Modifying Administrative Account Properties

SharePoint Portal Server 2003 Administrator Password Change Procedure

Introduction

Microsoft SharePoint Portal Server 2003 depends upon a number of services, application pools, external resources and code elements for successful operation. Most of these resources require a security context, in the form of an local/domain administrative account, in order to operate. Because there are so many elements which depend upon this type of security, modifying any of the accounts assigned during portal creation can cause one or more elements to cease operation, which could in turn lead to portal failure.

SharePoint Portal Server (hereinafter referred to as SPS) administrative accounts fall into two categories: 1) accounts required for services to run on the local machine, and 2) user accounts for different types of functionality, including server processes, user-developed code and shared elements. This document outlines the scope of such changes and provides detailed procedures for modifying administrative account information.

Service Accounts

SPS requires a specific set of services that must run on each Front-End Web Server (FEWS) and Job/Index server. Each service runs in either a local context, such as NT AUTHORITY\NetworkService, or a domain context, such as DOMAIN\SPSAdmin (Microsoft recommends that these services run in a domain context – see the SharePoint Portal Server Administrator's Guide for additional information).

The required services are as follows:

- Microsoft SharePointPS Search (SharePointPSSearch): Provides indexing and searching over the portal and external content.
- Microsoft SharePoint Administration (SPSAdmin): Enables the server to administer SharePoint Portal Server services.
- SharePoint Portal Alert (spsalert): Schedules and sends alerts and alert results to users on one or more servers running SharePoint Portal Server.
- SharePoint Timer Service (SPTimer): Sends notifications and performs scheduled tasks for Microsoft Windows SharePoint Services.

There may also be services installed by third-party utilities which run in a domain context using an SPS administrative account. All services should be reviewed to determine which context and account are being used.

User Accounts

SPS may utilize any number of user accounts to perform various functions such as searching and indexing, server administration, access to databases, and the like. For ease of administration, it is common (but not required) to use a single account for all functions; however, the account information is stored in a multitude of locations, each of which must be updated in the event that any account information, such as the password, is changed in Active Directory or via local machine administration.

Search and Indexing

The search function of SPS relies on two distinct account setting: the configuration database account and the default content access account. As it's name implies, the configuration database account connects to the SQL database to retrieve configuration settings (see Section 1.2.6.3, below); the content access account is used as the identity for the content crawling process when retrieving both internal and external content.

A content access account is associated with each content index. For internal content, such as portals and site directories, specific access accounts may be used, depending upon the content being crawled, through exclude and include rules. For intranet and portal content, this account should be a member of the SharePoint administrator groups, so it can access and crawl all content sources and their properties. The account uses Windows Integrated Authentication (NTLM) for accessing content by default. If this method of authentication fails, it uses Basic Authentication unless it has been explicitly disabled.

If no account is specified as the default content access account, the portal administrator account will be used. In some cases, such as external content and line-of-business applications, a specific account setting may be required. In such instances, the account is specified in the inclusion/exclusion rules for the index. If such indexes exist, they must be checked for account settings, along with the default content access account defined in SharePoint Central Administration.

Application Pools

An application pool is an IIS configuration option that links one or more applications to a set of one or more worker processes. During installation of SPS, two application pools are created:

- CentralAdminAppPool: Used by the SharePoint Portal Administration Web application and defined when you install the domain\svc-sharepoint user account.
- MSSharePointPortalAppPool: Can be used and shared for portal sites that are created.

In most cases, application pools use a built-in account, such as NETWORK SERVICE or LOCAL SYSTEM; however, it is common practice to run SharePoint application pools using the administrative account. If a domain account is used, the application pool identify must be modified in accordance with any account changes; failure to do so will result in the portal being inaccessible.

Server Administration

Any user that is a member of either the domain administrators or local administrators on the FEWS may administer the portal and access SharePoint Central Administration. It is not necessary to use the administrative account defined during installation and portal creation to access these settings; however, if the account is local to the FEWS and not a domain account, any password changes must be duplicated on each individual FEWS, job server, and index server in the farm.

Code

Any code which connects to web services, the SharePoint database, or other secured SPS resources must include security account information. If the code references an administrative account, and if this information is hard-coded, then the binaries must be changed, recompiled, and redeployed. If the code references an external configuration file (such as machine.config) then the settings within the reference file must be altered accordingly. All code should be reviewed for any references to account information and, where possible, this information should be moved to a configuration file to reduce maintenance requirements.

Tools

Most SharePoint-specific tools require administrative access to SPS. In many cases, the default administrative account is used to provide the necessary access, especially if the tool must connect to the database (as is the case with the STSADM GUI tool used on both FEWS's). Tool configurations should be checked to determine which account, if any, is being used to access SPS.

Some common tools include:

- STSADM GUI Utility
- SPSBackup Utility
- Virus Protection Software

Databases

SPS relies upon several data sources, including a back-end SQL 2000 database, a profile database for user account information, and a configuration database for portal operation, each of which may require credentials to be supplied in one or more administration areas. In some instances, such as using an external SQL database, account information may need to be modified in one or more places on each server in the farm.

SQL Database

By default access to all the core SharePoint databases – [Portal_Name]_PROF, [Portal_Name]_SERV, [Portal_Name]_SITE, and [Portal_Name]_Config_db – is assigned to the administrative account specified during portal creation. If the SQL database is configured for

Windows Authentication, no change is necessary to the database configuration; however, if the database is configured for SQL Authentication, the password must be changed by a database administrator or the portal will cease to function.

Profile Database

User profile information is stored within the Profile Database. In order to import profile data from Active Directory, SPS must use an access account with sufficient permissions to query the AD data store. This account is often the portal administrative account and is set in the profile configuration page for the profile database. An invalid password for this account will not prevent the portal from functioning but it will cause the import process to fail.

Configuration Database

The configuration database administration account is the user name and password that SPS uses when connecting to the configuration database or when propagating full-text indexes from index management servers to search servers. Typically, this account is the same as the portal administrator account. If the portal cannot read from/write to the configuration database, it will stop functioning; if index propagation fails, search results will be out-of-date and the search function may fail. Changes to this account must be made in SharePoint Central Administration.

Procedure

Perform the following steps in order to successfully implement administrative password changes.

Disable Services and Application Pools

Before making any changes to the administrative account, stop all SharePoint-related services and application pools.

1. Go to **Start > Administrative Tools > Services**
2. Locate the following services, the right-click on each one and select **Stop**.
    a. **Microsoft SharePointPS Search**
    b. **SharePoint Portal Administration**
    c. **SharePoint Portal Alert**
    d. **SharePoint Timer Service**
3. Repeat for any other services which show the administrative account in the **Log On As** column.
4. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**
5. Expand the **Application Pools** node under the server node.
6. Locate **CentralAdminAppPool** and **MSSharePointPortalAppPool**.

7. Right-click on each and select **Stop**.

Modify Account Information

After stopping the ShrarePoint services and application pools, change the password for the administrative account. Next, change the password for each SharePoint-related service. Finally, change the password for each application pool.

Changing Service Passwords

1. Go to **Start > Administrative Tools > Services**
2. Right-click on the service and choose **Properties**.
3. Click the **Log On** tab at the top.
4. Enter the new password in the appropriate fields.
5. Click **OK**.

Changing Application Pool Passwords

1. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**
2. Expand the **Application Pools** node under the server node.
3. Right-click on the application pool and select **Properties**.
4. Enter the new password in the appropriate field under the **Identity** tab, then confirm the new password in the pop-up dialog
5. Click **OK**.

Enable Services and Application Pools

After changing all account information, restart the SharePoint services and application pools.

NOTE: Before doing so, insure that SQL Server is configured to use Windows Authentication for the administrative account; otherwise, the SQL account password will need to be changed prior to staring any services or application pools.

Starting Services

1. Go to **Start > Administrative Tools > Services**
2. Right-click on the service and choose **Start**.

Starting Application Pools

1. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**
2. Expand the **Application Pools** node under the server node.
3. Right-click on the application pool and select **Properties**.

4. Enter the new password in the appropriate field under the **Identity** tab, then confirm the new password in the pop-up dialog
5. Click **OK**.

Change Central Administration Settings

After restarting the services and application pools, enter SharePoint Central Administration and change the account settings.

1. On a Front End Web Server, go to **Start > All Programs > SharePoint Portal Server > SharePoint Central Administration**.
2. Click **Configure Server Farm Account Settings**.
3. In the **Configuration Database Administration Account** section, select Specify Account. Enter the new password in the appropriate fields.
4. Click **OK**.
5. Repeat Steps 2 – 4 for the **Default Content Access Account** and **Portal Site Application Pool Identity** sections.

Miscellaneous Settings

Once the portal is functional using the new administrative account settings, proceed with changes to any other settings, such as code, configuration files, third-party tools, search and indexing credentials, the profile database, etc.