Dell’s Implementation of Microsoft Advanced Group Policy Management

Dell implemented AGPM in June of 2011 and is taking advantage of the benefits it offers for managing Group Policy.

By Pat Pitre
Sr. Systems Engineer at Dell Inc.
November, 2011

Abstract

Dell implemented Microsoft Advanced Group Policy Management to take advantage of features like change control, and offline editing, when managing group policy objects. This paper focuses on both the benefits of AGMP and some of the unique challenges encountered during integration testing, and how they were resolved. This information may help other large organizations who are considering or are in the process of implementing AGPM.

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Contents

Introduction

Dell uses Group Policy technology extensively in its large enterprise environment and wanted to improve control and reduce risk of related widespread outages. Microsoft Advanced Group Policy Management (AGPM) helps reduce risk by allowing Group Policy Objects (GPOs) to be edited offline, outside of the production environment. AGPM provides better overall control for Group Policy by providing Change Control, Roles based Workflow, as well as other advanced features that make GPO management for efficient.

This paper provides an overview of AGPM and its capabilities, as well as a look at Dell's implementation and the challenges faced during testing and deployment.

For details on how to install and configure AGPM in your environment, related references to Microsoft documentation can be found at the end of this document.

AGPM Feature Overview

Offline Editing

The AGPM server archive provides offline storage for GPOs. Changes you make to GPOs in the archive do not affect production until you deploy them. You can edit GPOs and test them in a safe area. After reviewing the changes you can deploy them, knowing that instant rollback is possible. With Dell's large system base, offline editing reduces the risk associated with production group policy changes.

Change Control

- A Check in/Check out feature prevents simultaneous editing of a GPO
- History of individual actions on a GPO can be used for audit and rollbacks
- Detailed settings report are available for each entry in history
- Instant rollback is available by deploying a specific instance in a GPO's history
- Differences feature lets you compare any two GPO entries in history to determine differences

Role Based Delegation

The following roles allow you to assign specific privileges to GPO administrators and can be used to limit the actual deployment to more senior administrators:

Reviewer - Can view and compare GPOs. They cannot edit or deploy GPOs.

Editor - Can check out GPOs from the archive, edit GPOs, and check in GPOs to the archive. Editors can request deployment of a GPO. Editors can also view and compare GPOs

Approver - Approvers can approve the creation and deployment of GPOs. (When Approvers create or deploy a GPO, approval is automatic.) Approvers can also view and compare GPOs

Workflow
AGPM supports creation of GPO template libraries that allow more efficient GPO creation. A repeatable workflow can be obtained using a series of tasks like Controlling, Check-out, Edit, Check-in, Requests, Reporting, and Deployment along with Roles and automatic e-mail notification.

Search and Filter – AGPM 4.0 allows you to search the list of GPOs for specific attributes and filter the list of GPOs displayed.

Export and Import - You can copy a controlled GPO from a domain in one forest to a domain in a second forest using the export/import feature. This feature was not previously available with GPMC.

Overview of Dell’s Implementation

AGPM Server Architecture

An AGPM server runs the AGPM Service and is used to manage an archive. Each AGPM Server can manage only one archive, but a single archive can contain data for multiple domains in a forest.

Dell chose to implement a single server to manage its main production domain and 4 sub-domains. Although an archive can be hosted on a computer other than an AGPM Server, Dell obviously wanted to install and maintain AGPM on a dedicated server in a managed data center. AGPM is also used to manage group policy in Dell’s Proof of Concept Lab forest.

Server Configuration

Dell’s AGPM servers are Virtual Machines running Windows Server 2008 R2, with dual processors and 2GBs of RAM. This server configuration performs well with all of the domains in the dell.com forest (Americas, EMEA, Japan, and APAC), that are contained in the production archive.

AGPM Prerequisites

This section covers groups and account creation that was done to prepare for the AGPM server installation and roles based delegation.

1) Service Account to run the AGPM Server Tool (named ***Service AGPM)***. This account must be a member of the Domain Admins group, or for a least-privilege configuration

(used by Dell), it should be a member of the following groups in each domain that is managed by the AGPM Server:

- Group Policy Creator Owners (Or explicit access to sysvol in each domain)
- Backup Operators (in each domain)

2) Additionally, this account requires Full Control permission for the following folders:
   - The AGPM archive folder, for which this permission is automatically granted during the installation of AGPM Server if it is installed on a local drive.
   - The local system temp folder, typically %windir%\temp.
3) Create a Universal Group named ***AGPM Administrators***. This will be used as the Archive Owner during the AGPM Server install.
4) Create the following Universal Groups. Each one represents a role within the archive:
   1. AGPM Approvers
   2. AGPM Editors
   3. AGPM Reviewers

Additional Permissions Requirements (Post AGPM install):

1. Grant Full Control on the Group Policy Objects container in GPMC, to the "Service AGPM" account.
2. Service account needs full control delegation to all production GPOs. There is a sample script included with AGPM that allows you to automate this task: http://msdn.microsoft.com/en-us/library/windows/desktop/aa814151(v=vs.85).aspx#_win32_grant_permissions_for_all_gpos_in_a_domain
3. Make the "Service AGPM" account a local admin on AGPM server.

Issues and Challenges

This section lists the main issues and challenges that Dell worked through during implementation.

AGPM's DC Locator Process in the Dell Environment

Dell restricts sysvol share permissions on its domain controllers beyond the default permissions for security purposes. Full Control is enabled for Authenticated Users only on PDCs but removed on all other DCs. This permissions configuration caused random access denied type errors and poor performance when initially testing AGPM with various functions within the tool.

AGPM uses a costing method to locate and write changes to the domain controller that is closest to the AGPM server. It does not automatically write changes to the DC or PDC specified in your Group Policy Management Console, like with GPMC.

To resolve this issue the AGPM server was moved into the same site where its PDCs from each domain reside. This configuration allows AGPM to locate and use the PDCs in the site that it resides in and that its service account has Full Control to. This configuration change resolved all of the random access denied issues we were seeing in AGPM.

Enforcing use of AGPM

Once AGPM is implemented, it's important to get all of your domain admins using it and to prevent GPO changes from being made directly in production. Making changes directly in production defeats the purpose of AGPM and has the potential for changes to be overwritten.

Prior to Dell's AGPM implementation, GPO Administrators were granted privileges to update GPOs through the Group Policy Creator Owners group in each domain. To enforce the use of AGPM, Dell moved all members of the Group Policy Creator Owners group to dedicated domain local groups that are privileged in the AGPM. Domain Admins still have the ability to elevate their privileges and make GPO changes directly in production, but this will only be used in the event that the AGPM Server is down when an urgent GPO change is needed.

Problems connecting to the AGPM Archive

- Ensure that AGPM client contains the correct server name (FQDN, or IP as needed) and port.
- Ensure that the AGPM Service is running on the server. If the issue persists, ensure that the password for the service has not changed.
- You can also install GPMC directly on the AGPM server to ensure that the archive is functional.

References

AGPM Planning Guide – Microsoft Corporation

Technical Overview of AGPM - Microsoft TechNet

AGPM Step-By-Step – Microsoft TechNet