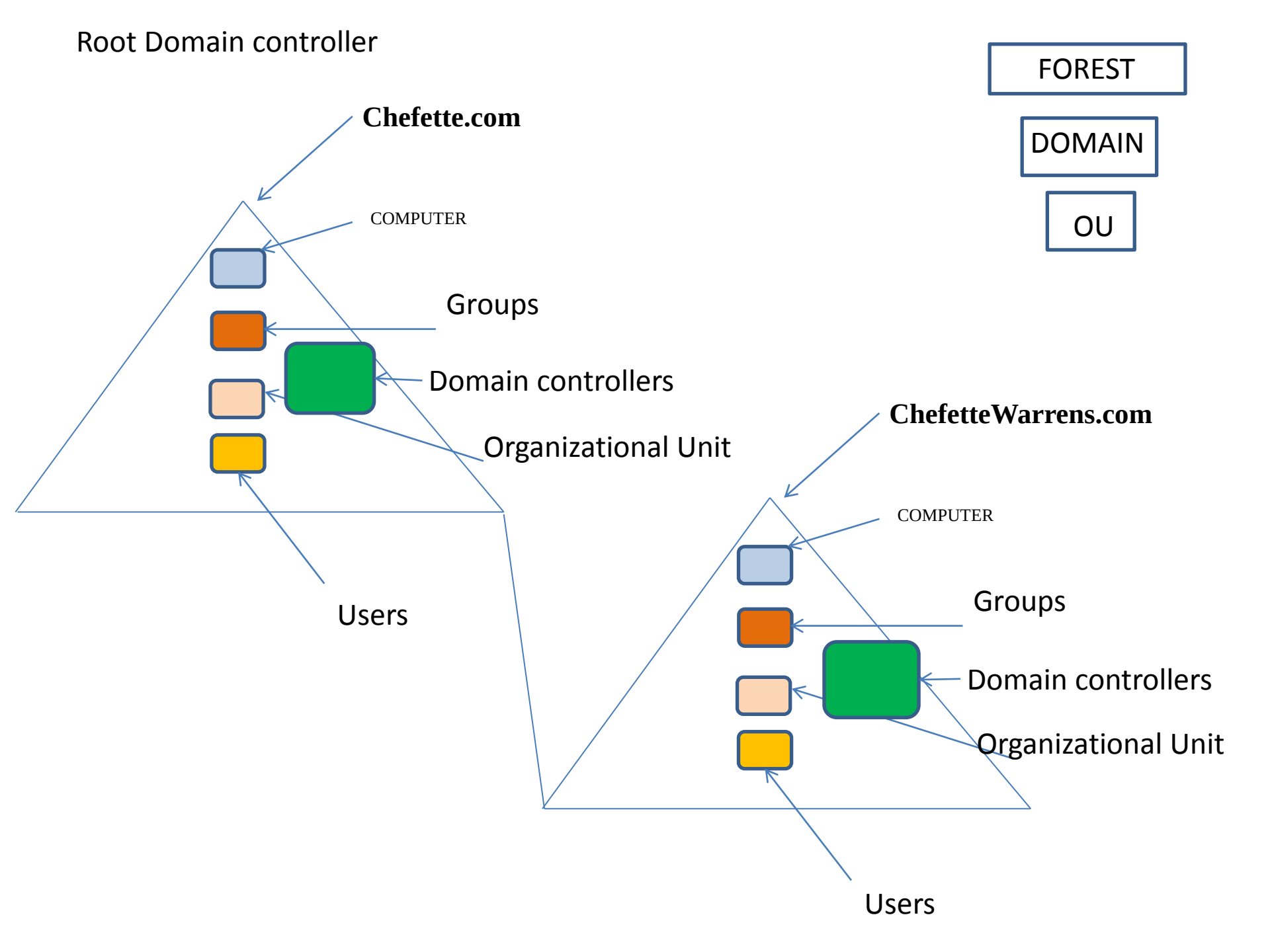
Domain Structure

Server 2012R2


Root Domain controller
FOREST
DOMAIN
OU
Chefette.com
COMPUTER
Groups
Domain controllers
Organizational Unit
Users
ChefetteWarrens.com
COMPUTER
Groups
Domain controllers
Organizational Unit
Users

What Are AD DS Domains?

- AD DS requires one or more domain controllers
- All domain controllers hold a copy of the domain database, which is continually synchronized
- The domain is the context within which user accounts, computer accounts, and groups are created
- The domain is a replication boundary
- The domain is an administratice center for configuring and managing objects
- Any domain controller can authenticate and sign-in anywhere in the domain
- The domain provides authorization

The AD DS Domain Contains User, Computers, Groups

- An AD DS domain is a logical container used to manage user, computer, group, and other objects.
- All of the domain objects are stored in the AD DS database, a copy of which is stored on each domain controller.
- There are many types of objects in the AD DS database, including user accounts, computer accounts, and groups. The following list briefly describes these three object types:

User accounts. User accounts contain the information required to authenticate a user during the sign-in process and build the user's access token.

Computer accounts. Each domain-joined computer has an account in AD DS. Computer accounts are used for domain-joined computers in the same ways that user accounts are used for users.

Groups. Groups are used to organize users or computers to make it easier to manage permissions and group policy in the domain.

The AD DS Domain Is a Replication Boundary

When changes are made to any object in the domain, the domain controller where the change occurred replicates that change to all the other domain controllers in the domain. If there are multiple domains in the forest, only subsets of the changes are replicated to other domains. AD DS uses a multimaster replication model that allows every domain controller to make changes to objects in the domain. Changes to relative identifier (RID) management in the Windows Server 2012 version of Active Directory Domain Services (Windows Server 2012 Active Directory) now allow a single domain to contain nearly 2 billion objects.

With this much capacity, most organizations could deploy only a single domain and ensure that all domain controllers contain all the domain information. However, organizations that have decentralized administrative structures, or that are distributed across multiple locations, might consider implementing multiple domains in the same forest to accommodate the administrative needs of their environment.

The AD DS Domain Is an Administrative Center

The domain contains an Administrator account and a Domain Admins group. By default the Administrator account is a member of the Domain Admins group, and the Domain Admins group is a member of every local Administrators group of domain-joined computers. Also, by default, the Domain Admins group members have full control over every object in the domain. The Administrator account in the forest root domain has additional rights, as detailed in the "What Is an AD DS Forest?" topic.

The AD DS Domain Provides Authentication

Whenever a domain-joined computer starts, or a user signs in to a domain-joined computer, AD DS authenticates them. Authentication verifies that the computer or user has the proper credentials for an AD DS account.

The AD DS Domain Provides Authorization

Windows operating systems use authorization and access control technologies to allow authenticated users to access resources. Typically, the authorization process is performed locally at the resource. Windows Server 2012 introduced domain-based Dynamic Access Control to enable central access rules to control access to resources. Central access rules do not replace the current access control technology, but rather provide an additional level of control.