# CP List-02

1. What is USN?

Active Directory uses Update Sequence Numbers (USNs) to track updates. USNs are generated by each domain controller’s local counter, so it’s reliable compared to ‘Timestamp’.

It’s consisted of Local USN, USN changed (Highest USN), Originating USN (Travel with replication)

1. What is Lost and found?

It’s a container for orphaned object. For example, two actions happened on two DC at the same time. Adding *x* object to *y* container on DC A, and removing y container on DC B. Then, x object would be an orphaned object which will be stored in *lostandfound* container.

1. Explain AD Replication conflicts.

An attribute is changed on DC A. Before the replication process someone change the same attribute, then there will be a replication conflict that which attribute should Active Directory choose.

Active Directory solves this kind of problem by attaching the unique stamp which is consisted of version, originating time, originating domain controller’s GUID.

ver > ori time > ori dc guid

1. Explain intrasite replication and intersite replication

Intra-site replication

That means the replication between Domain Controllers in the same site by connecting all the Domain Controllers together in a ring. Replication happens 15 seconds after a change. There will be no more than 3 hops between two domain controllers, so any domain controller can get the change in a minute.

Inter-site replication

You have to manually create a site links to connect sites, then bridgehead server which is automatically selected replicates between domain controllers in different sites. Bridgehead server can be configured manually, but if the configured one is not available, replication will not occur at that site.

1. What is Site？

Site is a group of well-connected computers, and site can model a physical network to some extent. It’s an efficient way to control network traffic according to the connectivity status. The inter-site replication will be less latency, and the intra-site replication can be scheduled.

1. What is Multi-master replication?

Multi-master means that all domain controllers within a domain are equivalent. They are connected by a robust set of connections.

* Easy to update
* Reduce network traffic
* Fault tolerance
* Handle more queries

1. In what kind of condition can the parent domain and child domain replicate each other?

When schema or configuration directory partition changes, and also application directory partition, such as DNS integrate zone.

1. What is GUID? The GUIDs under NEDS, server and invocation are the same one？

objectGUID:

That’s called DSA GUID which is used to identify a DC, and this GUID will not change unless the DC is demoted or re-promoted

invocationId:

That’s Active Directory Database’s (ntds.dit) GUID which is used to identify the database, so in that case the same database will have the same invocationId. Invocation ID will change when Active Directory is restored.

1. What is USN rollback

The reason why USN rollback occurs is that Active Directory keep track of changes by USN to determine if the updates will be accepted.

For example:

1. DC 1’s USN is 5, then take a snapshot.
2. DC 1 does some update, and the USN goes to 9
3. Other DCs get the change and record the DC 1’s USN which is 9.
4. DC 1 rolls back the snapshot. The USN goes back to 5 again.
5. DC 1 makes several changes. The USN is 8.
6. Other DCs get confused when they start to replicate from DC 1.
7. What partitions can be replicated between parent domain and child domain?

Schema directory partitions, configuration directory partitions and application directory partitions.

1. What ports would be needed during the process of replication?

TCP port 135: RPC (Remote Procedure Call)

TCP,UDP port 389: LDAP

TCP port 3268: Global Catalog LDAP

TCP, UDP port 53: DNS

TCP, UDP port 88: Kerberos

TCP port 445: SMB

1. Explain Urgent replication

Certain important security and time sensitive changes to objects and settings trigger Urgent Replication, overriding existing change notification and schedule settings.

The following Events will trigger an immediate change notification on all DC within a site:

Assigning Account Lockout

Changing the password on a DC

Changing the Account Lockout and Domain Password policy

Changing LSA secret

Changing RID master role

1. what is KCC

Knowledge Consistency Checker (KCC)

It’s a built-in process which will generate and modify the replication topology.

By default, KCC will run every 15 minutes. It can be changed by modifying registry. Server objects and NTDS Settings objects are required by the KCC to run.

Enforce running:

repadmin /kcc

repadmin /istg

1. Bridge head server? The benefits of bridge head server.

Bridgehead server is the server which is responsible for inter-site replication. It can be selected automatically by KCC or configured manually.

The benefit of bridgehead server is that when replication occurs between sites, we only need one configured link to perform that process. Because the connection between sites are WAN, it’s slow and unstable compared to fast LAN. Bridgehead servers help us control the inter-site replication and reduce the bandwidth.

1. 站点间的DC--ISTG ?

Inter-site Topology Generator is a component of KCC.

ISTG is responsible for create connection object between sites. You have to configure sites, site link at first, then ISTG can perform its responsibility.

ISTG role is selected automatically, the first domain controller in the site will get the role. If the current ISTG server is unavailable, the system will choose the first Windows Server 2003 domain controller in a list sort by DC’s GUID (if there is no Windows Server 2003, go Windows 2000).

1. Connection object ?

It’s a child of NTDS settings object which defines one-way inbound route. The KCC will automatically creates connection object according to the information in Sites and Services. Attributes of a connection object is name, From Server, From Site. The manually created connection object or we can say the connection’s name is not ‘<automatically generated>’, then the connection object will not be automatically configured by the KCC any more.