Solution Security

Decouple CCE Authorizations from Active Directory

Prior to Release 12.0(1), Packaged CCE uses Microsoft Active Directory Security Groups to control user access rights to perform setup and configuration tasks. Microsoft AD also grants permissions for system components to interact; for example, it grants permissions to a Distributor to read the Logger database. Microsoft AD manages the user privileges that are associated with the Security Groups - Setup, Config, and Service. Thus, Microsoft AD handled both authentication and authorization. In such cases, Microsoft AD must assign user privileges to the Security Groups. To accomplish this, Packaged CCE solution administration requires write permissions to Microsoft AD for authorization.

By default, Packaged CCE now decouples authentication and authorization functions.

Decoupling authentication and authorization removes the need to use Microsoft AD to manage authorization in Packaged CCE components. The Packaged CCE solution requires that you add user IDs to the local user groups on each local machine for authorizations. User privileges are provided by memberships to local user groups in the local machines. Microsoft AD is only used for authentication.

To authorize a user ID that is already present in the Microsoft AD, you associate or add the user ID to the local user groups:

- Associate the user ID with the local `UcceService` security group to provide the SQL server authorizations to the user ID for read/write operations in the SQL database. Use the Service Account Manager tool to assign a domain user as a service account user.
- Add the user ID to the local Administrators group for Packaged CCE Setup operations. Add the user ID to the local `UcceConfig` security group for Packaged CCE configuration operations using the Configuration Manager tools.

ADSecurityGroupUpdate Registry Key

This Registry key allows or disallows updates to the Config and Setup security groups in the Domain under an instance Organizational Unit (OU).

The key has two values as follows:

- 0—Indicates that the Administrator gadget only updates the User_Role column in the User Group table in the database schema and *not* the Config and Setup security groups in the domain under instance OU.
- 1—Indicates that the Administrator gadget updates the User_Role column in the User Group table in the database schema *and* the Config and Setup security groups in the domain under instance OU.

The default value is 0.

User Health in Service Account Manager

After upgrade, the Service Account Manager checks the users in the `UcceService` local group. If the users are not in the `UcceService` local group, then the Service Account Manager displays the status as *Unhealthy*. In such a case, run **Fix Group Membership** to make the status healthy. Alternatively, provide the new domain user in the Service Account Manager (SAM) tool or in `Websetup`

For more information about the enhancements, see the following guides:

- The chapter on the Service Account Manager in the Staging Guide for Cisco Unified ICM/Contact Center Enterprise.
- The sections on adding components to Packaged CCE instances, configuring permissions in the local machine, and migrating databases in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide*.

Organizational Units

Application-Created OUs

When you install the solution software, the AD Domain in which the VMs are members must be in Native Mode. The installation adds several OU objects, containers, users, and groups for the solution. You need delegated control over the Organizational Unit in AD to install those objects. You can locate the OU anywhere in the domain hierarchy. The AD Administrator determines how deeply nested the contact center enterprise solution OU hierarchy is created and populated.

Note All created groups are Domain Local Security Groups, and all user accounts are domain accounts. The Service Logon domain account is added to the Local Administrators' group of the application servers.

The contact center enterprise installation integrates with a Domain Manager tool. You can use the tool standalone for preinstalling the OU hierarchies and objects required by the software. You can also use it when the Setup program is invoked to create the same objects in AD. The AD/OU creation can be done on the domain in which the running VM is a member or on a trusted domain.

Active Directory Administrator-Created OUs

An administrator can create certain AD objects. A prime example is the OU container for Unified CCE Servers. This OU container is manually added to contain the VMs that are members of a given domain. You move these VMs to this OU once they are joined to the domain. This segregation controls who can or cannot

administer the servers (delegation of control). Most importantly, the segregation controls the AD Domain Security Policies that the application servers in the OU can or cannot inherit.