Windows Server 2012 Directory Partition Containers- A Walk Through

Introduction:

Active Directory Users and Computers form a centralized management console to manage User objects, computer objects, Groups, Service accounts, Security Principals, Trusted Platform Module Devices, Application information, Organizational Units, per domain operational information etc.

Windows Server 8 Active directory has following directory partitions such as

- Schema Partition
- Configuration Partition
- Domain Partition

What are the New Containers?

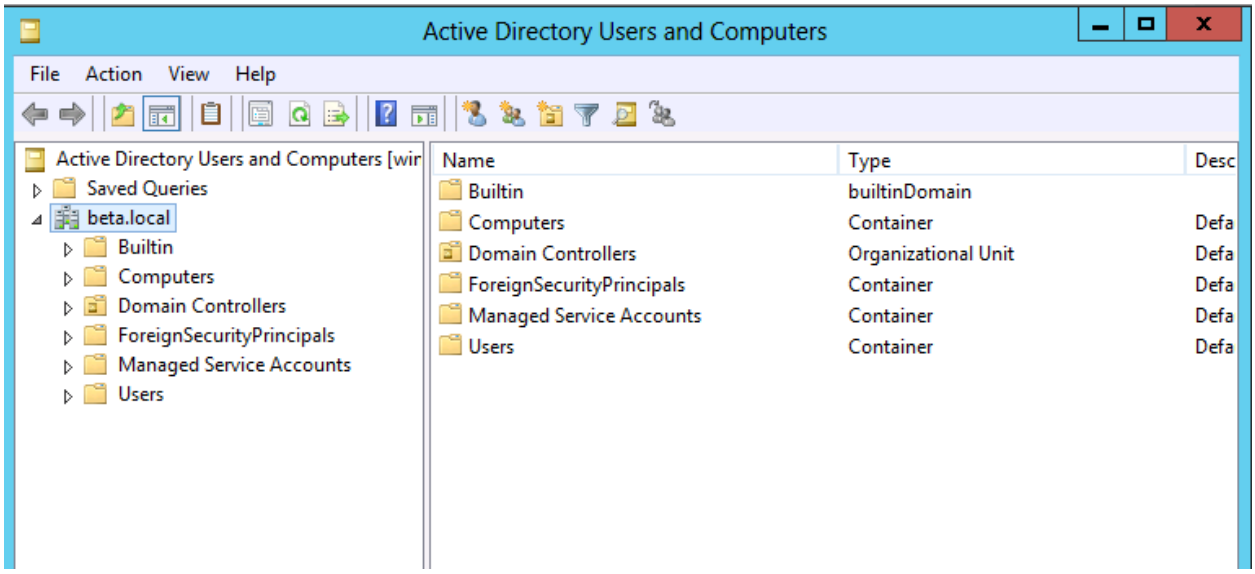
Most of the containers which are part of Windows 2008 R2 Directory Partition are brought to Windows Server 2012 Directory Partition. One of the new container which got added is **TPM Devices.**

In this document we will verify the default containers created under Domain Partition. The Domain Partition stores User object, groups, computer objects and other objects. The data gets replicated across the Domain controllers within the domain and to the Global catalog servers if the object is mark for GC replication.

Following are the child containers which can be viewed at Active directory Users and Computers snap-in or when you launch DSA.msc snap-in.

Note: user should be part of **Domain admins** group / **Enterprise admins** group to launch ADUC / Dsa.msc, or an appropriate delegation should be set for the user. The recommended and usual practice is to load the RSAT utilities and launch the ADUC snap-in for non-domain administrator accounts

The default Containers in Windows Server 8 Directory partition is classified as **Basic View** and **Advanced View.** We would run through the **Basic view** and their functionality. Below diagram shows the **Basic view** containers.



a) ***Builtin*** *:This container consists of default Groups such as*
To view the ***Builtin*** *container, navigate to* ***Start → Active Directory Users and Computers*** *or from the command prompt* ***Start → Run → Dsa.msc***

Following are the Groups which can be viewed under the container.

Name	Type	Description
Access Control Assistance Operators	Security Group - Domain Local	Members of this group can remotely query authorization attributes and permissions for resources on this computer.
Account Operators	Security Group - Domain Local	Members can administer domain user and group accounts
Administrators	Security Group - Domain Local	Administrators have complete and unrestricted access to the computer/domain
Backup	Security Group -	Backup Operators can override security restrictions for the

Operators	Domain Local	sole purpose of backing up or restoring files
Certificate Service DCOM Access	Security Group - Domain Local	Members of this group are allowed to connect to Certification Authorities in the enterprise
Cryptographic Operators	Security Group - Domain Local	Members are authorized to perform cryptographic operations.
Distributed COM Users	Security Group - Domain Local	Members are allowed to launch, activate and use Distributed COM objects on this machine.
Event Log Readers	Security Group - Domain Local	Members of this group can read event logs from local machine
Guests	Security Group - Domain Local	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	Security Group - Domain Local	Members of this group have complete and unrestricted access to all features of Hyper-V.
IIS_IUSRS	Security Group - Domain Local	Built-in group used by Internet Information Services.
Incoming Forest Trust Builders	Security Group - Domain Local	Members of this group can create incoming, one-way trusts to this forest
Network Configuration Operators	Security Group - Domain Local	Members in this group can have some administrative privileges to manage configuration of networking features
Performance Log Users	Security Group - Domain Local	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	Security Group - Domain Local	Members of this group can access performance counter data locally and remotely
Pre-Windows 2000 Compatible Access	Security Group - Domain Local	A backward compatibility group which allows read access on all users and groups in the domain
Print Operators	Security Group - Domain Local	Members can administer domain printers
RDS Endpoint Servers	Security Group - Domain Local	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	Security Group - Domain Local	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

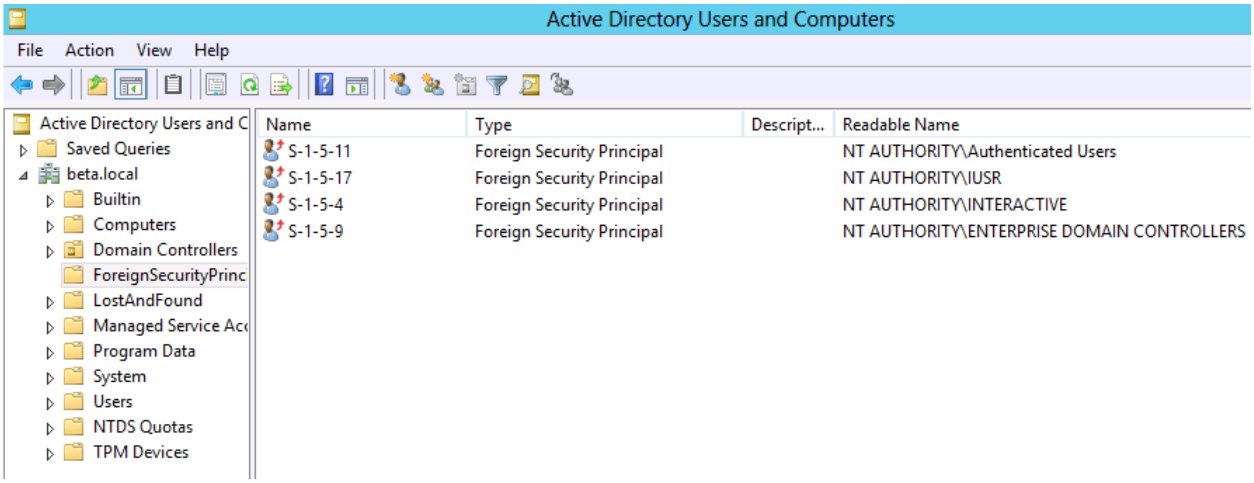
		group.
RDS Remote Access Servers	Security Group - Domain Local	Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. In Internet-facing deployments, these servers are typically deployed in an edge network. This group needs to be populated on 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	Security Group - Domain Local	Members in this group are granted the right to logon remotely
Remote Management Users	Security Group - Domain Local	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	Security Group - Domain Local	Supports file replication in a domain
Server Operators	Security Group - Domain Local	Members can administer domain servers
Terminal Server License Servers	Security Group - Domain Local	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	Security Group - Domain Local	Users are prevented from making accidental or intentional system-wide changes and can run most applications
Windows Authorization Access Group	Security Group - Domain Local	Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects

b) ***Computers:*** *This container stores computer objects. Most organizations has their dedicated OU structure built below the default containers, so that computer objects belongs to different departments can be staged accordingly. The famous tools such as* ***Redircmp.exe*** *are still valid and can be used to redirect computer objects to different OU respectively.*

c) ***Domain Controllers:*** *The container stages the Domain controller computer objects, administrators cannot rename this container. It is not recommended to move Domain controller computer objects out of* ***Domain Controllers*** *container.*

d) ***Foreign Security Principal:*** *The container stores the security principal from different Active directory forest. Example: When user from trusted Forest A wants to access resources from Forest B Domain controller under Forest B will create Foreign security principal for the user. And further the administrator can add the user to Domain local group to manage the resources efficiently.*

Some of the pre-defined Foreign Security Principal can be viewed by enabling the **Advance** View from **ADUC** snap-in, as shown below

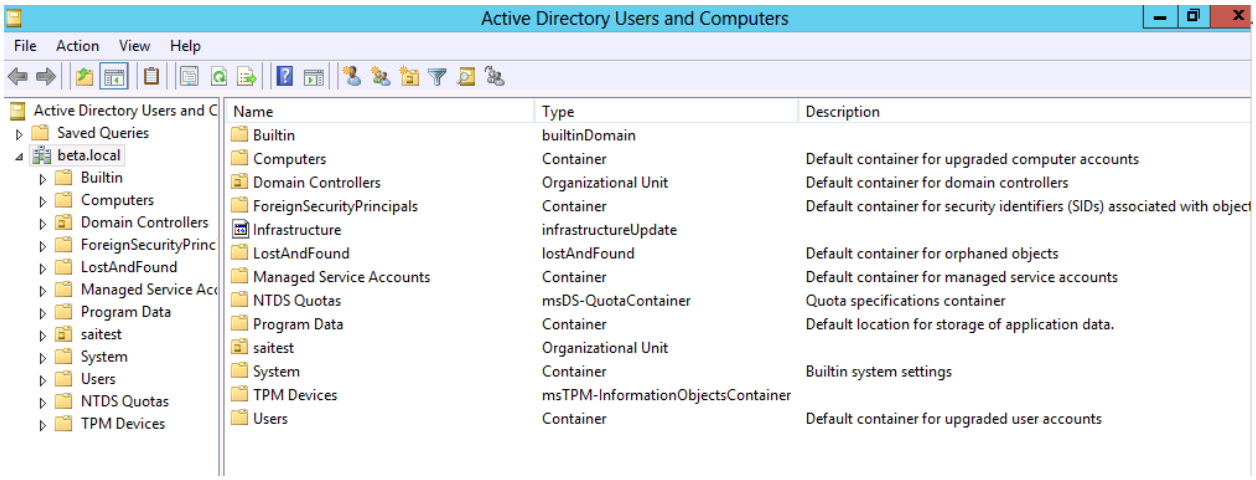


To understand more about the Security Principals, I would like to

e) ***Manage Service****: It was introduced in Windows Server 2008 R2 and Windows 7 , and now available on Windows 8 and Windows Server 2012. To have a simplified SPN management , administrators can rely on MSA (managed service accounts). Manage service account can be added into security groups.*

f) ***User Container:*** *Users created under a domain are automatically placed under the* ***User container.*** *Groups in this container as have* ***Domain local*** *and* ***Global Scope.*** *But it is always advisable to have your own OU hierarchy.*

Below diagram shows the **Advanced View** containers in Active directory Users and Computers Snap-in.

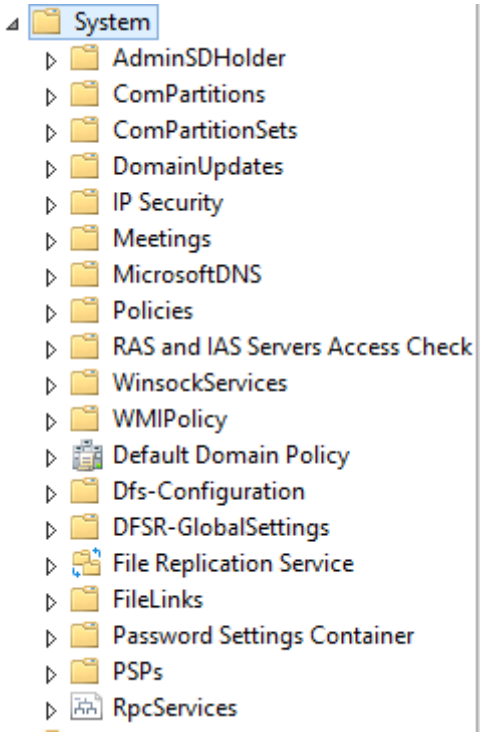


The above wizard exposes few additional containers such as

g) ***Lost and Found :*** *This container is part of directory partition of each Active directory domain. This container manages the orphan objects. Example: If an User / computer object is created under an OU and the same OU is deleted on another domain controller, in these conditions the object will be placed under* ***Lost and Found*** *container.*
To check the Object parent location , check the ***Last Known Parent attribute*** *value.*

h) ***Program Data:*** *It is an empty container which allows applications to store application related data. Eg: ADFS related information.*

i) ***System*** *Container: This container stores information about Microsoft application service accounts and system accounts. Administrators cannot create a Sub OU underneath the* ***System*** *container. When administrator install Directory aware Microsoft application, a container gets automatically gets created under* ***system*** *directory. The sample structure is shown below*



j) ***NTDS Quota:*** *NTDS quota is used to store objects which are configured to limit the number of AD objects that can be created. For eg: I can limit my account to create 50 objects in AD. There is not GUI based solution to set the NTDS quota. Administrators have to rely on DSAdd, DSMod or DSQuery to add , modify , view or delete the quotas.*

k) ***TPM Device*** *: This is the new container introduced in Windows Server 2012, this container stores the recovery information for a Trusted Platform Module Device*

Summary: ADUC used to efficiently manage the Active Directory objects. In this article we have walk through the new AD containers in Windows server 2012 and outlined the Active directory Containers with new information and few real world examples.