**EPM Farm set up Admin and Service Accounts**

You must prepare your service accounts before you begin your installation. The account roles used in a SharePoint Server 2007 environment with Project Server 2007 deployed are numerous. For secure farm environments and organizations that require compliance with Windows security best practices, following the principle of least privilege involves creating separate physical service accounts for each of the logical account roles for potentially all of the following account roles:

**SQL Server Process Account Role:** The system uses the account assigned to this account role to run the various services that are part of Microsoft SQL Server. This includes SQL Server itself, the SQL Server Agent, Analysis Services, and Reporting Services. Depending on your organization’s requirements, you may use multiple accounts to fulfill this role (e.g. DOMAIN\Sql\_Svc for SQL, DOMAIN\SSAS\_Svc for Analysis Ser-vices, and DOMAIN\SSRS\_Svc for Reporting Services). **This account must be a domain account and the physical account allocated to this account role should be unique within the deployment for security purposes.** You can create separate accounts for SQL Server and Analysis Services. The Analysis Services service account will require db\_datareader access to all Project Server reporting databases for which it builds cubes.

**Server Farm Account Role:** The system uses the account assigned to this account role to access the SharePoint Configuration database and as the Application Pool identity for the SharePoint Central Administration site. This is also the account under which the Windows SharePoint Services Timer service runs. This account receives membership in the Logins, db\_Creator, SecurityAdmin, and db\_owner SQL Server security roles during the configuration of the SharePoint farm. Microsoft’s documentation also refers to this account role as the Database Access Account.

**Warning:** You cannot use a local Windows account for the Server Farm account role. You must install SharePoint Server 2007 into a domain environment.

Note: If you want to build a Virtual machine environment for development or demo purposes, you must enable the Active Directory Role on your server.

**Application Pool Process Account Role:** The system uses the account assigned to this account role as the Application Pool identity for a Web application and for accessing the content database associated with that particular Web application. The account must be a domain account, but it does not need to be a member of any particular security group. You should consider providing each Web application you plan to create with its own Application Pool Process Account Role.

**Note:** Application pools are an Internet Information Services feature that enables you to run Web applications in an isolated process from other Web applications. This isolation construct prevents a crash in one application from affecting other applications running on the same server farm.

**Site Collection Owner Account Role:** The account assigned to this account role has administrative rights over the Windows SharePoint Services site collection you create to host a SharePoint site. First, you create a Web application, which is essentially an extended Web site, to host the SharePoint site. Then, you create a new Windows SharePoint Services site collection. You enter this account when you specify a primary site collection owner. This account should be a domain user. In all likelihood, you will want to use either your personal account or the standardized administrator account provided by your organization for this purpose.

**Note:** A site collection is a group of Microsoft Windows SharePoint Services sites that are sub-sites of a single top-level site.

**Project Server Instance Administrator Role:** During the installation, you must specify the initial administrator for the instance of Microsoft Project Server 2007 that you are installing. This account must be a valid do-main user. In all likelihood, you will want to use either your personal account or the standardized administrator account provided by your organization for this purpose.

**SharePoint Search Service Account Role:** The SharePoint Search Services runs as the account assigned to this account role. The account also receives read/write access to the content databases for all Web applications, read access to the SharePoint Configuration database, and read/write access to the SharePoint Search data-base.

**SharePoint Search Content Access Account Role:** The SharePoint Content Access Service uses the account assigned to this account role to access content within the SharePoint farm. The account should be a domain account, and you may use the same account used for the SharePoint Search Service Account Role for this ac-count role. For security purposes, this account should not have permission to modify any content within the farm.

**Excel Services Account Role:** The account under which Excel Services runs.

**Project Server Application Account Role:** The application service account for the Project Server 2007 Service running on SharePoint Server.

**Secure Store Service Account Role:** The account under which the Secure Store Service runs.

**PerformancePoint Services Service Account Role:** The account under which PerformancePoint Services runs

**Secure Store Target Application Role:** The account that the *Target Application* for the Secure Store instance for the Business Intelligence Center uses to access data for the *Report Viewers* group in the Business Intelligence Center.

**State Services Account Role:** The account under which the State Services runs.

Note: For single-front-end-server farm environments, It is recommended that you create a single Active Directory account to use for all account roles except the SQL Server Process Accounts and the Target Application for the Secure Store Service.