Lesson 16: Configuring Sites

MOAC 70-412: Configuring Advanced Windows Server 2012 Services

Microsoft Official Academic Course

WILEY

Overview

- Objective 5.3 – Configure sites.
  - Create and configure site links
  - Manage site coverage
  - Manage registration of SRV records
  - Move domain controllers between sites

Configuring Sites and Subnets

Lesson 16: Configuring Sites

Configuring Sites and Subnets

- Sites and subnets define the physical design of an Active Directory Domain Services (AD DS) domain.
- Sites allow clients, authentication, and applications to access domain controllers and services within a physical location before needing to cross a Wide Area Network (WAN) link.
- Sites also utilize the high-speed networks of the local network to quickly replicate data between domain controllers within the site.
- With AD DS sites, each site represents a physical location.

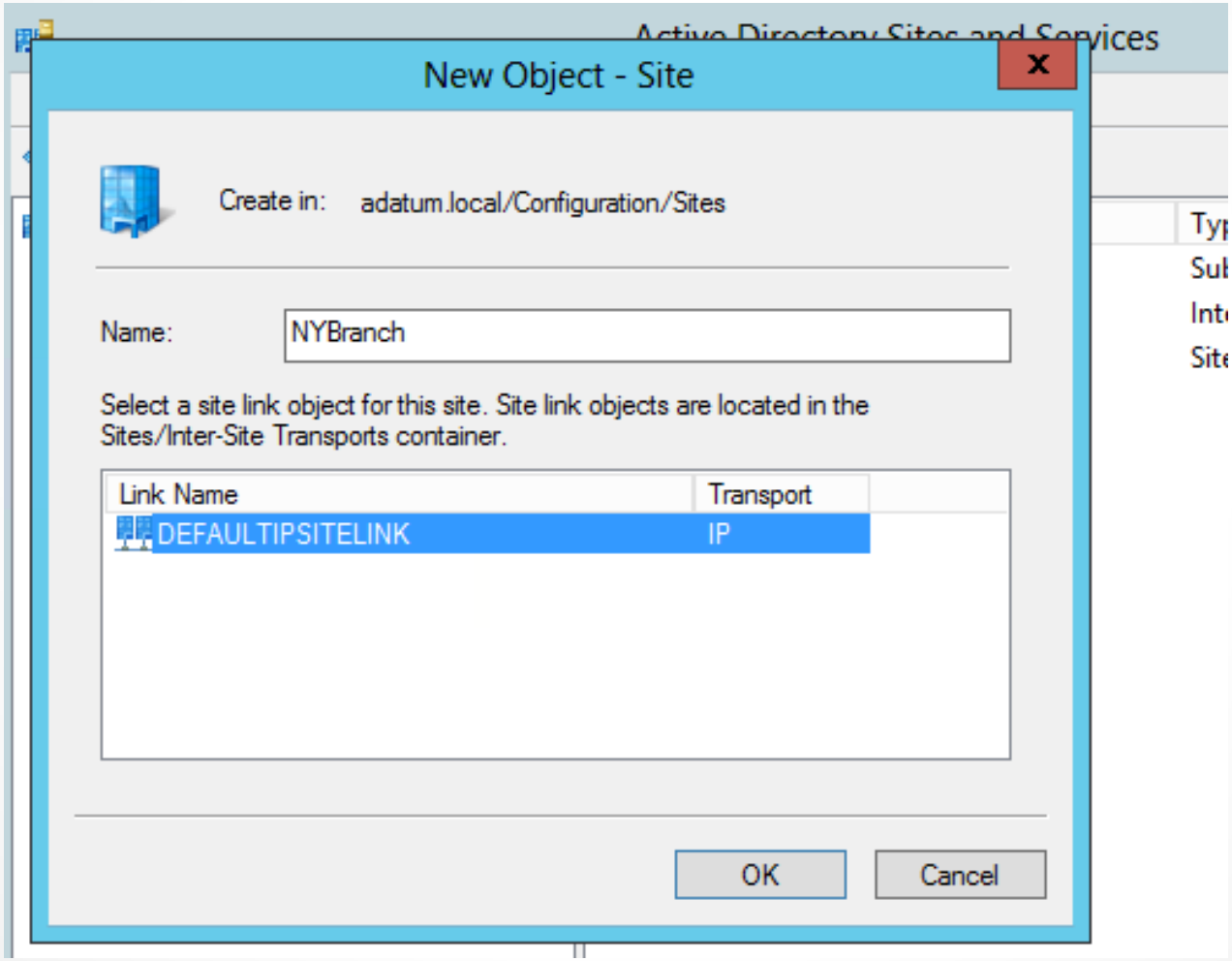
Configuring Sites

- ***Sites*** are representative of the physical AD DS domain topology and contain domain controllers, clients, and services.
- At forest creation, the default site created is called *Default-First-Site-Name*, which contains all domain controllers added to the domain until new sites and subnets are created.
- Sites group domain controllers together at the same physical location to allow efficient replication between one another on high-speed internal networks before sending any directory changes to remote locations or branch offices.

Intrasite and Intersite Replication

- All domain controllers within a site replicate with one another in a process called ***Intrasite replication***, which is the replication of compressed data that occurs across site links between domain controllers located in different sites.
- ***Intersite replication***, through the use of Bridgehead servers, replicates directory partitions from one site's bridgehead server to another site's bridgehead server.
- Each bridgehead server then replicates the changes internal to its replica domain controllers through Intrasite replication.

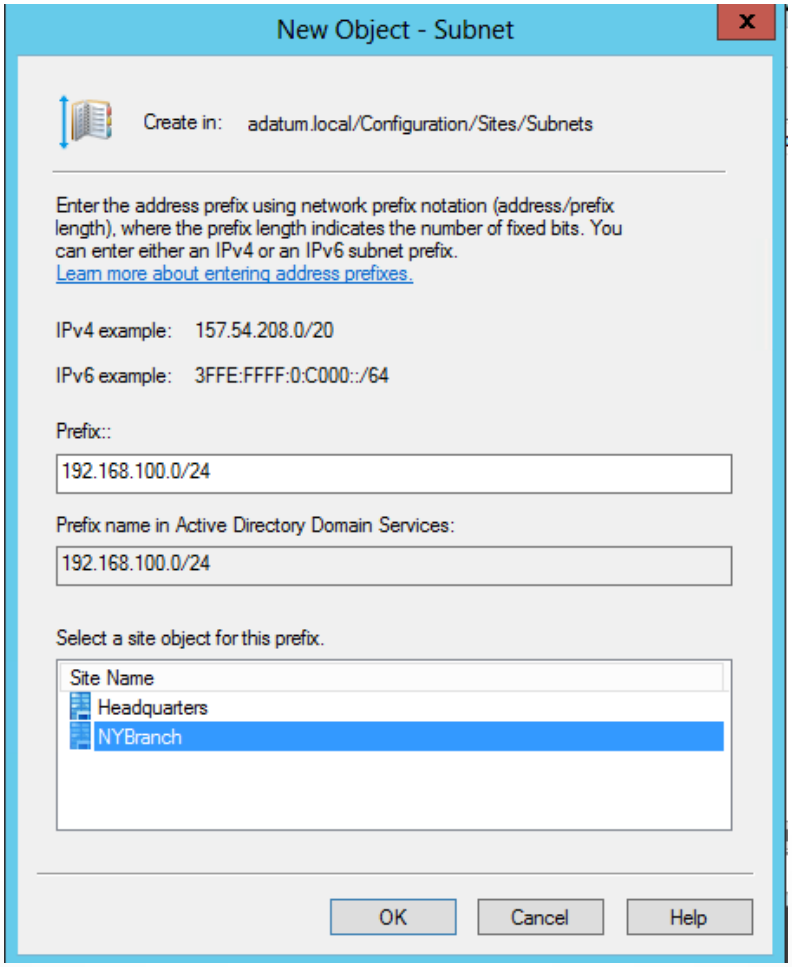
Adding a Site



Configuring Subnets

- ***Subnets*** are created to group and assign computers within the same network subnet to a site. Subnets can be assigned only to one site and can be IPv4 or IPv6 subnets.
- At logon, domain controllers assign clients to sites based on their network address and subnet.
- When designing an AD DS site topology, make sure all IP ranges used by clients and servers are added to a subnets list and assigned to a site for optimized service access and domain controller referencing.

Adding a Subnet



Site Links

- Site links define the logical replication link between sites to perform Intersite replication, allowing for faster and optimized replication between sites based on configured costs and frequencies.
- Site links manage the logical flow of replication between physical sites.
- The DEFAULTIPSITELINK site link object is created by default at forest creation.
- When new domains and domain controllers are added to the forest, if new sites links are not manually created, they will all become members of the DEFAULTIPSITELINK site.

Site Links

- In large enterprise environments, spanning several physical locations, replication traffic is at the mercy of the WAN links between physical locations.
- This situation can cause replication issues when there is a mix of reliable and unreliable network paths between sites.
- Physical infrastructure between sites might differ and have different requirements about when to utilize bandwidth.
- To resolve the problem of costly bandwidth and timing restrictions of physical connections, you can implement site links.

Knowledge Consistency Checker (KCC)

- The ***Knowledge Consistency Checker (KCC)*** dynamically creates connection objects between domain controllers allowing for addition and removal of domain controllers without manual configuration of replication partners within the Active Directory Sites and Services tool.
- When domain controllers are added, removed, failed, or modifications are made to the replication schedule, the KCC actively monitors and makes the required changes to keep replication running efficiently between all domain controllers.
- Although the KCC can be disabled, it is not an efficient use of administrative resources when numerous changes are to be made within an enterprise environment.
- It is recommended to leave the KCC enabled and let it dynamically make the changes for you to eliminate unneeded administrative overhead.

Intersite Topology Generator

- Assigned by the KCC, the ***Intersite Topology Generator (ISTG)***:
  - Is a domain controller, one in each site
  - Monitors and makes connections with domain controllers in other sites to domain controllers in its site
  - Manages inbound replication objects for bridgehead servers within its site

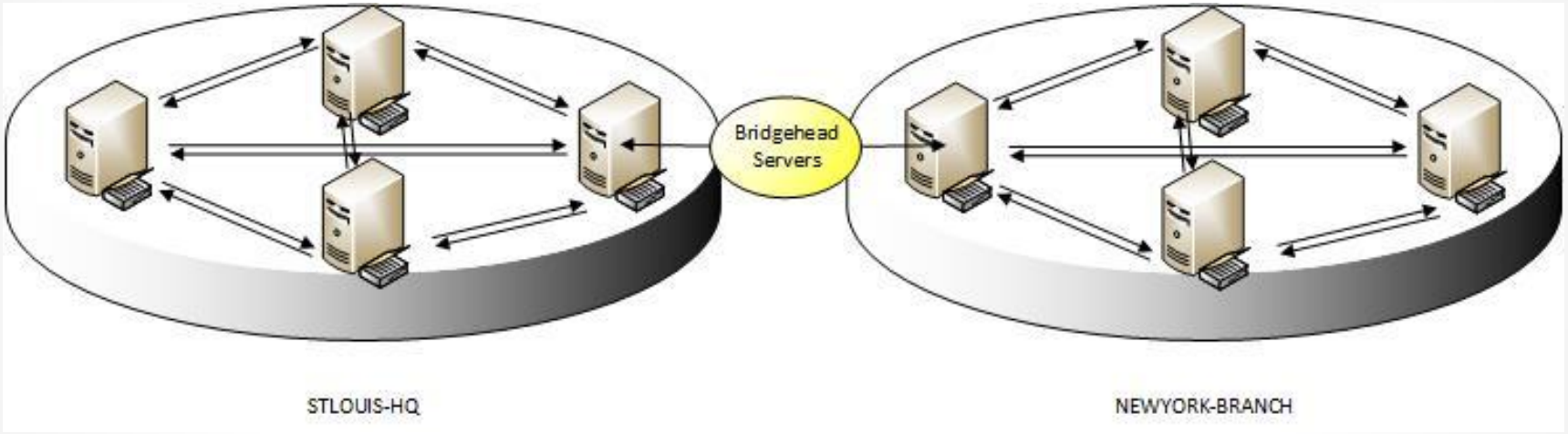
Intersite Transport Protocols

- ***IP Transport***
  - Replicates all AD DS partitions synchronously to domain controllers in well-connected sites.
  - Is efficient, reliable, and the preferred method of replication between Intersite partners.
- ***SMTP Transport***
  - Is configured with the Simple Mail Transport Protocol (SMTP)
  - Sends replication asynchronously via e-mail messages.
  - Requires the implementation of Active Directory Certificate Services (AD CS).
  - Replicates only the schema, configuration, and Global Catalog partitions. Using SMTP does not replicate the domain partition.
  - Can be used in situations where RPC over TCP/IP is not configured between two sites.

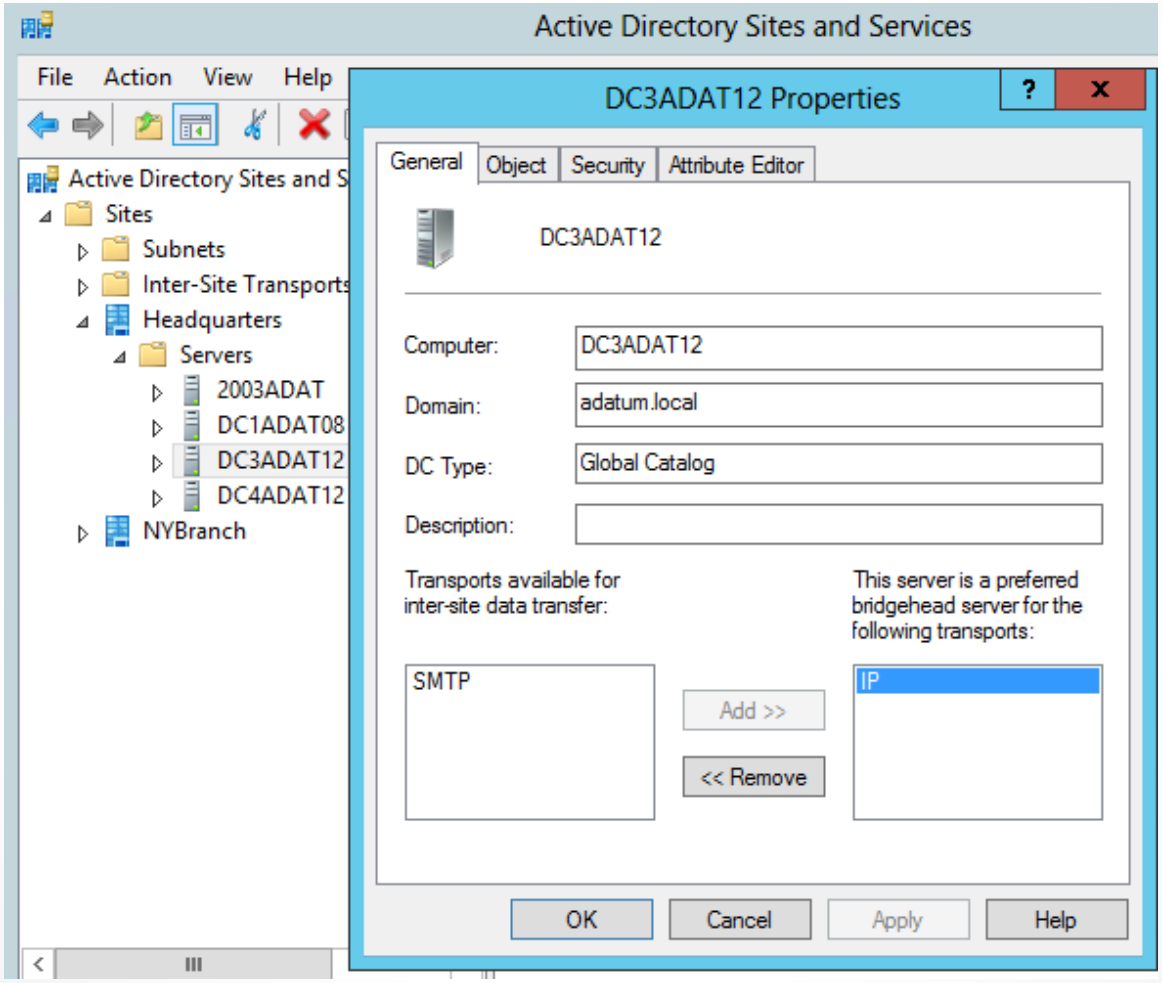
Bridgehead Servers

- ***Bridgehead servers***
  - Are automatically configured by AD DS.
  - Take the changes made during Intrasite replication and then replicate those changes to the bridgehead server in a connected site.
- It is best practice to allow AD DS to handle the assignment of the bridgehead server tasks to specific domain controllers.
- In certain environments, you might need to manually configure a bridgehead server dedicated to the additional processing and traffic requirements.

Bridgehead Servers



Bridgehead Servers

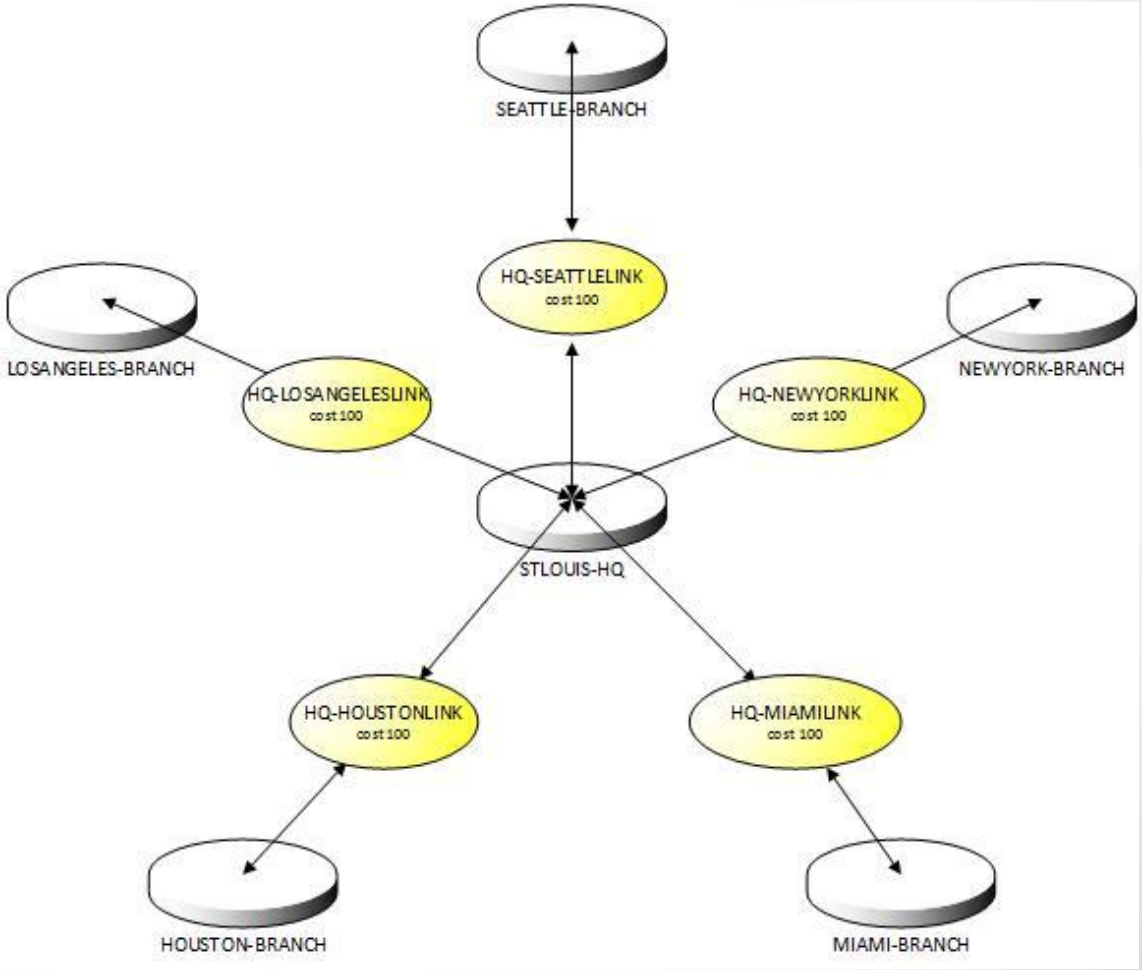


Site Link Bridges

- Site link bridging allows transitive linking between all sites in the forest.
- Bridge All Site Links is enabled by default to permit site link bridging between all sites in the forest.

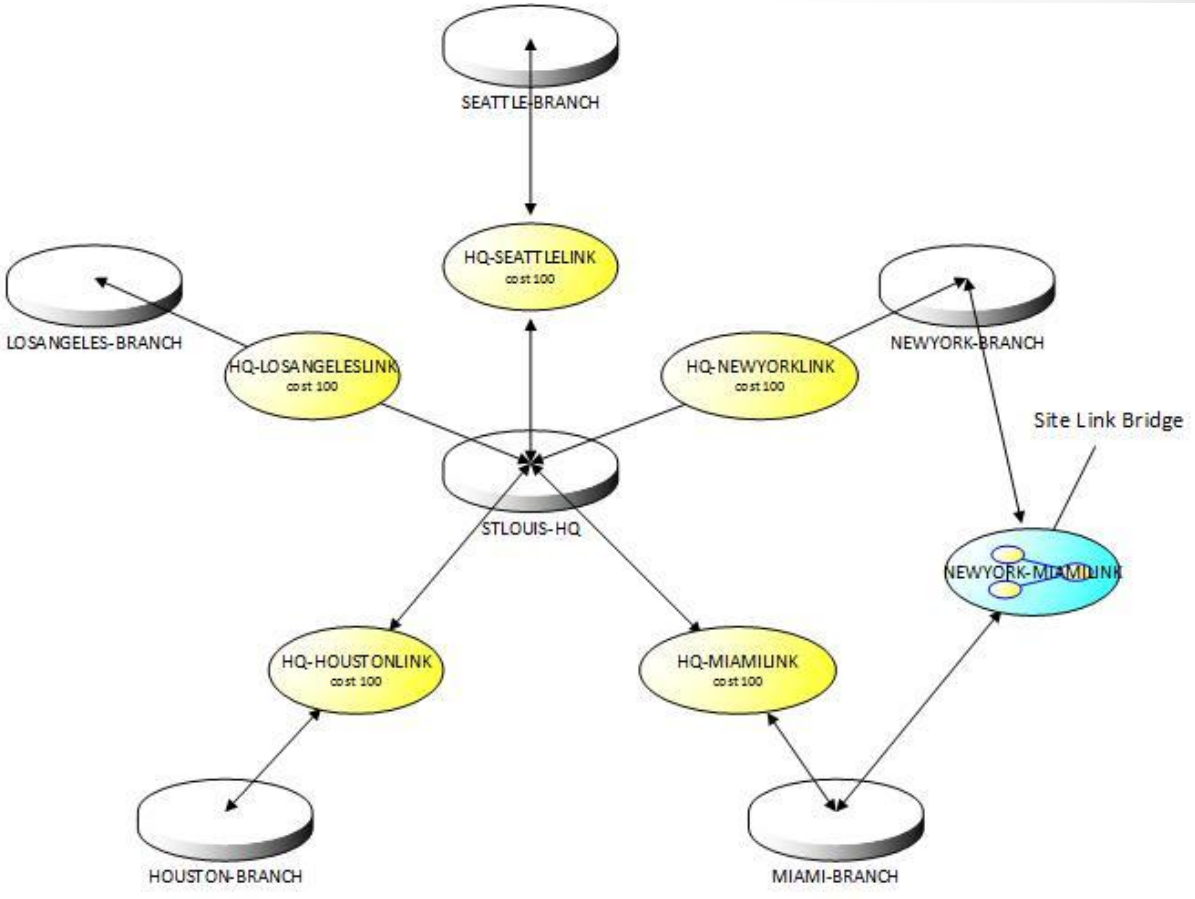
Hub-and-Spoke Topology

A ***Hub-and-Spoke Topology***, created by an Enterprise Administrator, disables the Bridge All Site Links option and then creates site link bridges between a central "hub" site and each of its remote "spoke" sites.

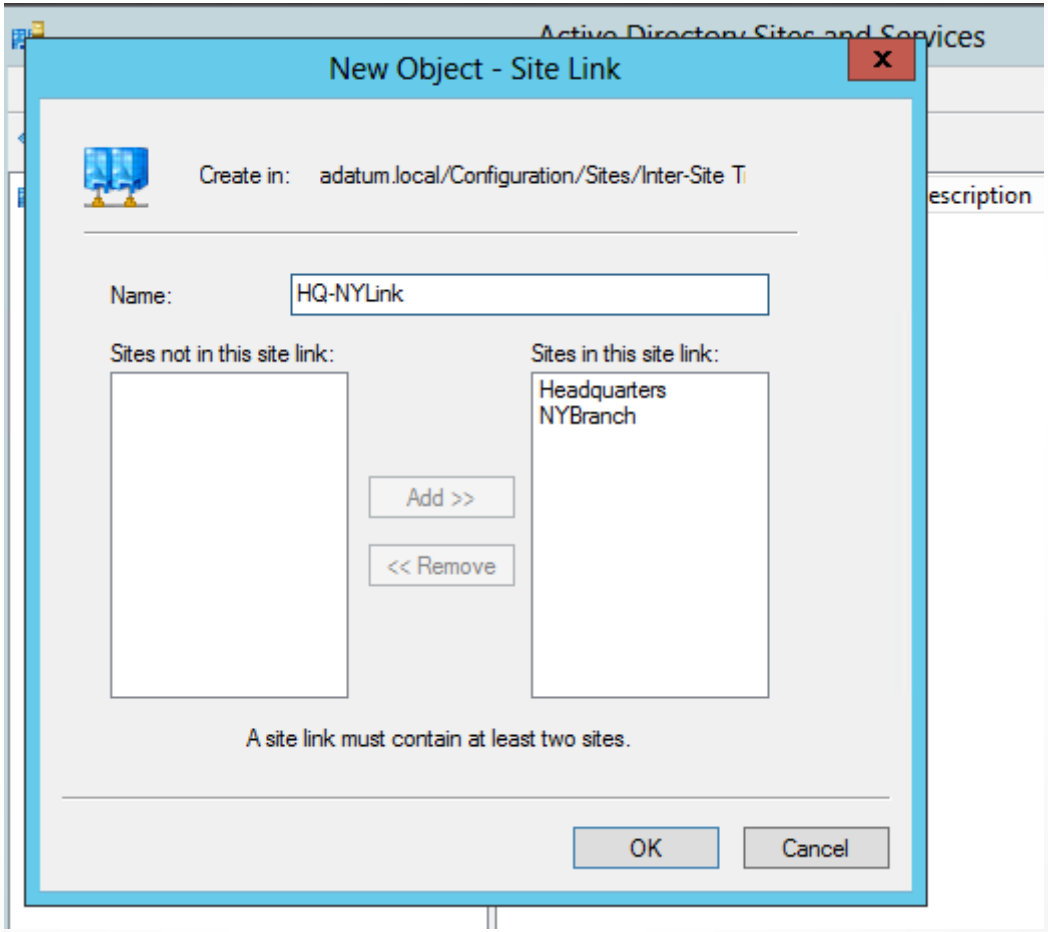


Site Link Bridges

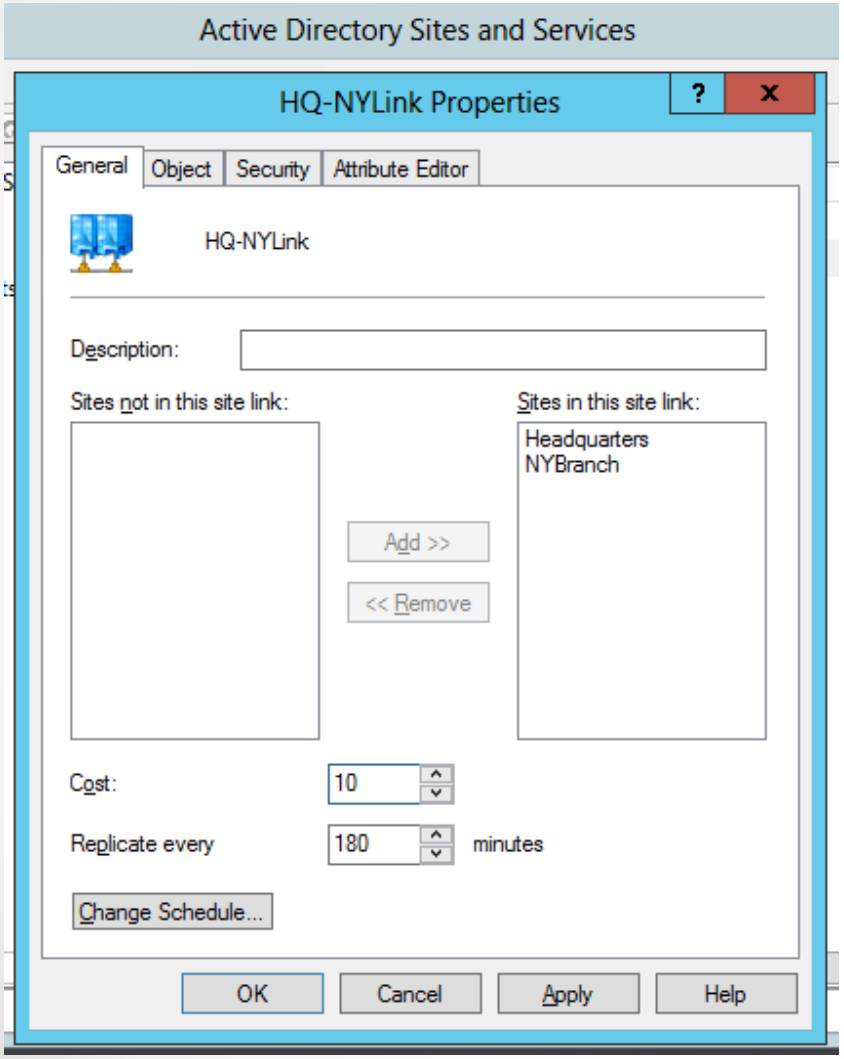
Site link bridges are used when the Bridge All Site Links option is disabled to allow transitive linking between sites not directly connected.



Site Link Bridges



Site Link Costs



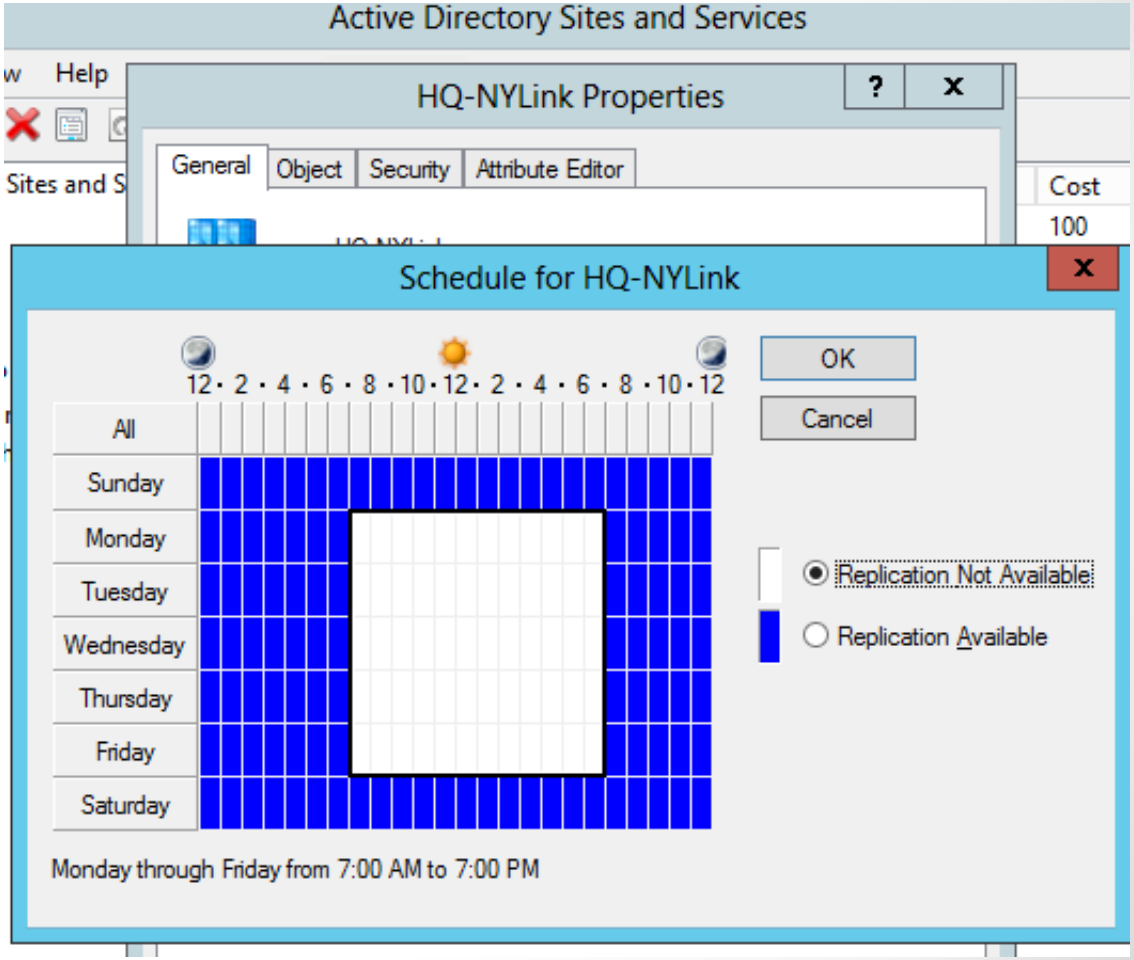
- By default, site link costs are configured with a cost value of 100.
- Site link costs can be configured to allow AD DS to replicate over one link before replicating over another one.
- Replication always replicates over the lowest cost link between sites.

Replication Interval

- The ***replication interval*** defines how often replication across the site link occurs.
- By default, replication on site links are configured to occur every 180 minutes and can be modified within the site link properties.
- Replication between sites might need to occur more frequently if there are constant changes to AD DS that need to be seen in branch offices immediately.
- The replication interval can be configured to allow replication every 15 minutes across site links.

Replication Schedule

- The ***replication schedule*** defines when the replication is allowed to occur.
- By default, replication is scheduled to occur 24 hours a day, 7 days a week, and can be modified within the site link properties.
- This ensures replication occurs constantly.



Managing Site Coverage

- Not all environments require a domain controller at each site.
- Domain controllers in sites can take over for missing domain controllers in remote sites.
- If a site does not have a domain controller to authenticate clients against, depending on cost, domain controllers in the closest site will automatically register an SRV record in the client site to automatically cover the site for the missing domain controller.
- This allows clients to contact the closest domain controller to access the resources needed.
- The clients in the site that are automatically covered are still traversing the WAN to connect to the domain controller for authentication and resource access.

Managing Registration of SRV Records

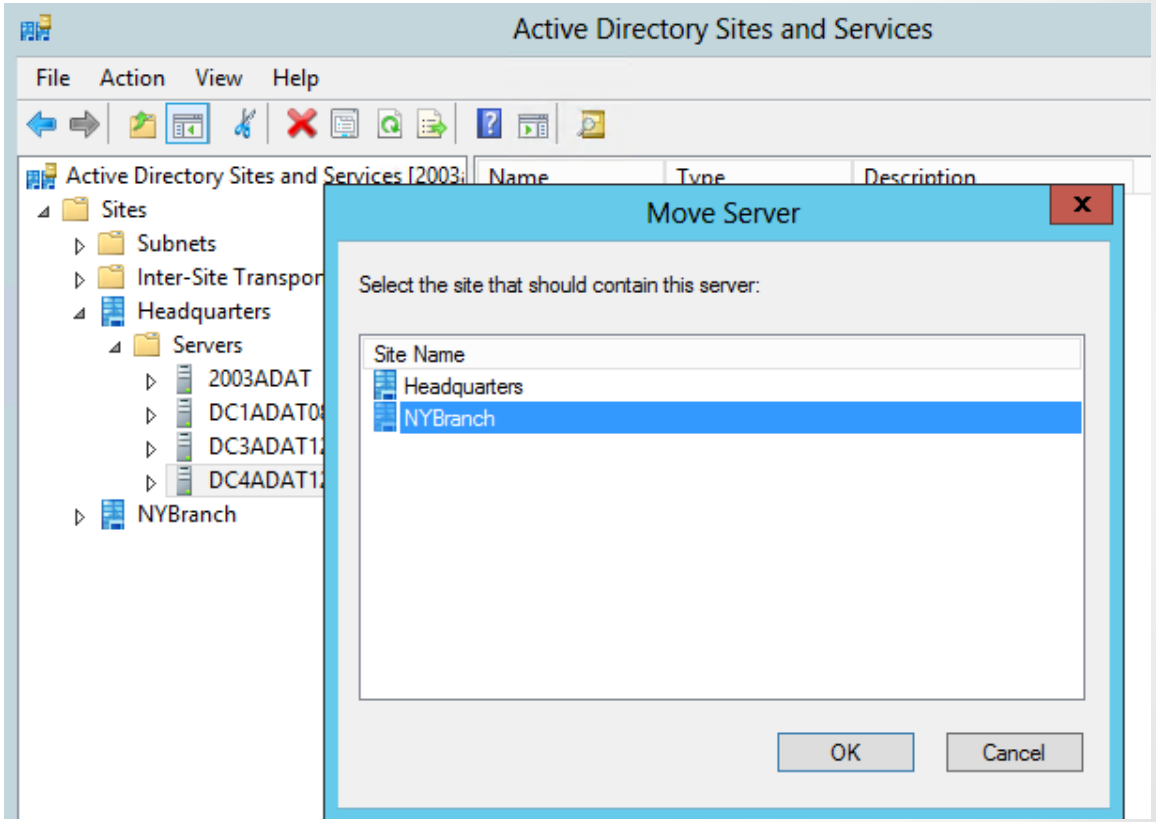
- Domain controller SRV records are a critical part of domain controller and client communications.
- All domain controllers register an SRV record for their clients to find them.
- During SRV registration, the _kerberos and _ldap SRV records are created and advertised at the following locations in the domain's zone: _msdcs/dc/_Sites/Sitename/_tcp and _msdcs/dc/_tcp.

Moving Domain Controllers Between Sites

- Moving a domain controller to a different site is a simple task once your environment is ready for the change.
- During domain controller promotion, you are prompted to assign the domain controller to a site.
- If you do not choose the site for the domain controller to be added to during promotion, it will assign itself to a site based on its IP address at the time of promotion.
- If it is one of the first domain controllers added to a forest, the domain controllers will be placed into the Default-First-Site-Name site until the site, subnet, and site link topology are in place.
- Once the site topology is in place, the domain controllers can be moved to the appropriate sites and replicate properly with one another.

Default-First-Site-Name

The Default-First-Site-Name site can be renamed to match the naming standard for its current location or it can be removed if it is not part of the new topology.



Lesson Summary

- Clients separated by physical locations are grouped through the creation of sites and subnets.
- Multiple sites are linked together to perform Intersite replication between domain controllers spread across multiple physical locations.
- Domain controllers can register their records in remote sites when a domain controller is not present in that site.

Lesson Summary

- When Read-Only Domain Controllers (RODCs) are the only domain controllers in a site, and the next closest site contains only Windows 2003 domain controllers, Automatic Site Coverage can be disabled. This prevents the Windows Server 2003 domain controllers from automatically registering their SRV records in the RODCs site.
- Domain controller SRV records can be reregistered by restarting the NETLOGON service. A copy of the records that are registered is saved locally to the domain controller's NETLOGON.dns file.
- Domain controllers can be easily moved between sites, once careful planning and strategies are in place to ensure clients can connect to the domain controller once it is moved to its destination site.