Agenda

Under the hood of Active Directory

On objects, attributes, replication, multi-master and flexible single master operations

The role of Active Directory

On network services and in the most basic of features towards end users

Best practices

When deploying Active Directory

Domain Controllers

Installed with Windows Server
Physical hosts
Virtual machines

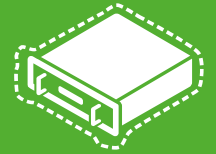## Configured with Server Roles and Features
Active Directory Domain Services role
Active Directory Domain Services management tools

Two types of Domain Controllers exist*
Read/write Domain Controllers
Read-only Domain Controllers

Grouping of Domain Controllers

Active Directory Sites
Geographic sites with high-speed connectivity
Sites govern replication and authentication traffic

Active Directory Domains
Containers of replication
Identified by a DNS domain name

Active Directory Forests
Collection of one of more domains
Forest shares a single Active Directory schema

The Active Directory database

NTDS.dit and supporting files
Definition of objects
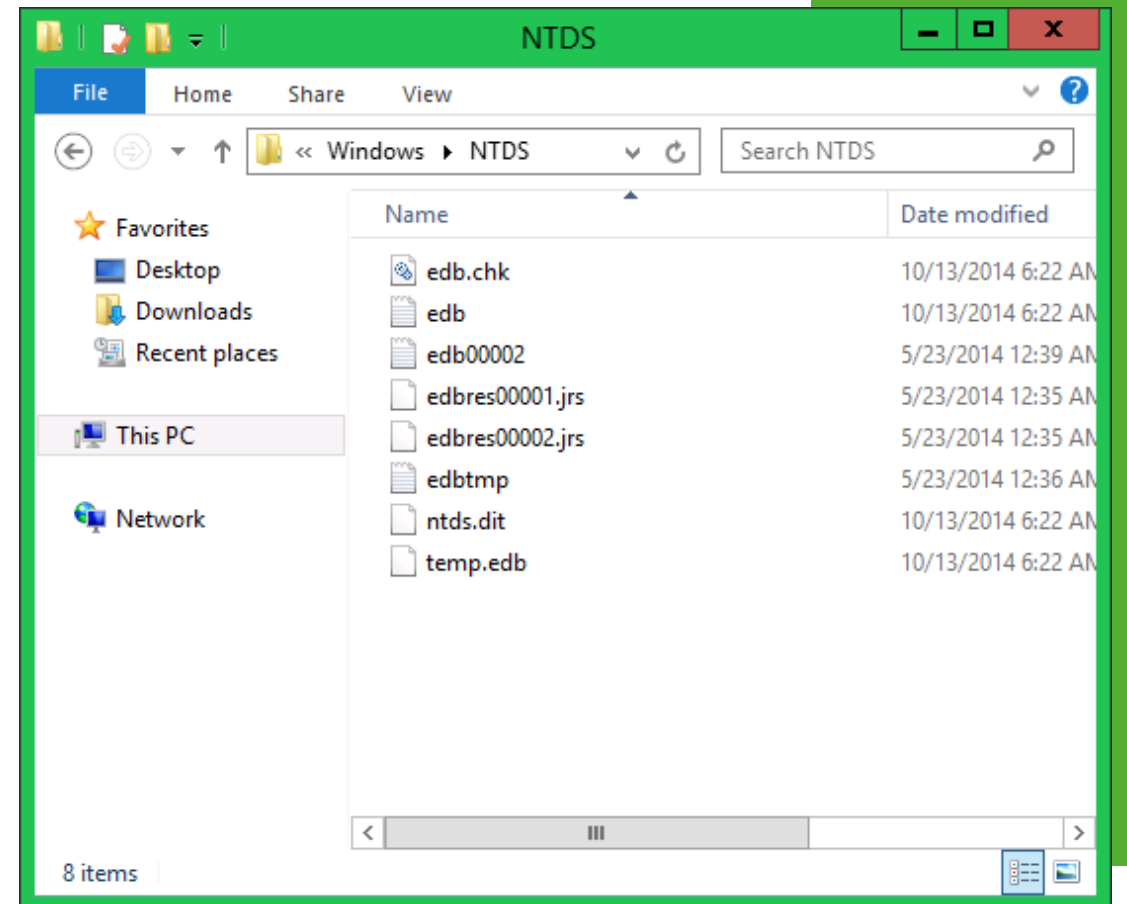Configuration of objects

Schema
Definition of object classes and relations
Definition of behavior and rights

Configuration
Objects in Active Directory themselves
Attributes for objects

Inside the database

Objects
User objects, computer objects, etc.
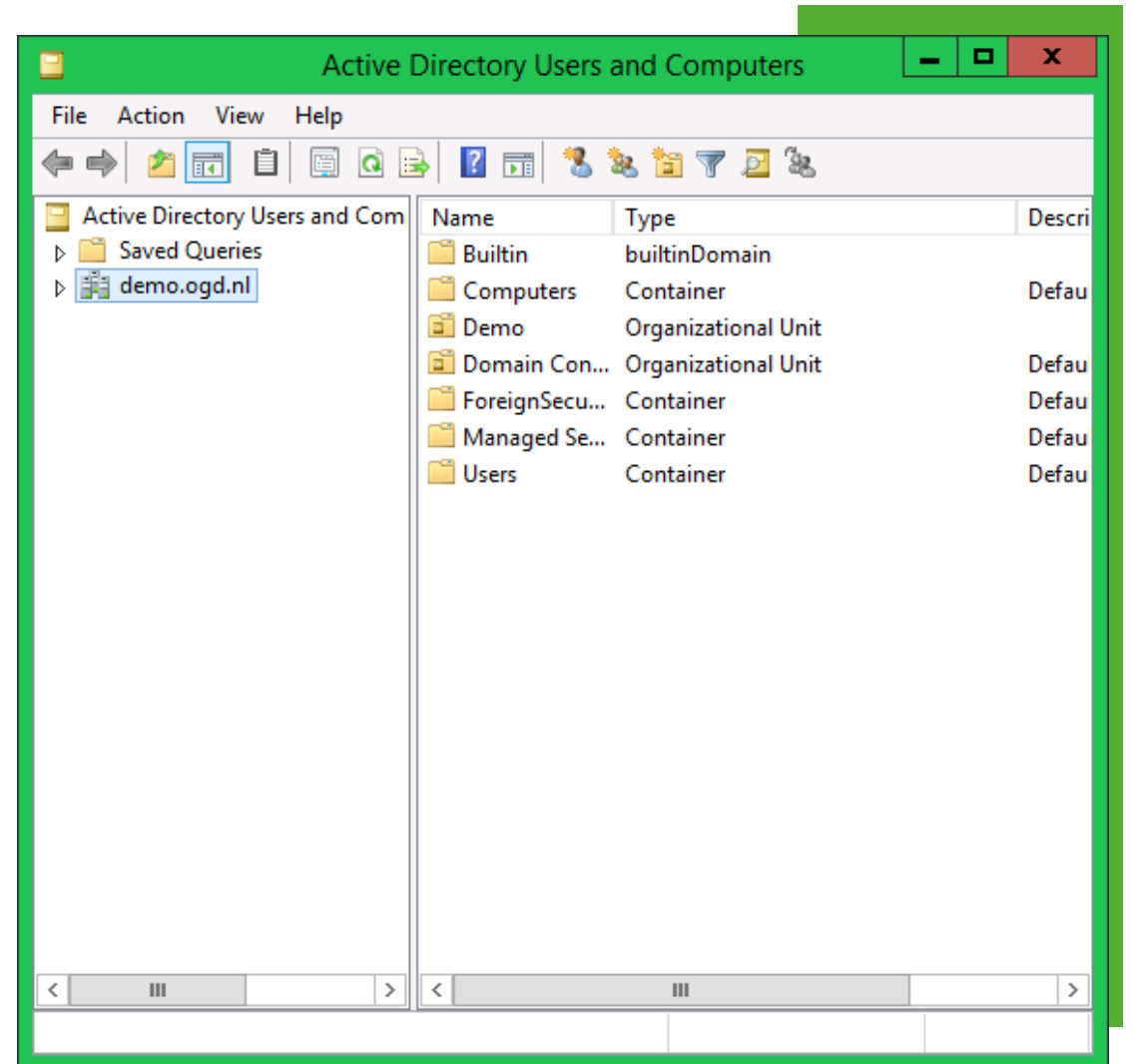Identified with Security Identifiers (SIDs)

Containers
Containers
Organizational Units

Attributes
Properties for objects
Single valued vs. multi-valued attributes

Replication and High Availability

Intrasite replication

Change notifications with pull replication
Two-way ring topology

Intersite replication
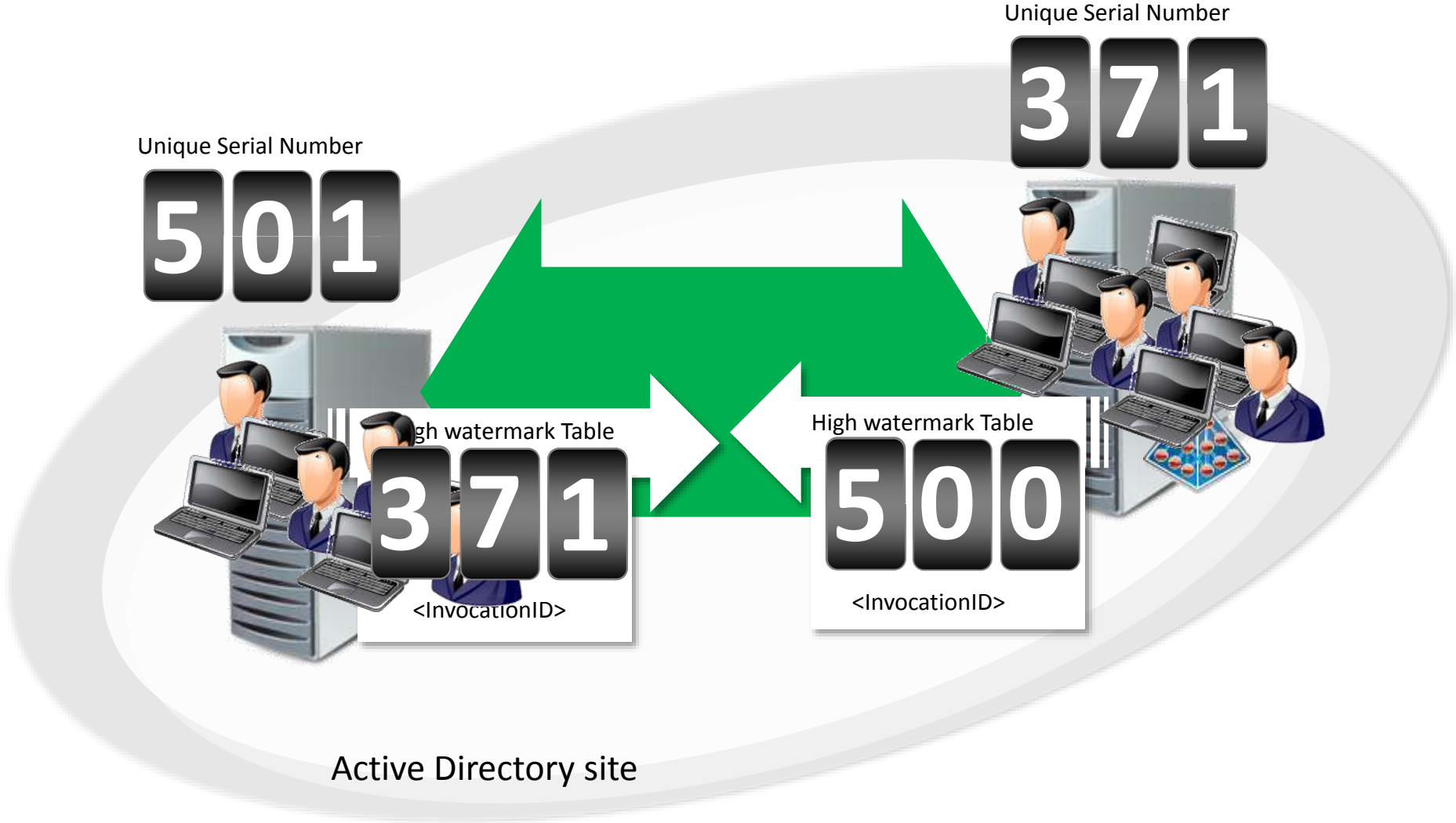
Schedule-based pull replication
Bridgehead to bridgehead server

Knowledge Consistency Checker (KCC)

Responsible for the replication topology
Alternatively, you can manually modify the topology

Unique Serial Number

371

Unique Serial Number

501

High watermark Table

371

<InvocationID>

High watermark Table

500

<InvocationID>

Active Directory site

Multi-master and FSMO Roles

Everything is awesome!

Changes can be made on every Domain Controller
Changes are replicated to all Domain Controllers in scope

Flexible Single Master Operations (FSMO) Roles

FSMO Role	Scope
Primary Domain Controller emulator	Domain
RID Pool master	Domain
Infrastructure master	Domain
Schema master	Forest
Domain naming master	Forest

The role of Active Directory

On network services and in the most basic of features towards end users

Networking Services

Domain Name System (DNS)
DNS Domain names for domains
DNS Zones and records

Dynamic Host Configuration Protocol (DHCP)
DHCP Authorization
DHCP and Dynamic DNS

3rd party services
LDAPS for standards-based quering of Active Directory
RADIUS for pre-authentication by routers, firewalls, etc.

Active Directory

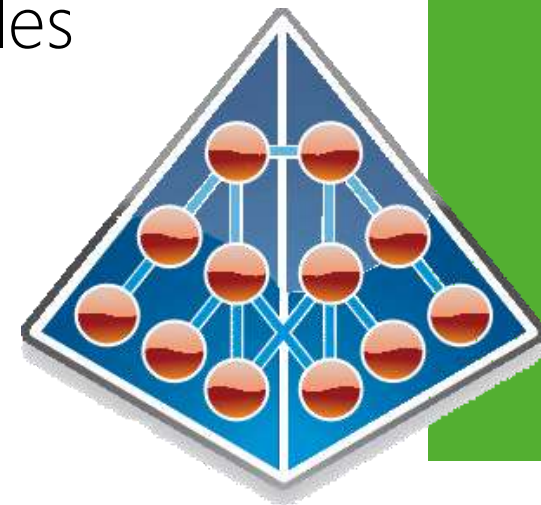Device-independent productivity

On-premises Single Sign-On

Cloud Single Sign-On

Centralized Systems Management

Consistent User Experience

Distributed File System for optimized access to files

Best Practices

When deploying Active Directory

Best practices for planning Domain Controllers

Intend to create at least 2 Domain Controllers per domain.

Domain Controllers automatically offer High Availability
Domain Controller resiliency is easily achieved

Intend to implement server role separation.

Don't misuse Domain Controllers as IIS Servers or SQL Servers.
(unless it's Windows Small Business Server)

Use hardware and software still covered by the producers (extended) guarantee, support for the period in which you need to rely on the Domain Controller.

Best practices for placing Domain Controllers

Properly dimension the server's hardware and software.

Use RAID and separate spindles for storage of Active Directory data.
Use the Infrastructure Planning & Design (IPD) Guide

When the DC is a VM, have the correct procedures in place.

Always run sysprep.exe when working with Windows Server templates.
Don't let virtualization admins ruin your Active Directory

Before you install Windows Server, run the Memory Diagnostics from the Windows Server DVD.

Possible memory corruption issues show early this way.

Best practices for promoting Domain Controllers

Document passwords

Document the Directory Services Restore Mode password
The built-in Domain Admin password

Implement information security measures

Install and configure anti-malware, ups, monitoring agents, etc.
Follow vendor's best practices on exclusions and configuration

To promote Domain Controllers, use answer files.

Write them, get them checked, signed off and then use them.
Include them in your documentation after you've used them.

After you've promoted your Domain Controllers

Check the logs

Check C:\Windows\debug\dcpromo.log
Check C:\Windows\debug\dcpromoui.log

Run Windows Update after promotion.

You will only be offered Active Directory-specific updates, after promoting a Windows Server installation to a Domain Controller

Run the Active Directory Best Practices Analyzer

The Best Practices Analyzer warns you for misconfigurations.
Recommendations may protect you against 90% of data loss scenarios.

Concluding

Concluding

Active Directory consists of many components

These components make up an entire identity solution
High Availability is achieved through multi-master replication

Active Directory plays an important role in your infrastructure

Network services like DNS and DHCP benefit from Active Directory
Colleagues benefit from device-independent SSO and management

Best Practices for Active Directory

Think before you act.
Don't forget to document.

👍 Thank you!