SUPPORT NOTE

SN-138

RDS Intranet Website Will Not Start

Introduction

After customer specific network security policies are applied to either an RDS Intranet Lab Edition workstation or Enterprise server, sometimes the RDS Intranet website/application fails to start on the computer. One symptom that the application isn't running is that whenever the application is launched from the browser, it reports that the site is down.

Several security settings can cause the website not to start or have problems after it starts, including:

- Passwords are more secure, requiring local user passwords to be changed so that it matches the corporate policy.
- Services used by the website are no longer available to IIS (Internet Information Services), the Windows service that hosts the website.

COM+ Service Crashes

Passwords are the most common reason that the application won't start. Another reason is because a service fails to launch or crashes when attempting to launch. To find out why, the Windows Administration Services tool can be used to find out which services set to Automatic are not starting.

The Administration Event Viewer can also be used to identify other errors that might be happening when the website starts.

During one RDS Intranet installation, the Network Connections Service would not start after the security policies were applied. In addition, the error message "Win32: Access denied" occurred when trying to view dependent services.

In that case, the event viewer logged that the COM+ Service was crashing each time WWW Service (IIS as seen in Services) was restarted. That service also restarts the website application.

Modifying Security Policies

The COM+ and Network Connections Service errors were tracked down to the "Impersonate a client after authentication" policy setting. This error is described in Microsoft article 933994 that covers Windows 2003 and XP, even though the article only refers to Win2003.

Step 2 in the Microsoft article has the following details that were used to resolve this issue:

View the "Impersonate a client after authentication policy settings." In this policy, the following accounts must appear on the Local Security Setting tab:

- SERVICE
- IIS_ComputerName
- NETWORK
- Administrators

To view this policy, follow these steps:

1) Click Start, click Run, type gpedit.msc, and then click OK.
2) In the Group Policy Object Editor window, expand Computer Configuration, expand Windows Settings, and then expand Security Settings.
3) Expand Local Policies, and then click User Rights Assignment.
4) In the details pane, double-click Impersonate a client after authentication.
5) Determine whether the appropriate accounts are listed on the Local Security Setting tab.