIPSITELINK

# SMTP

## SMTP

Description	
Bridge All Site Links	False
Ignore Schedules	False

## Site Links

Name	Type	Description	Cost	Replication Interval
 Sample Bridge	Site Link		100	180
 Sample SMTP link 2	Site Link		100	180
 SMTPTest	Site Link	Sample SMTP connection	100	180
 Sample SMTP bridge	Site Link Bridge			



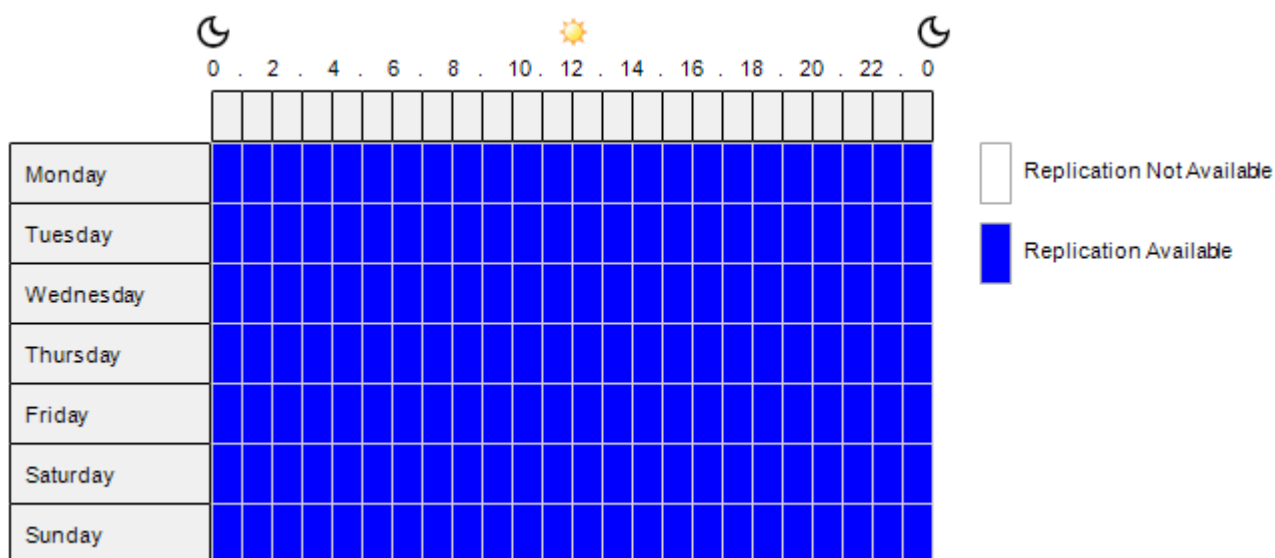
## Sample Bridge

Site links represent logical paths that the knowledge consistency checker (KCC) uses to establish a connection for Active Directory replication. A site link object represents a set of sites that can communicate at uniform cost through a specified inter-site transport.

### Sample Bridge

Description	
Transport Type	SMTP
Sites in link	SalesOffice HQ
Cost	100
Replication Interval	180

### Schedule



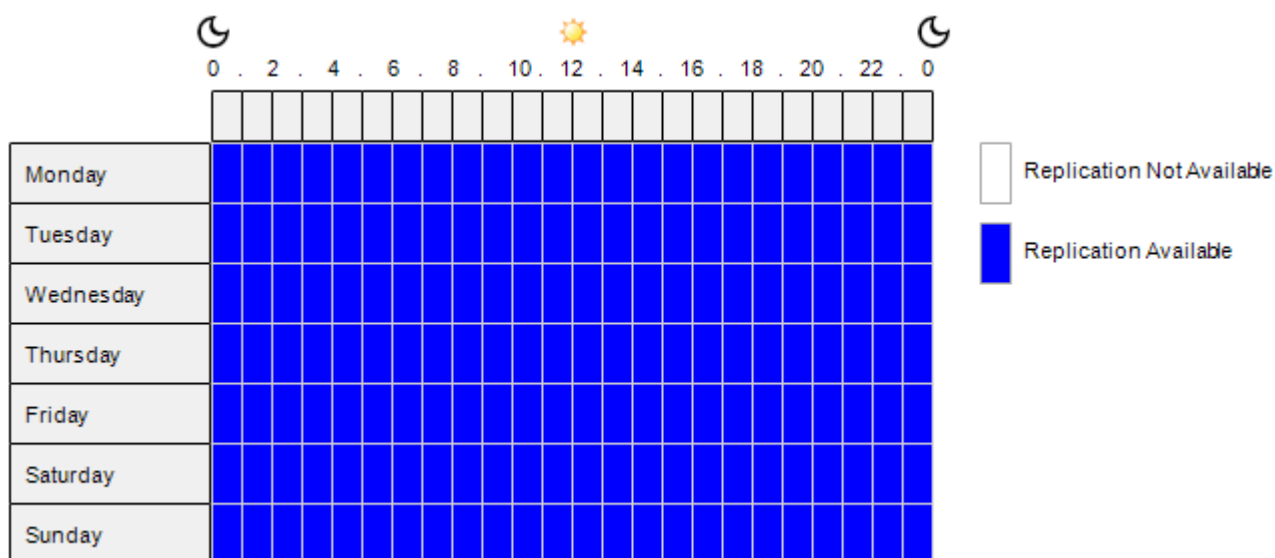
## Sample SMTP link 2

Site links represent logical paths that the knowledge consistency checker (KCC) uses to establish a connection for Active Directory replication. A site link object represents a set of sites that can communicate at uniform cost through a specified inter-site transport.

### Sample SMTP link 2

Description	
Transport Type	SMTP
Sites in link	SalesOffice HQ
Cost	100
Replication Interval	180

### Schedule



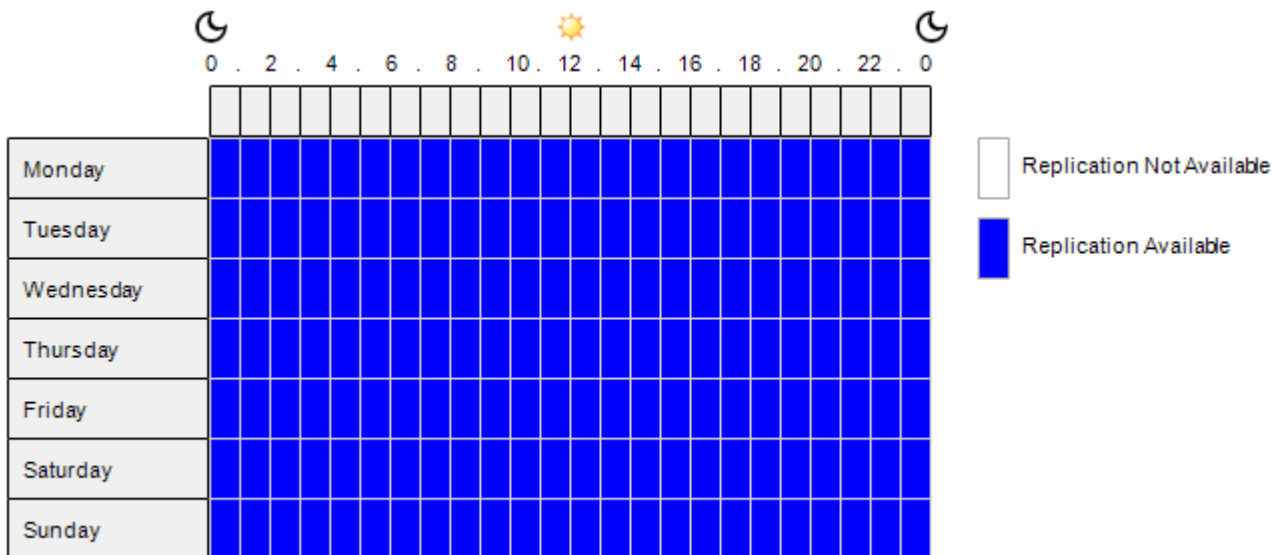
# SMTPTest

Site links represent logical paths that the knowledge consistency checker (KCC) uses to establish a connection for Active Directory replication. A site link object represents a set of sites that can communicate at uniform cost through a specified inter-site transport.

## SMTPTest

Description	Sample SMTP connection
Transport Type	SMTP
Sites in link	SalesOffice HQ
Cost	100
Replication Interval	180

## Schedule



## Sample SMTP bridge

A site link bridge represents a set of site links, all of whose sites can communicate by using a common transport. Site link bridges enable domain controllers that are not directly connected by means of a communication link to replicate with each other.

---

### **Sample SMTP bridge**

Description	
Site Links	Sample SMTP link 2 SMTPTest

# Subnets





Provides information about the subnets configured in the environment.

Name	Site	Location	Description
 192.168.89.0/24	HQ	Oxford	HQ subnet

# Sites

Active Directory sites represent the physical structure, or topology, of a network. Active Directory uses topology information, stored as site and site link objects in the directory, to build the most efficient replication topology and permits clients to locate the nearest resources such as domain controllers or distributed file system (DFS) servers.

A site consists of well-connected networks as determined by the subnet addresses assigned to that site.

Name	Location	Description
 ContosoHQ		
 HQ		
 Purchasing		
 SalesOffice	Sales Office	

# ContosoHQ

A site consists of well-connected networks as determined by the subnet addresses assigned to that site allowing clients to locate the nearest resources such as domain controllers or distributed file system (DFS) servers.

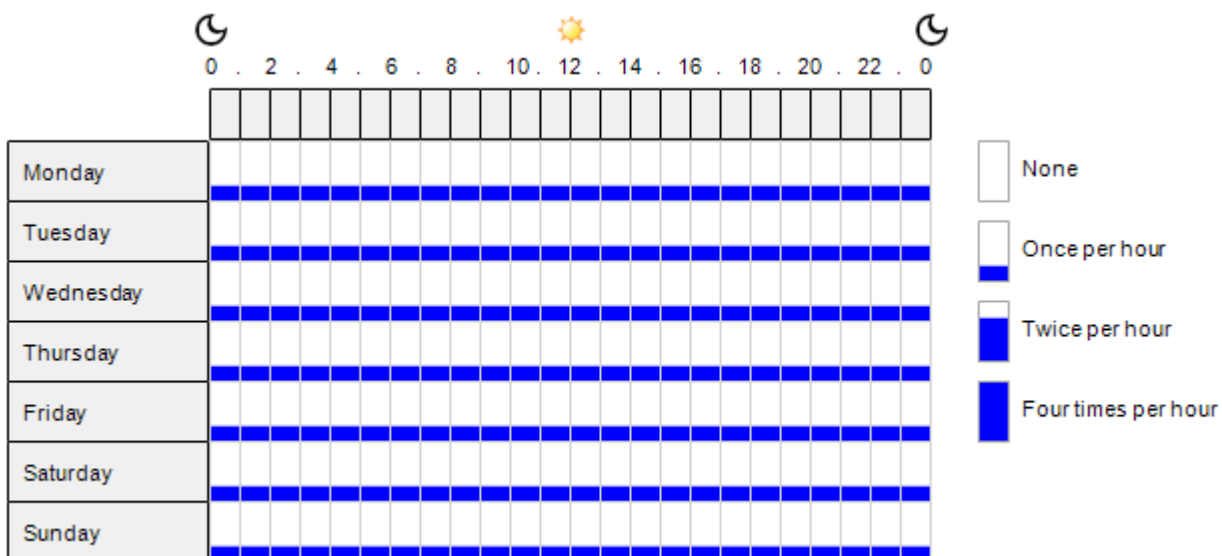
## ContosoHQ

Description	
Location	
Subnets	
Inter-Site Topology Generator	DEMO-2012R2-DC4
Inter-Site Topology Generator Site	ContosoHQ







## Universal Group Membership Caching

Enabled	False
Refresh Cache From	<Default>

## Replication Schedule



## Permissions


Type	Principal	Access
 Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read
 Allow	NT AUTHORITY\Authenticated Users	Read
 Allow	NT AUTHORITY\SYSTEM	Full Control
 Access Allowed Object	DEMO2012R2\Enterprise Read-only Domain Controllers	Self
 Allow	DEMO2012R2\Enterprise Admins	Full Control
 Allow	DEMO2012R2\Domain Admins	Create all child objects, Delete, ExtendedRight, Modify owner, Modify permissions, Read, Write



## Domain Controllers

An Active Directory domain controller authenticates and authorizes all users and computers in a Windows domain type network. Every domain controller supports multi-master operations allowing autonomy in the reading and writing information to the directory service with the exception of read-only domain controllers (RODCs) which allow only read-only access to the directory service.

RODC servers are useful in less secure physical environments such as a branch office.

Name	Domain	Bridgehead	Global Catalog	Server Type
 DEMO-2012R2-DC4	contoso.com		True	Domain Controller

## DEMO-2012R2-DC4

An Active Directory domain controller authenticates and authorizes all users and computers in a Windows domain type network

### DEMO-2012R2-DC4

Server Type	Domain Controller
DNS Hostname	DEMO-2012R2-DC4.contoso.com
Domain	contoso.com
Global Catalog	True
Description	
Bridgehead server transports	
Query Policy	
Created	19/09/2013 16:36:04
Last Modified	17/04/2014 13:15:33

### Host Information

Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Processors	Intel(R) Core(TM) i7-3537U CPU @ 2.00GHz
Serial Number	VMware-56 4d 01 13 a8 2a 19 9d-e4 f9 94 e4 6c eb 2f 26
Operating System Name	Microsoft Windows Server 2012 R2 Datacenter
Service Pack	[None Installed]



### Directory Service Installation Paths

Database Folder	C:\Windows\NTDS
Log Files Folder	C:\Windows\NTDS
SYSVOL Folder	C:\Windows\SYSVOL\sysvol

### Replicate From



Name	Site
 DEMO-2012R2-DC1	HQ
 DEMO-2012R2-DC3	Purchasing

### Replicate To

Name	Site
 DEMO-2012R2-DC1	
 DEMO-2012R2-DC3	

---

 **Replication Connections**

Name	From Server	From Site	Description
 <automatically generated>	DEMO-2012R2-DC1	HQ	
 <automatically generated>	DEMO-2012R2-DC3	Purchasing	

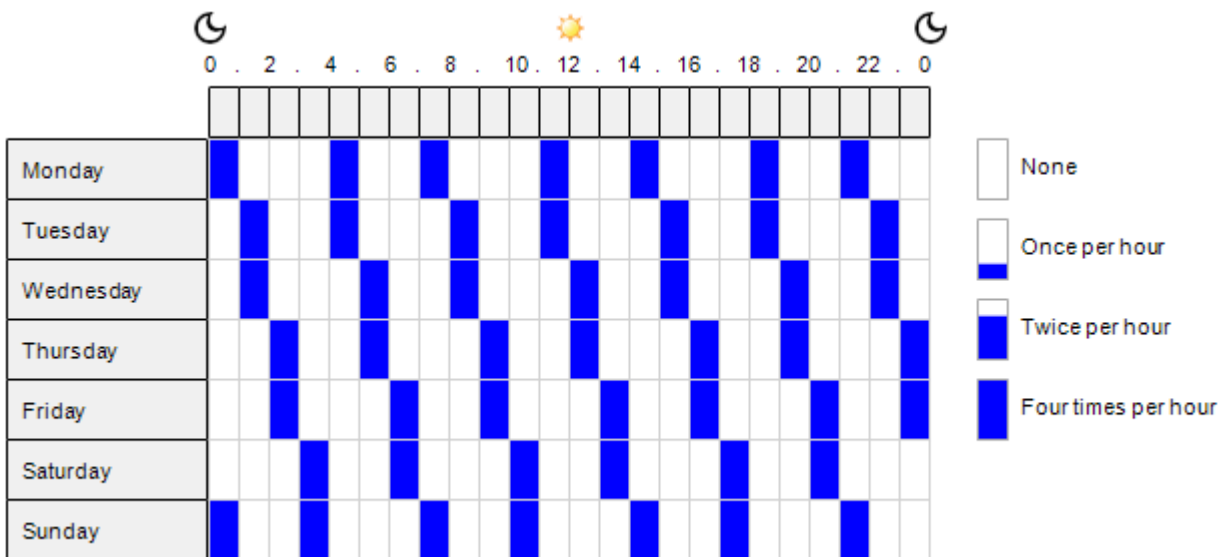
<automatically generated>

A connection object represents a replication connection from one domain controller to another and includes information about the transport type to use as well as the replication schedule.

### Connection Details

Description	
Transport Type	IP
Data Compression Enabled	True
Enabled	True
Generated By KCC	True
Notification Status	No Notification
Source Server	DEMO-2012R2-DC1
Source Site Name	HQ

### Schedule



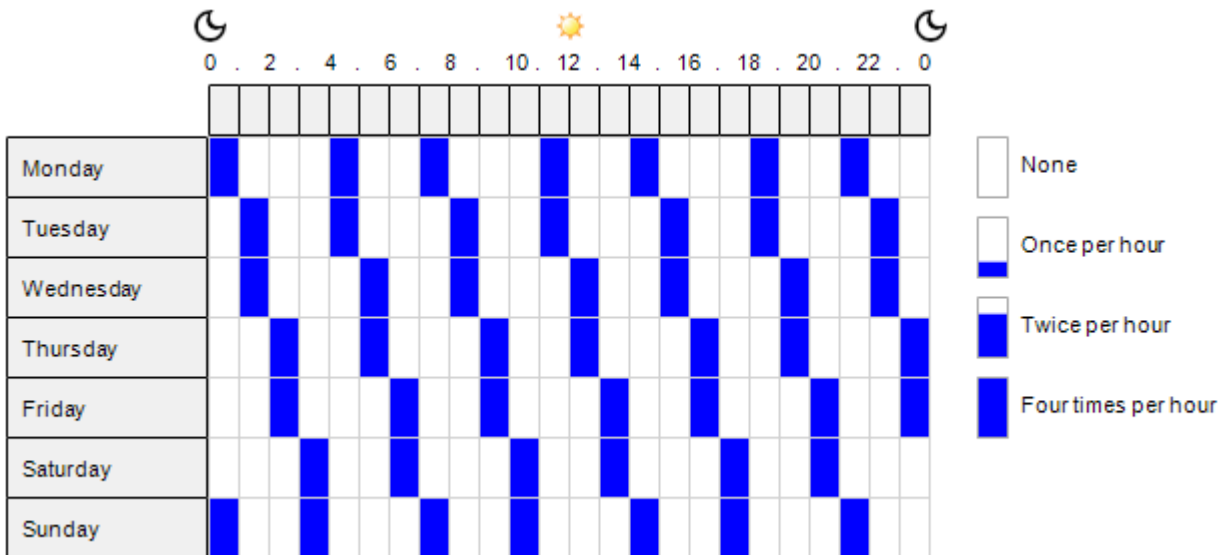
<automatically generated>

A connection object represents a replication connection from one domain controller to another and includes information about the transport type to use as well as the replication schedule.

### Connection Details

Description	
Transport Type	IP
Data Compression Enabled	True
Enabled	True
Generated By KCC	True
Notification Status	No Notification
Source Server	DEMO-2012R2-DC3
Source Site Name	Purchasing

### Schedule



# HQ

A site consists of well-connected networks as determined by the subnet addresses assigned to that site allowing clients to locate the nearest resources such as domain controllers or distributed file system (DFS) servers.

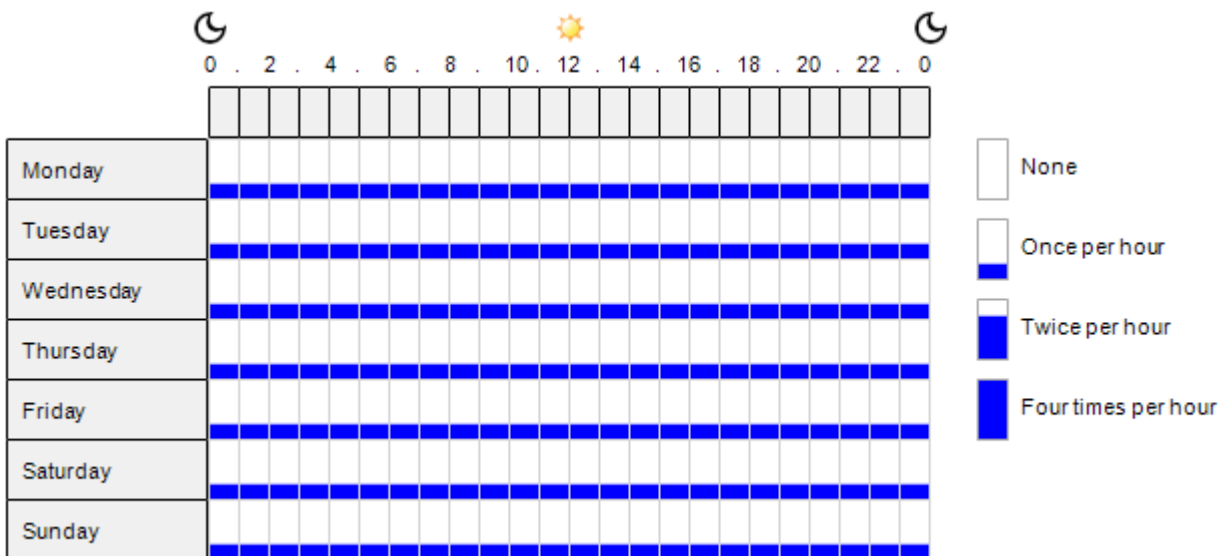
## HQ

Description	
Location	
Subnets	192.168.89.0/24
Inter-Site Topology Generator	DEMO-2012R2-DC1
Inter-Site Topology Generator Site	HQ







## Universal Group Membership Caching

Enabled	False
Refresh Cache From	<Default>

## Replication Schedule



## Permissions

Type	Principal	Access
 Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read
 Allow	NT AUTHORITY\Authenticated Users	Read
 Allow	NT AUTHORITY\SYSTEM	Full Control
 Access Allowed Object	DEMO2012R2\Enterprise Read-only Domain Controllers	Self
 Allow	DEMO2012R2\Enterprise Admins	Full Control
 Allow	DEMO2012R2\Domain Admins	Create all child objects, Delete, ExtendedRight, Modify owner, Modify permissions, Read, Write

## Domain Controllers

An Active Directory domain controller authenticates and authorizes all users and computers in a Windows domain type network. Every domain controller supports multi-master operations allowing autonomy in the reading and writing information to the directory service with the exception of read-only domain controllers (RODCs) which allow only read-only access to the directory service.

RODC servers are useful in less secure physical environments such as a branch office.

Name	Domain	Bridgehead	Global Catalog	Server Type
 DEMO-2012R2-DC1	demo2012r2.int		True	Domain Controller



## DEMO-2012R2-DC1

An Active Directory domain controller authenticates and authorizes all users and computers in a Windows domain type network

### DEMO-2012R2-DC1

Server Type	Domain Controller
DNS Hostname	DEMO-2012R2-DC1.demo2012r2.int
Domain	demo2012r2.int
Global Catalog	True
Description	
Bridgehead server transports	
Query Policy	
Created	19/09/2013 16:36:04
Last Modified	17/04/2014 13:15:33

### Host Information

Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Processors	Intel(R) Core(TM) i7-3537U CPU @ 2.00GHz
Serial Number	VMware-56 4d e8 35 a3 d0 53 e2-dd b2 ad b4 47 01 dd 14
Operating System Name	Microsoft Windows Server 2012 R2 Datacenter
Service Pack	[None Installed]




### Directory Service Installation Paths

Database Folder	C:\Windows\NTDS
Log Files Folder	C:\Windows\NTDS
SYSVOL Folder	C:\Windows\SYSVOL\sysvol

### Replicate From



Name	Site
 DEMO-2012R2-DC3	Purchasing
 DEMO-2012R2-DC4	ContosoHQ

### Replicate To

Name	Site
 DEMO-2012R2-DC4	
 DEMO-2012R2-DC3	
 DEMO-2012R2-DC2	

---

 **Replication Connections**

Name	From Server	From Site	Description
 <automatically generated>	DEMO-2012R2-DC3	Purchasing	
 454d2609-2ca3-4f69-8147-709ce24ebf47	DEMO-2012R2-DC4	ContosoHQ	

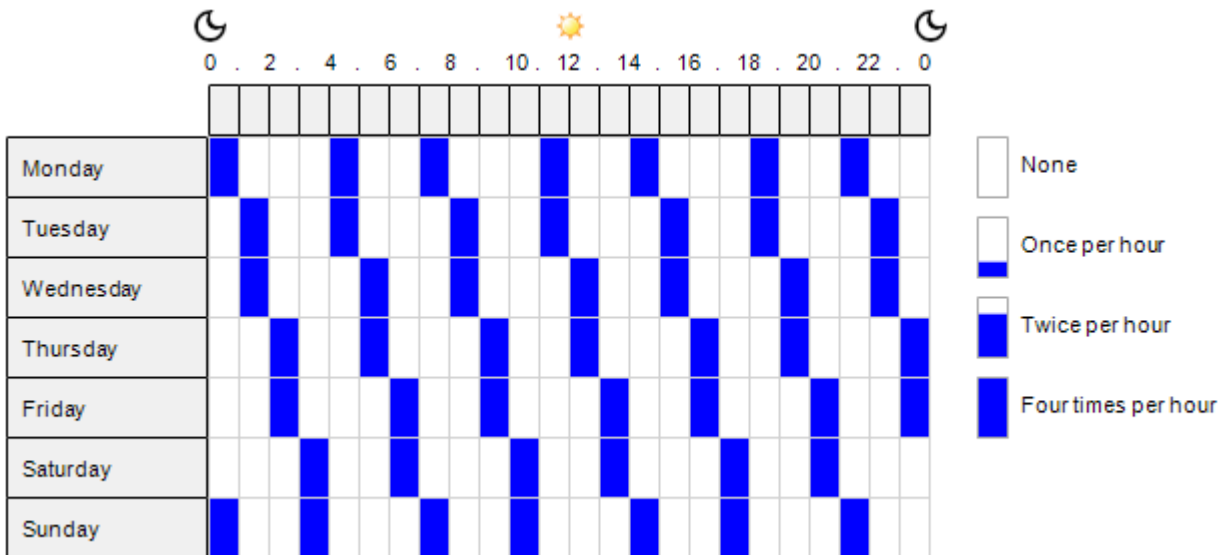
<automatically generated>

A connection object represents a replication connection from one domain controller to another and includes information about the transport type to use as well as the replication schedule.

### Connection Details

Description	
Transport Type	IP
Data Compression Enabled	True
Enabled	True
Generated By KCC	True
Notification Status	No Notification
Source Server	DEMO-2012R2-DC3
Source Site Name	Purchasing

### Schedule

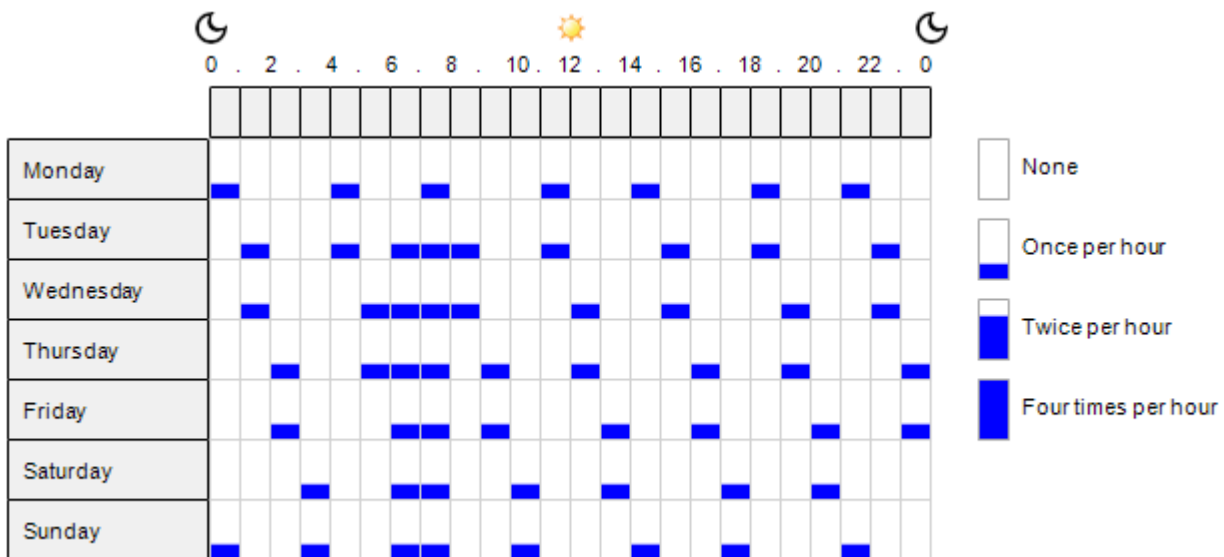


A connection object represents a replication connection from one domain controller to another and includes information about the transport type to use as well as the replication schedule.

 **Connection Details**

Description	
Transport Type	IP
Data Compression Enabled	True
Enabled	True
Generated By KCC	False
Notification Status	No Notification
Source Server	DEMO-2012R2-DC4
Source Site Name	ContosoHQ

 **Schedule**



# Purchasing

A site consists of well-connected networks as determined by the subnet addresses assigned to that site allowing clients to locate the nearest resources such as domain controllers or distributed file system (DFS) servers.

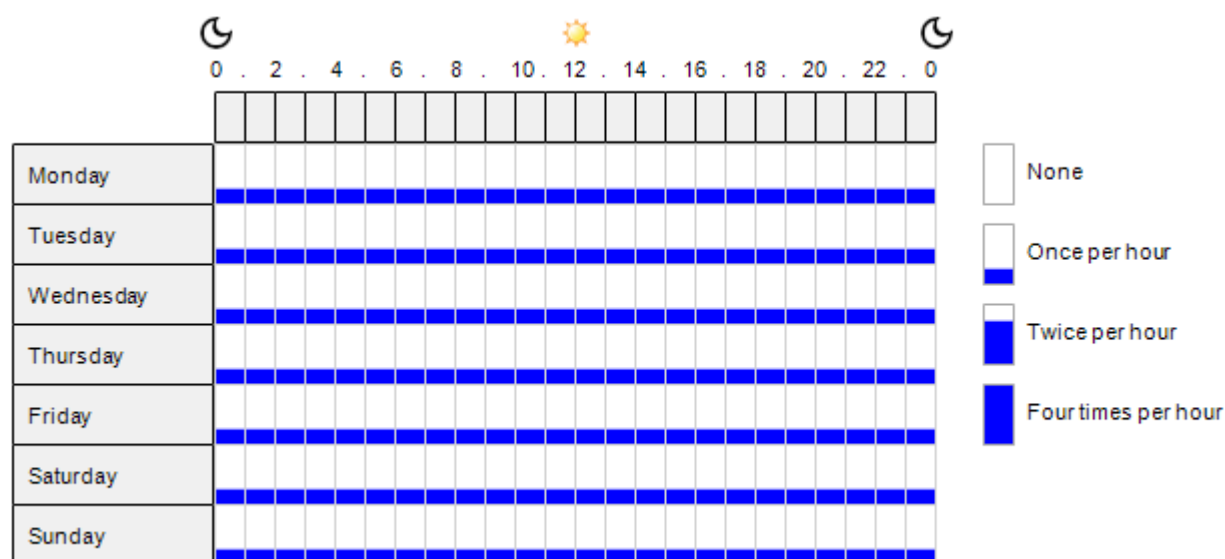
## Purchasing

Description	
Location	
Subnets	
Inter-Site Topology Generator	DEMO-2012R2-DC3
Inter-Site Topology Generator Site	Purchasing

## Universal Group Membership Caching







Enabled	False
Refresh Cache From	<Default>

## Replication Schedule



---

**Permissions**

Type	Principal	Access
 Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read
 Allow	NT AUTHORITY\Authenticated Users	Read
 Allow	NT AUTHORITY\SYSTEM	Full Control
 Access Allowed Object	DEMO2012R2\Enterprise Read-only Domain Controllers	Self
 Allow	DEMO2012R2\Enterprise Admins	Full Control
 Allow	DEMO2012R2\Domain Admins	Create all child objects, Delete, ExtendedRight, Modify owner, Modify permissions, Read, Write

## Domain Controllers

An Active Directory domain controller authenticates and authorizes all users and computers in a Windows domain type network. Every domain controller supports multi-master operations allowing autonomy in the reading and writing information to the directory service with the exception of read-only domain controllers (RODCs) which allow only read-only access to the directory service.

RODC servers are useful in less secure physical environments such as a branch office.

Name	Domain	Bridgehead	Global Catalog	Server Type
 DEMO-2012R2-DC3	Purchasing.demo2012r2.int		True	Domain Controller

## DEMO-2012R2-DC3

An Active Directory domain controller authenticates and authorizes all users and computers in a Windows domain type network

### DEMO-2012R2-DC3

Server Type	Domain Controller
DNS Hostname	DEMO-2012R2-DC3.Purchasing.demo2012r2.int
Domain	Purchasing.demo2012r2.int
Global Catalog	True
Description	
Bridgehead server transports	
Query Policy	
Created	19/09/2013 16:36:04
Last Modified	17/04/2014 13:15:33



### Host Information

Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Processors	Intel(R) Core(TM) i7-3537U CPU @ 2.00GHz
Serial Number	VMware-56 4d 6e ce 00 0e b4 37-9b 12 a4 84 d7 cc 8e e6
Operating System Name	Microsoft Windows Server 2012 R2 Datacenter
Service Pack	[None Installed]



### Directory Service Installation Paths

Database Folder	C:\NT\DB
Log Files Folder	C:\NT\Log
SYSVOL Folder	C:\NT\Sys\sysvol

### Replicate From

Name	Site
 DEMO-2012R2-DC4	ContosoHQ
 DEMO-2012R2-DC1	HQ



### Replicate To

Name	Site
 DEMO-2012R2-DC4	
 DEMO-2012R2-DC1	



---

 **Replication Connections**

Name	From Server	From Site	Description
 <automatically generated>	DEMO-2012R2-DC4	ContosoHQ	
 <automatically generated>	DEMO-2012R2-DC1	HQ	

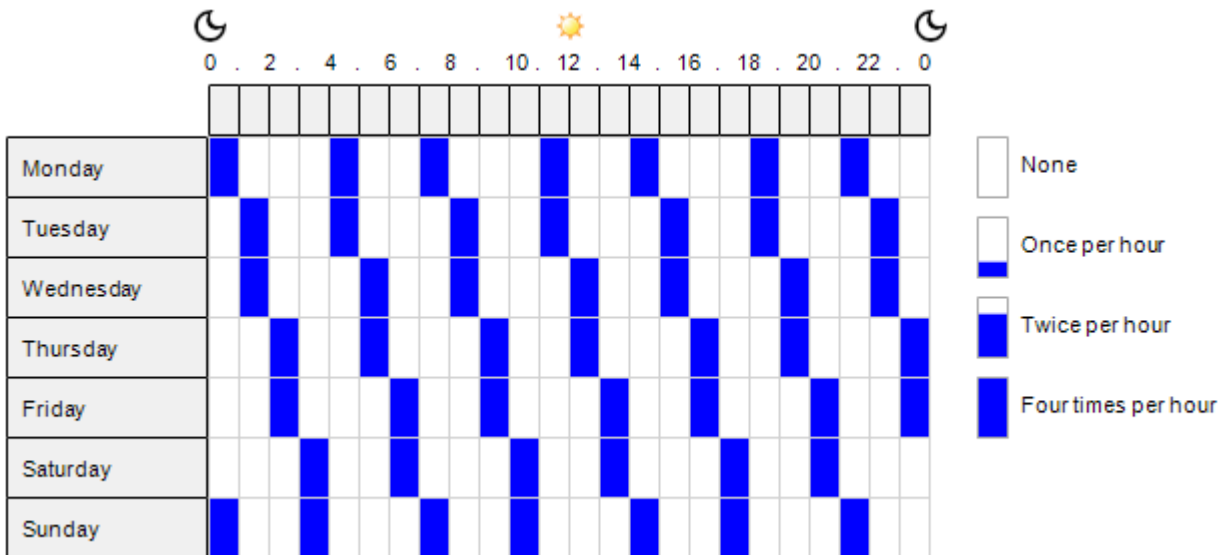
<automatically generated>

A connection object represents a replication connection from one domain controller to another and includes information about the transport type to use as well as the replication schedule.

### Connection Details

Description	
Transport Type	IP
Data Compression Enabled	True
Enabled	True
Generated By KCC	True
Notification Status	No Notification
Source Server	DEMO-2012R2-DC4
Source Site Name	ContosoHQ

### Schedule



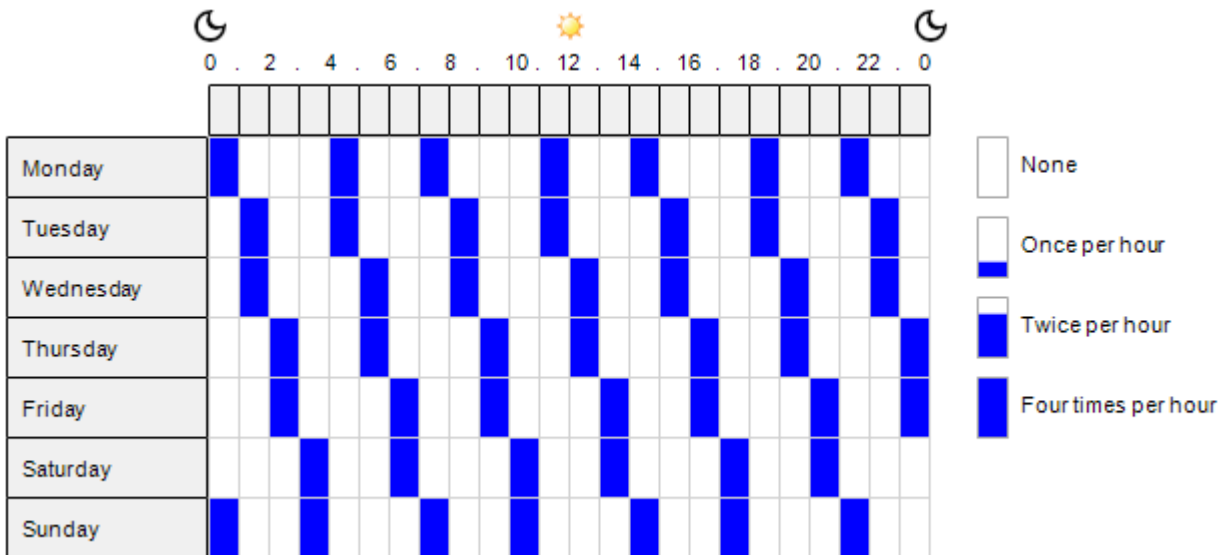
<automatically generated>

A connection object represents a replication connection from one domain controller to another and includes information about the transport type to use as well as the replication schedule.

### Connection Details

Description	
Transport Type	IP
Data Compression Enabled	True
Enabled	True
Generated By KCC	True
Notification Status	No Notification
Source Server	DEMO-2012R2-DC1
Source Site Name	HQ

### Schedule



# SalesOffice

A site consists of well-connected networks as determined by the subnet addresses assigned to that site allowing clients to locate the nearest resources such as domain controllers or distributed file system (DFS) servers.

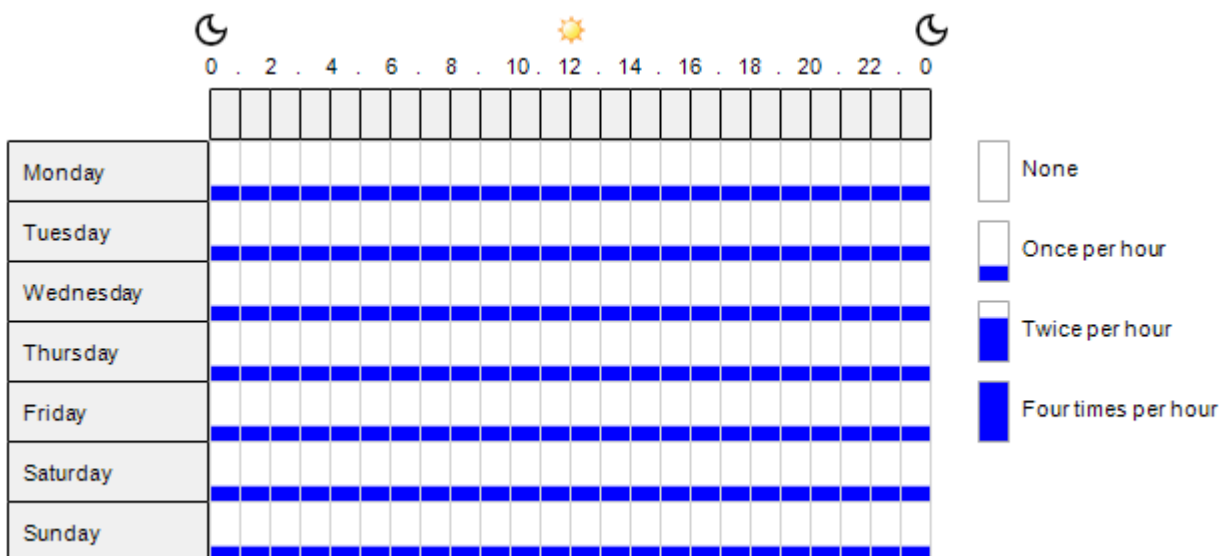
## SalesOffice

Description	
Location	Sales Office
Subnets	
Inter-Site Topology Generator	
Inter-Site Topology Generator Site	







## Universal Group Membership Caching

Enabled	False
Refresh Cache From	<Default>

## Replication Schedule




## Permissions

Type	Principal	Access
 Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read
 Allow	NT AUTHORITY\Authenticated Users	Read
 Allow	NT AUTHORITY\SYSTEM	Full Control
 Access Allowed Object	DEMO2012R2\Enterprise Read-only Domain Controllers	Self
 Allow	DEMO2012R2\Enterprise Admins	Full Control
 Allow	DEMO2012R2\Domain Admins	Create all child objects, Delete, ExtendedRight, Modify owner, Modify permissions, Read, Write

## Domain Controllers

An Active Directory domain controller authenticates and authorizes all users and computers in a Windows domain type network. Every domain controller supports multi-master operations allowing autonomy in the reading and writing information to the directory service with the exception of read-only domain controllers (RODCs) which allow only read-only access to the directory service.

RODC servers are useful in less secure physical environments such as a branch office.

Name	Domain	Bridgehead	Global Catalog	Server Type
 DEMO-2012R2-DC2	demo2012r2.int		True	Read-Only Domain Controller

## DEMO-2012R2-DC2

A read-only domain controller (RODC) allow only read-only access to the directory service increasing security in environments such as branch offices.










### DEMO-2012R2-DC2

Server Type	Read-Only Domain Controller
DNS Hostname	DEMO-2012R2-DC2.demo2012r2.int
Domain	demo2012r2.int
Global Catalog	True
Description	Sample RODC in the sales office
Bridgehead server transports	
Query Policy	Default Query Policy
Created	19/09/2013 16:36:04
Last Modified	17/04/2014 13:15:33

### Read-Only Domain Controller (RODC) Settings

Manager	DEMO2012R2\tsmith
---------	-------------------

### Password Replication Policy

Name	Path	Setting
 DEMO2012R2\Simple	demo2012r2.int	Allow
 DEMO2012R2\Allowed RODC Password Replication Group	demo2012r2.int/Users	Allow
 DEMO2012R2\DEMO-2012R2-DC1\$	demo2012r2.int/Domain Controllers	Allow
 DEMO2012R2\Guest	demo2012r2.int/Users	Allow
 DEMO2012R2\Denied RODC Password Replication Group	demo2012r2.int/Users	Deny
 DEMO2012R2\Account Operators	demo2012r2.int/Builtin	Deny
 DEMO2012R2\Server Operators	demo2012r2.int/Builtin	Deny
 DEMO2012R2\Backup Operators	demo2012r2.int/Builtin	Deny
 DEMO2012R2\Administrators	demo2012r2.int/Builtin	Deny

### Host Information

Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Processors	Intel(R) Core(TM) i7-3537U CPU @ 2.00GHz
Serial Number	VMware-56 4d 31 0d ef 4f 82 95-4d e9 d8 be 90 b8 09 b8
Operating System Name	Microsoft Windows Server 2012 R2 Datacenter
Service Pack	[None Installed]

---

 **Directory Service Installation Paths**

Database Folder	C:\Windows\NTDS
Log Files Folder	C:\Windows\NTDS
SYSVOL Folder	C:\Windows\SYSVOL\sysvol

---



 **Replicate From**

Name	Site
 DEMO-2012R2-DC1	HQ



---

 **Replication Connections**

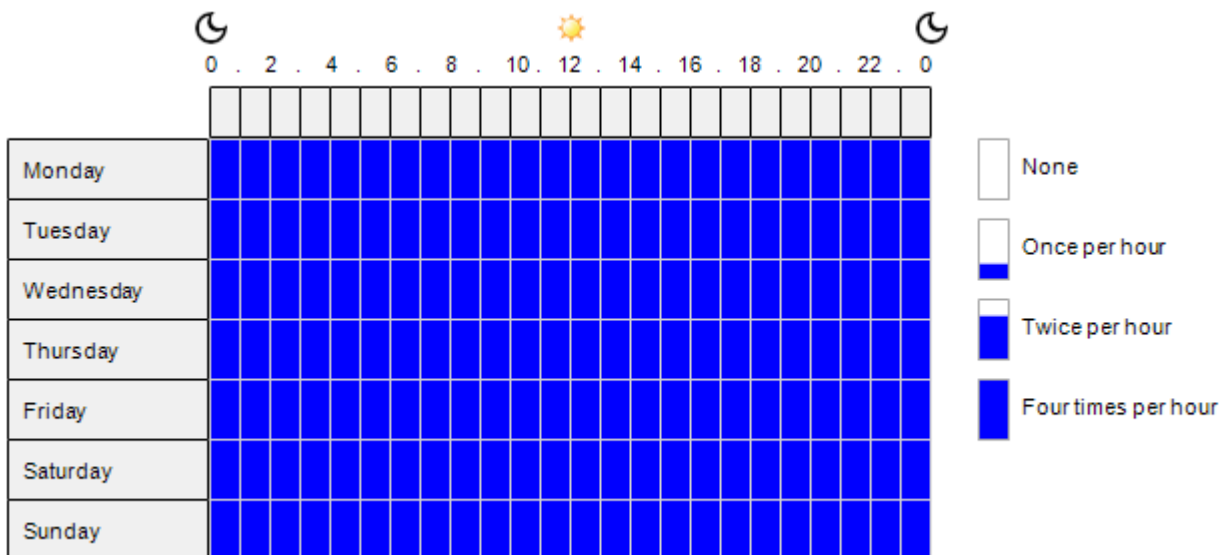
Name	From Server	From Site	Description
 DEMO-2012R2-DC1	DEMO-2012R2-DC1	HQ	
 RODC Connection (SYSVOL)	DEMO-2012R2-DC1	HQ	Sample replication connection

A connection object represents a replication connection from one domain controller to another and includes information about the transport type to use as well as the replication schedule.

 **Connection Details**

Description	
Transport Type	IP
Data Compression Enabled	True
Enabled	True
Generated By KCC	False
Notification Status	Intra-Site Only
Source Server	DEMO-2012R2-DC1
Source Site Name	HQ

 **Schedule**



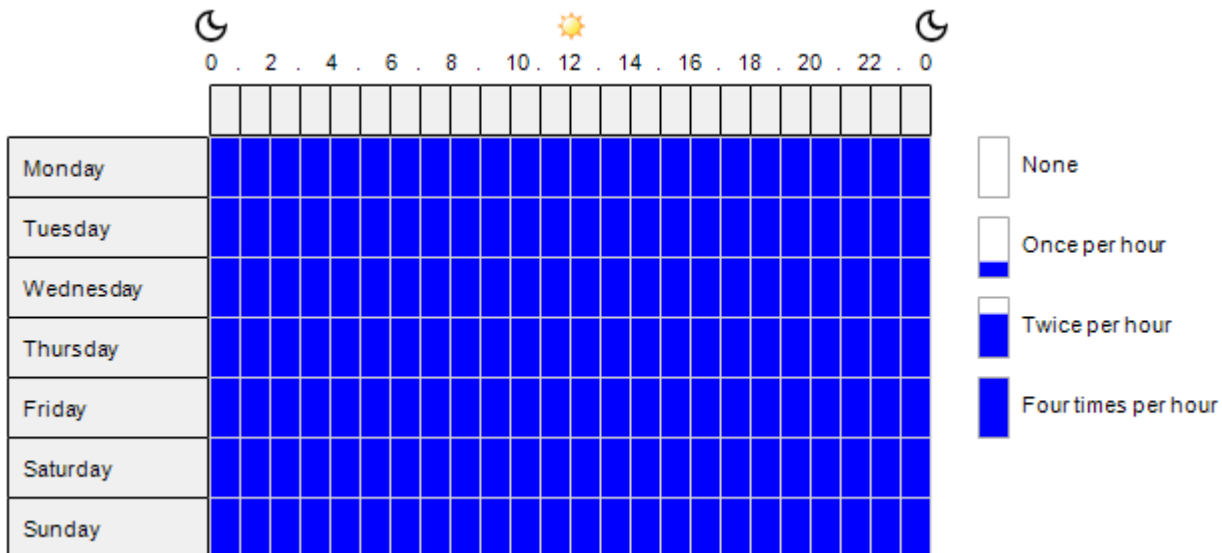
## RODC Connection (SYSVOL)

A connection object represents a replication connection from one domain controller to another and includes information about the transport type to use as well as the replication schedule.

### Connection Details











Description	Sample replication connection
Transport Type	
Data Compression Enabled	True
Enabled	True
Generated By KCC	True
Notification Status	Intra-Site Only
Source Server	DEMO-2012R2-DC1
Source Site Name	HQ

### Schedule



# Version History

The version history displays the changes that have been made to the documentation of this item over time - either automatically when a change has been detected, or manually by users of the system.

Version	Username	Date	Time	Description
 1.10	CENTREL-WS02\Administrator	24 April 2014	11:22	Updated by XIA Configuration Client Data
 1.09	CENTREL-WS02\Administrator	24 April 2014	10:13	Updated by XIA Configuration Client Data
 1.08	CENTREL-WS02\Administrator	24 April 2014	10:13	Updated by XIA Configuration Client Data
 1.07	CENTREL-WS02\Administrator	24 April 2014	10:13	Updated by XIA Configuration Client Data
 1.06	CENTREL-WS02\Administrator	24 April 2014	10:13	Updated by XIA Configuration Client Data
 1.05	CENTREL-WS02\Administrator	24 April 2014	10:13	Updated by XIA Configuration Client Data
 1.04	CENTREL-WS02\Administrator	24 April 2014	10:13	Updated by XIA Configuration Client Data
 1.03	CENTREL-WS02\Administrator	24 April 2014	10:13	Updated by XIA Configuration Client Data
 1.02	CENTREL-WS02\Administrator	24 April 2014	10:13	Updated by XIA Configuration Client Data
 1.01	CENTREL-WS02\Administrator	24 April 2014	10:13	Updated by XIA Configuration Client Data