Install Required Microsoft Patches for Reliable WMI Connections

Contents

Introduction

This document describes how to install the required Microsoft patches for reliable WMI connections.

Background Information

Cisco Umbrella Active Directory Integration relies on WMI to establish connections between a machine running the AD Connector and a remote domain controller (DC). The WMI connection, along with DCOM permissions, are what allow the Connector service to retrieve login events from remote DCs. If the WMI connection hangs, leaks, or otherwise becomes disconnected, then this can result in user and computer login events not being retrieved from the remote DCs.

Environment

Windows Server 2008, Windows Server 2008 R2

Problem

- Incorrect policy application and reporting for some users.
- AD Connector logs show this log line repeated over and over: **HandleState timer still blocked, skipping this execution…**

Solution

Install these patches to your DCs:

1. This patch fixes a memory leak in Microsoft's WMI, which prevents the Connector from establishing a successful connection with the domain controller: http://support.microsoft.com/kb/958124
2. These hotfixes are associated with the operation and functionality of the WMI service and its related components: http://support.microsoft.com/kb/2591403

These patches are required for Windows Server 2008 R2 (unless SP1 is installed):

1. This patch fixes a memory leak in Microsoft's WMI, which sporadically prevents the Active Directory domain controller from writing the necessary user login events to the Security Log of the domain controller. As a result the Connector can not get all user login events from this domain

controller: http://support.microsoft.com/kb/981314
2. This patch fixes unexpectedly slow startup or logon process in Windows Server 2008 R2: http://support.microsoft.com/kb/2617858

After these patches have been installed, reboot each of the DCs to which patches were installed and then restart the Connector service.