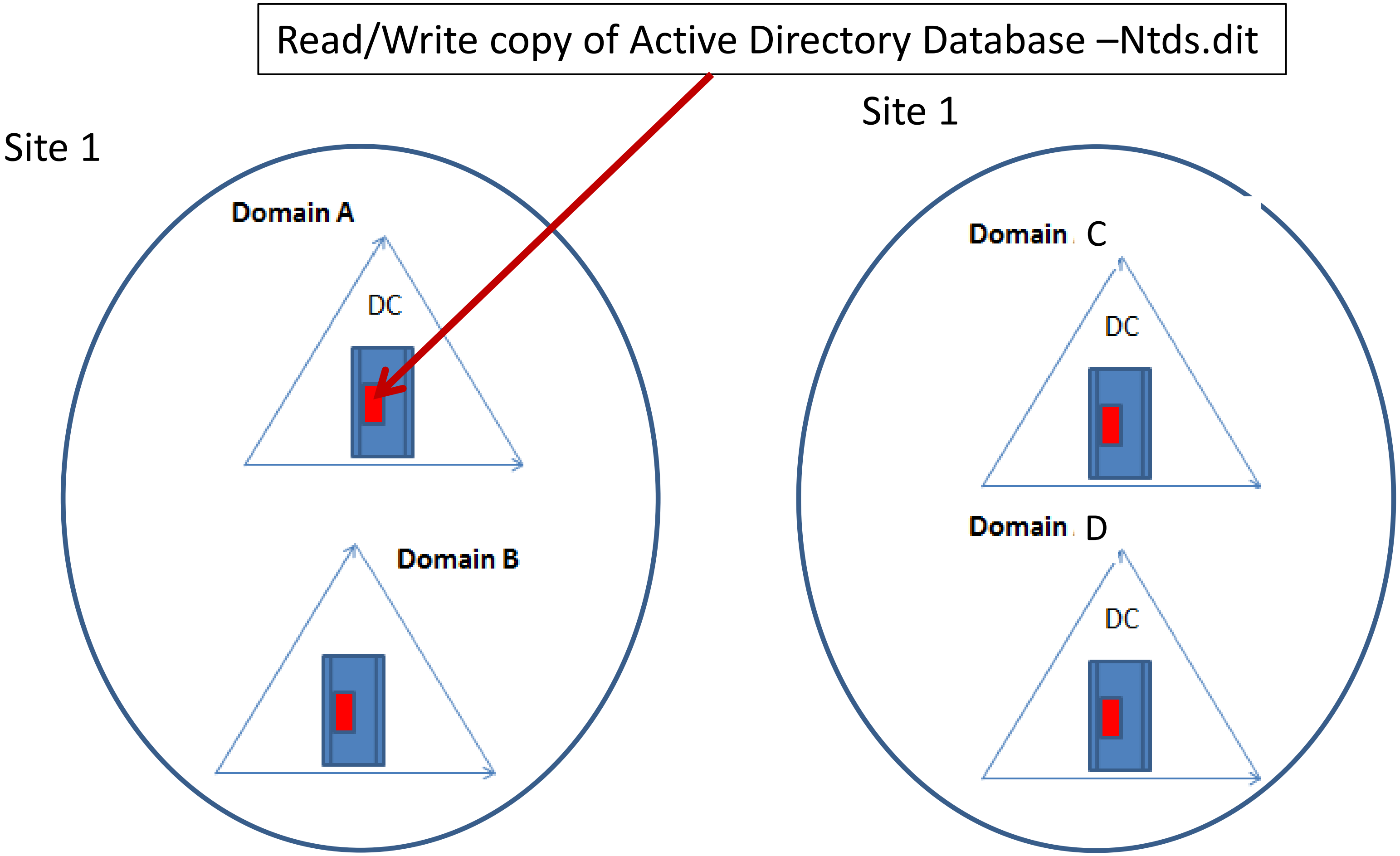
Active Directory Replicationm



<u>All domain controllers host a full replica of the domain information for its own domain</u>

- Replication: When an object (user, computer, group) in Active Directory is created, deleted, moved, or changed Active Directory replication is triggered.

- Replication is the process that ensures that changes made to a replica on one domain controller are transferred to replicas on the remainder of the domain controllers

Types of Active Directory replication:

1. Intrasite Replication

a. Replication between domain controllers within the same site
b. Utilizes the Remote Procedure Call (RPC) protocol to convey replication data over fast, reliable network connections.

2. Intersite Replication:

a. Takes place between sites
b. Can utilize either RPC over IP or SMTP to convey replication data
c. Has to be manually configured
d. Occurs between two domain controllers that are called bridgeheads or bridgehead servers

AD DS partitions

Replicated data is housed within the following Active Directory Domain Partitions:

Configuration partition data:

- created automatically when you create the first domain of a forest
- Contains object relating to domain structure and replication topology and is replicated to each domain controller in a domain and in a forest**.**
- stores information about forest-wide services such as Dynamic Host Configuration Protocol (DHCP) authorization and certificate templates

***Schema partition data*:**

Schema partition data include definitions of all the objects and attributes that you can create in Active Directory and is replicated to each domain controller in domains/forests. AD DS contains a default set of classes and attributes that you cannot modify. However, if you have Schema Admins credentials, you can extend the schema by adding new attributes and classes to represent application-specific classes. Only the schema master is permitted to make additions to classes and attributes.

***Domain partition data*:**

- When you create a new domain, AD DS automatically creates and replicates an instance of the domain partition to all of the domain’s domain controllers.
- Contains information about all domain-specific objects, including users, groups, computers, organizational units (OUs), and domain-related system settings.

***Application partition data*:**

- Applications and services store data in the application partition.
- When you create a new domain, AD DS automatically creates and replicates an instance of the domain partition to all of the domain’s domain controllers.
- The application partition stores nondomain, application-related information that may have a tendency to be updated frequently or have a specified lifetime.

AD DS replication within a single site – Intrasite Replication

The following concepts are related to intrasite replication:

1. Connections objects
2. The knowledge consistency checker
3. Notification
4. Polling

Connection Objects

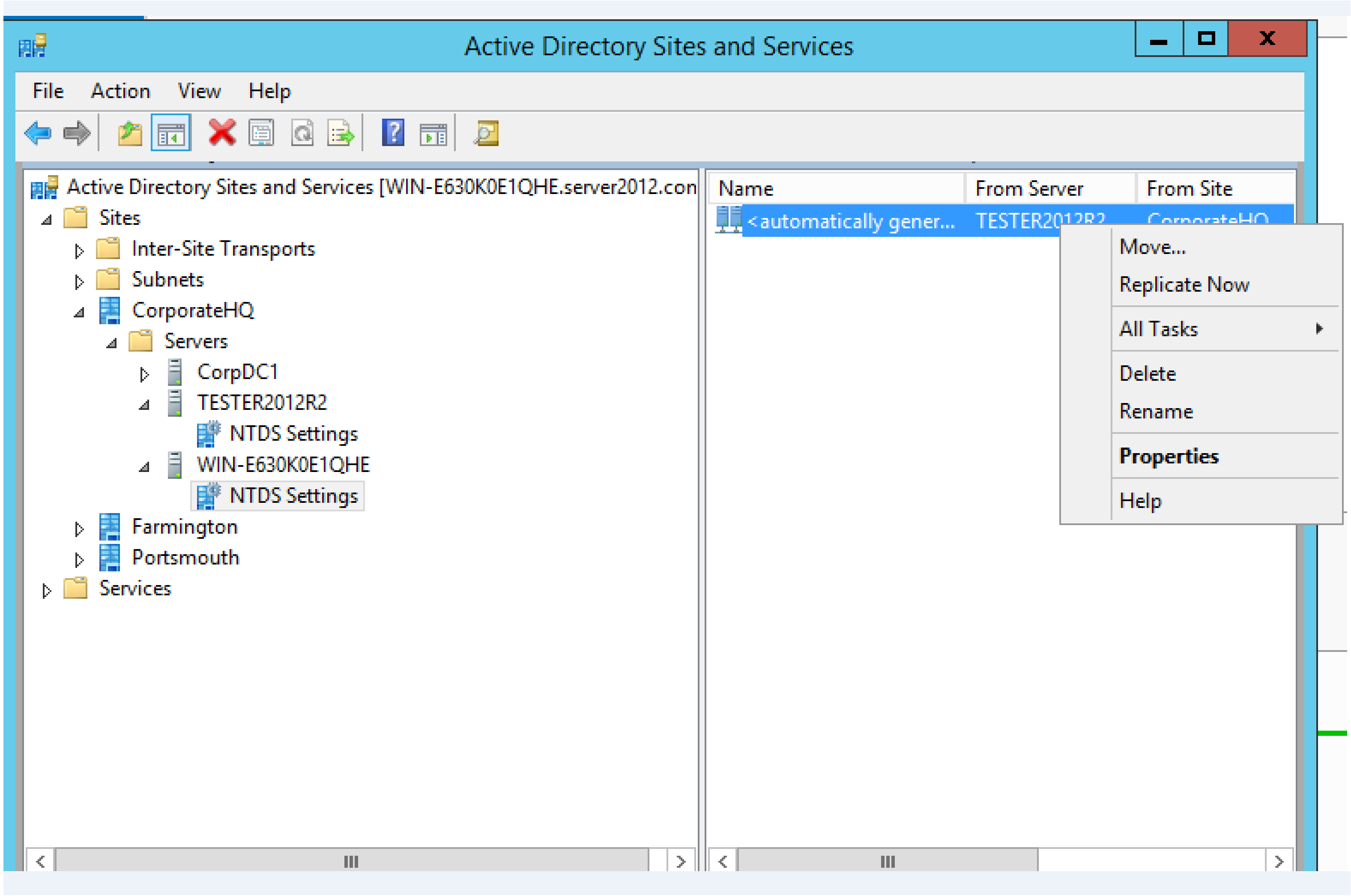
- A domain controller that replicates changes from another domain controller is called a **replication partner**.
- Replication partners are linked by **connection objects**.
- A connection object **represents a replication path from one domain controller to another.**
- Connection objects are **one-way, representing inbound-only pull** replication
- The connection object identifies the replication source server, contains a replication schedule, and specifies a replication transport.
- You can right click on the properties of the connection object to change the replication schedule

To view and configure connection objects:

1. open Active Directory Sites and Services, and then select the NTDS Settings container of a domain controller’s server object.
2. You can force replication between two domain controllers by right clicking the connection object, and then selecting **Replicate Now**.
3. Note that replication is inbound-only, so if you want to replicate both domain controllers, you need to replicate the inbound connection object of each domain controller.

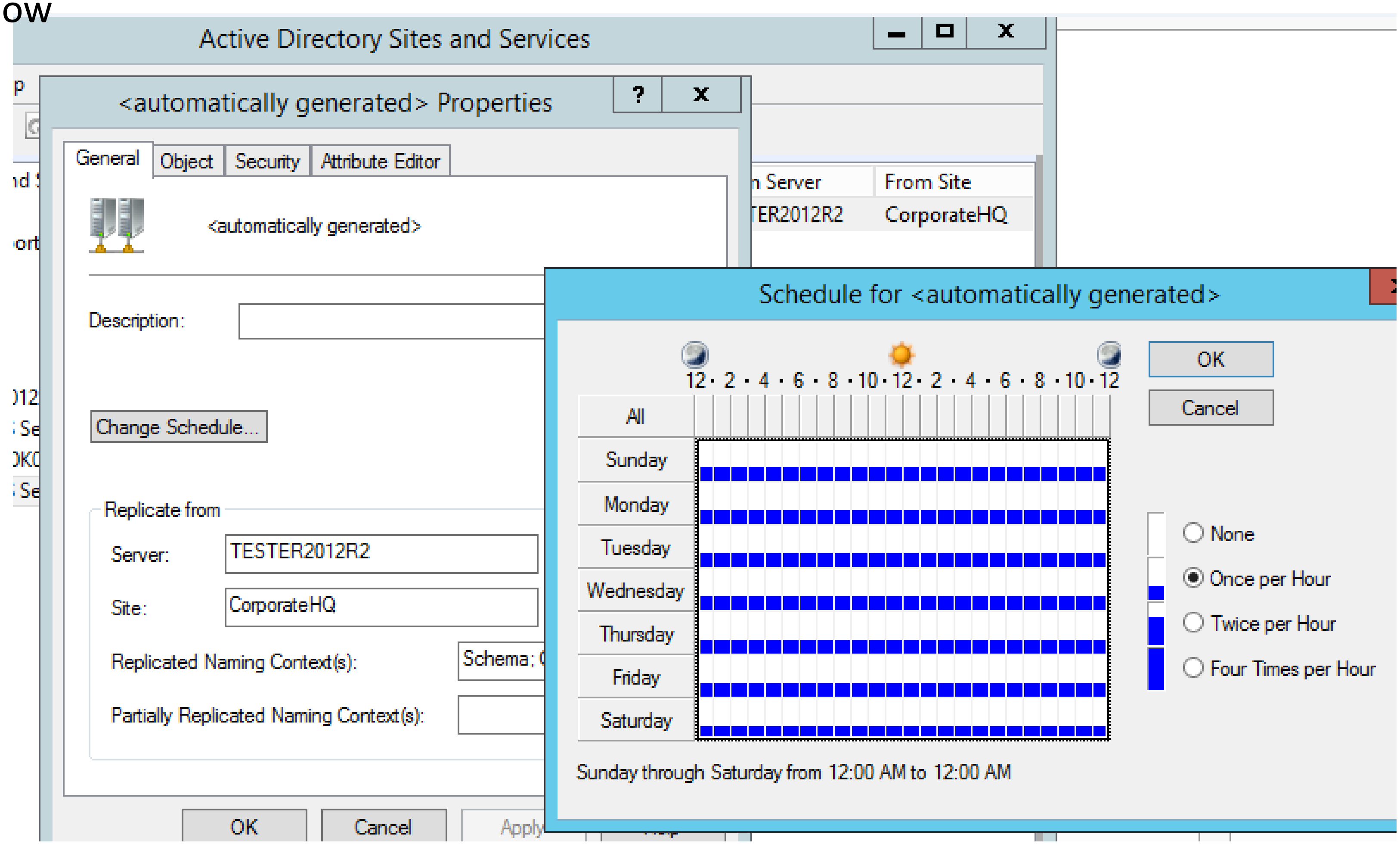
Let’s take a look:

In the corporateHQ site in the servers container we have TESTSERVER2012R2 and WIN-E630 Under both servers we have NTDS Settings. The Win-E630 is the replication partner of Tester. If you click on the NTDS Settings under Win-E630 you will see the connection object in the left pane. The replication is automatically generated but you can left click on the connection Object and say replicate now



Name	From Server	From Site
<automatically gener...	TESTER2012R2	CorporateHQ

You can right click on the properties of the connection object (screen shown above) to change the replication polling schedule. You will be presented with the screen below



Active Directory Sites and Services

<automatically generated> Properties

<automatically generated>

Description:

Replicate from

Server: TESTER2012R2

Site: CorporateHQ

Replicated Naming Context(s): Schema; (

Partially Replicated Naming Context(s):

Schedule for <automatically generated>

○ None

● Once per Hour

○ Twice per Hour

○ Four Times per Hour

Sunday through Saturday from 12:00 AM to 12:00 AM

The Knowledge Consistency Checker

- On each domain controller, a component of AD DS called the **knowledge consistency checker (KCC)** helps generate and optimize the replication automatically between domain controllers within a site

- The KCC evaluates the domain controllers in a site, and then creates connection objects to build the two-way, three-hop topology

- If you add or remove a domain controller, or if a domain controller is not responsive, the KCC rearranges the topology dynamically, adding and deleting connection objects to rebuild an effective replication topology

- You can manually create connection objects to specify replication paths that should persist. However, creating a connection object manually is not typically required or recommended

- The KCC will also not remove manual connection objects, which means that you must remember to delete connection objects that you create manually

Notification

- When a change is made to an Active Directory partition on a domain controller, the domain controller queues the change for replication to its partners
- By default, the source server waits 15 seconds to notify its first replication partner of the change
- **Notification** is the process by which an upstream partner informs its downstream partners that a change is available.
- By default, the source domain controller then waits three seconds between notifications to additional partners. These delays, called the *initial notification delay* and the *subsequent notification delay*, are designed to stagger the network traffic that intrasite replication can cause.
- Upon receiving the notification, the downstream partner requests the changes from the source domain controller, and the directory replication agent pulls the changes from the source domain controller

Polling

Lets suppose that a domain controller did not make any changes to its replicas for an extended time, particularly during off hours. This means that its downstream replication partner, will not receive notifications from that source domain controller. Thesource Somain controller might be offline, which would prevent it from sending notifications to downstream replication partner.

It is important for the downstream replication partner to know that its upstream partner is online and simply does not have any changes. This is achieved through a **process called polling.**

During polling, the downstream replication partner contacts the upstream replication partner with queries as to whether any changes are queued for replication.By default, the **polling interval for intrasite replication is once per hour**.

You can configure the polling frequency from a connection object's properties by clicking **Change Schedule**, although it is not recommended.

Replication Conflicts

Typically, there are three types of replication conflicts that may occur in AD DS:

- modifying the same attribute value of the same object on two domain controllers at the same time. For example changing the password of a user at the same time on two DCs.
- Adding or modifying the same object on one domain controller at the same time that the container object for the object is deleted on another domain controller
- Adding objects with the same relative distinguished name into the same container

Solving the Conflict

- all domain controllers in the forest record and replicate object changes at the attribute level rather than at the object level
- Therefore, changes to two different attributes of an object, such as the user's password and postal code, do not cause a conflict even if you change them at the same time from different locations.
-

The following table outlines several conflicts, and describes how AD DS resolves the issue

Conflict	Resolution
Attribute value	If the version number value is the same, but the attribute value differs, then the timestamp is evaluated. The update operation that has the higher stamp value replaces the attribute value of the update operation with the lower stamp value.
Add or move under a deleted container object, or the deletion of a container object	After resolution occurs at all replicas, AD DS deletes the container object, and the leaf object is made a child of the folder's special LostAndFound container. Stamps are not involved in this resolution.
Adding objects with the same relative distinguished name	The object with the larger stamp keeps the relative distinguished name. AD DS assigns the sibling object a unique relative distinguished name by the domain controller. The name assignment is the relative distinguished name + CNF: + a reserved character (the asterisk,) + the object's GUID. This name assignment ensures that the generated name does not conflict with any other object's name.

Replication Topology

- Replication topology is the route by which replication data travels through a network. To create a replication topology, AD DS must determine which domain controllers replicate data with other domain controllers

- AD DS replicates schema and configuration partitions to all domain controllers.
- Domain controllers in the same domain also replicate the domain partition
- Domain controllers that host an application partition also replicate the application partition.
- Domain controller may have several replication partners for different partitions.

How the Schema and Configuration Partitions Are Replicated

Replication of the schema and configuration partitions follows the same process as all other directory partitions. However, because these partitions are forest-wide rather than domain-wide, **connection objects for these partitions may exist between any two domain controllers regardless of the domain controller’s domain**. Furthermore, the replication topology for these partitions includes all domain controllers in the forest.

How the Global Catalog Affects Replication

The configuration partition contains information about the site topology and other global data for all domains that are members of the forest. **AD DS replicates the configuration partition to all domain controllers through normal forest-wide replication.** Each global catalog server obtains domain information by contacting a domain controller for that domain and obtaining the partial replica information. The configuration partition also provides the domain controllers with a list of the forest’s global catalog servers.

Global catalog servers register DNS service records in the DNS zone that corresponds to the forest root domain. These records, which are registered only in the forest root DNS zone, help clients and servers locate global catalog servers throughout the forest to provide client logon services.

Sysvol Replication

- Domain controllers use a special shared folder named SYSVOL to replicate logon scripts and Group Policy object files to other domain controllers.

- The contents of the SYSVOL folder replicate to every domain controller in the domain using the connection object topology and schedule that the KCC creates.

- Windows 2000 Server and Windows Server 2003 use File Replication Service (FRS) to replicate SYSVOL, whereas Windows Server 2008 and up use the newer DFS Replication service when in domains that use the Windows Server 2008 domain functional level, and FRS for domains that run older domain functional levels.

- **Note:** You can use the dfsrmig.exe tool to migrate SYSVOL replication from the FRS to DFS Replication. For the migration to succeed, the domain functional level must be at least Windows Server 2008.
-