

Microsoft | Open Door

**MDOP : Advanced Group
Policy Management**

**Vijay Kolli
MEA Architect
Microsoft Corp**

AGPM : The Sell

- GPO Management
 - Offline editing
 - History
 - Difference reporting
 - Search
 - Multi forest
- Workflow
 - Delegation
 - Source control

Architecture

Archive/Offline

Production

AGPM Server

Domain Controller

Server
Component

XML File of backups

GPO 2

Backups
GPO 1

Backups
of GPO 2

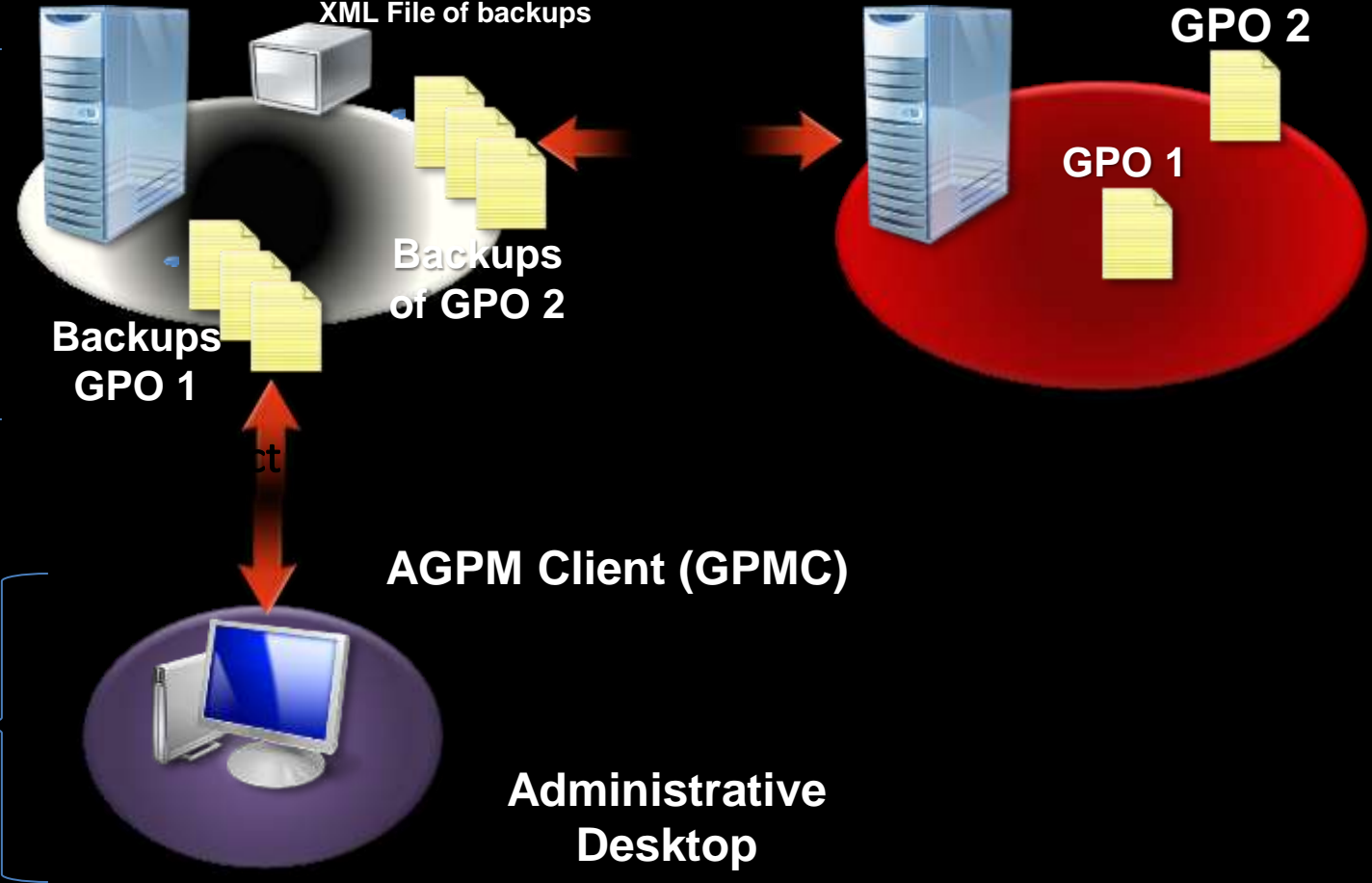
GPO 1

ct

AGPM Client (GPMC)

Admin
Component

**Administrative
Desktop**



AGPM 4.0 Client and Server Support

Operating system on which AGPM Server 4.0 runs	Operating system on which AGPM Client 4.0 runs	Status of AGPM 4.0 support
Windows Server 2008 R2	Windows 7/R2	Supported Best Experience
	Windows Vista with SP1/2008	Partially supported Cannot edit policy settings or preference items that exist only in Windows Server 2008 R2 or Windows 7
Windows Server 2008	Windows 7/R2	Unsupported
	Windows Vista with SP1/2008	Supported with limitations Cannot report or edit policy settings or preference items that exist only in Windows Server 2008 R2 or Windows 7

AGPM : The Sell

- GPO Management
 - Offline editing
 - History
 - Difference reporting
 - Search
 - Multi forest
- Workflow
 - Delegation
 - Source control

Offline Editing



Edit GPOs offline before deploying live

Microsoft

MISS SCARLET



CANDLESTICK



BILLIARD ROOM



History

History is a list of complete backups

Rollback to a safe state

Safeguard live environment from
unapproved changes and untested settings

Authoring, History Demo

Differences

The screenshot shows a 'Difference Report' in a Windows Internet Explorer browser window. The report is organized into sections, each with a status icon in the top-left corner and a 'hide' link in the top-right corner.

- Added (Green):** A new TCP/IP printer configuration is shown. The status icon is a plus sign in a square. The section includes:
 - TCP/IP Printer (name: 10.0.0.1)
 - 10.0.0.1 (order: 2)
 - General properties: IP Address (10.0.0.1), Local Name (HPLaserJet2500), Shared printer path (\\Server2\Printer2), Set as default printer (True), Only if a local printer is not present (False).
 - Port Settings
 - Common
- Changed (Blue):** An existing shared printer configuration is shown with a status icon of a square with diagonal lines. The section includes:
 - Shared Printer (name: \\server\share)
 - share5 (order: 1)
 - Name: share, share5
 - General options: Stop processing items on this extension if an error occurs on this item (No), Run in logged-on user's security context (user policy option) (No), Remove this item when it is no longer applied (No), Apply once and do not reapply (No).
- Removed (Red):** A previously configured shared printer is shown with a status icon of a square with a minus sign. The section includes:
 - Shared Printer (name: \\Server2\share5)
 - share5 (order: 2)
 - General properties: Share Path (\\Server2\share5), Set as default printer (False), Local Port.

added

changed

removed

Compare settings between GPOs

Reporting

- Settings
 - Parity with Group Policy settings reports
- Difference
 - Versions: older compared to newer
 - Any 2 GPOs
 - Template: GPO compared to its baseline



Security
Template

VS



Security
Kiosk

Search (Filtering)

- What it does
 - Filters GPOs by properties
 - Allows for column precision
 - Maintains a list of the recent 10 searches
- What it doesn't do
 - Search for settings



Multi Forest Support

- What it does
 - Allows GPO movement from AGPM to AGPM
 - Preserves origin metadata
 - Supports migration tables
- What it doesn't do
 - Online moves between domains/forests
 - GPP and Migrations

Windows 7/Server 2008 R2

- What was supported
 - Group Policy Preferences
 - Reporting for all new extensions
 - Applocker, DNSSEC, IE8, Scheduled Tasks
 - Service execution
 - RSAT

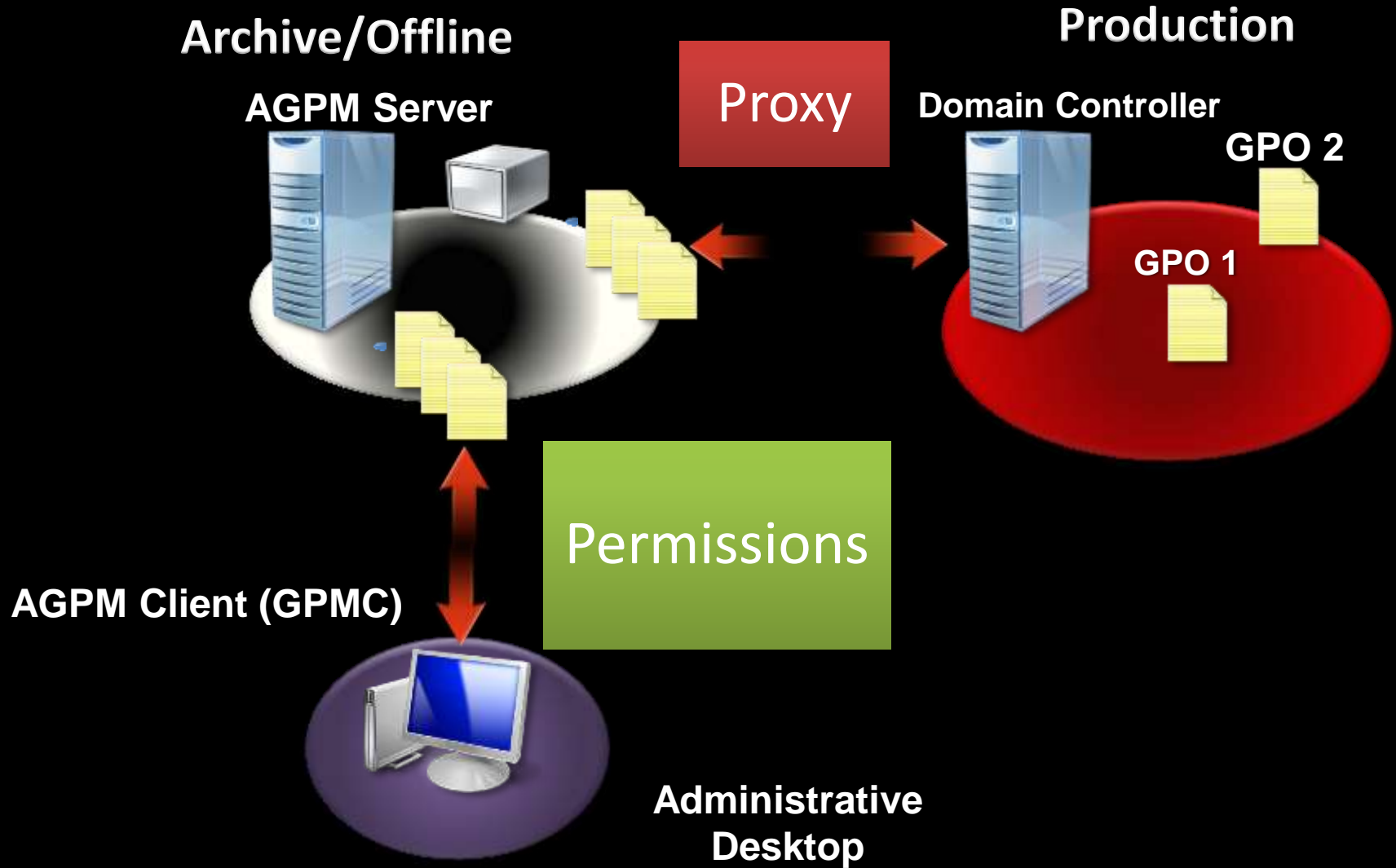


Differences Demo

AGPM : The Sell

- GPO Management
 - Offline editing
 - Difference reporting
 - History
 - Search
 - Multi forest
- *Workflow*
 - Delegation
 - Source control

Service



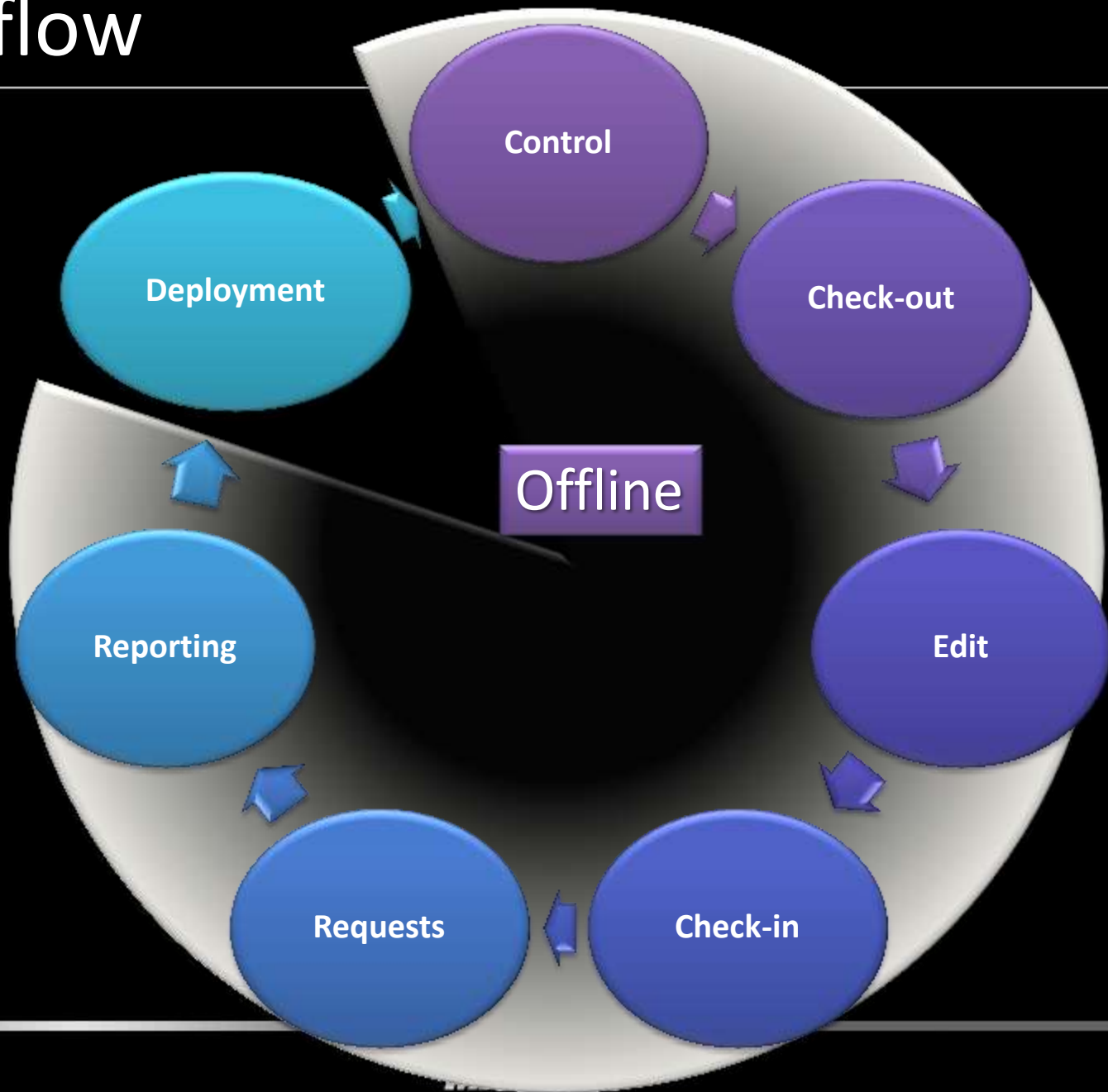
Delegation - Roles



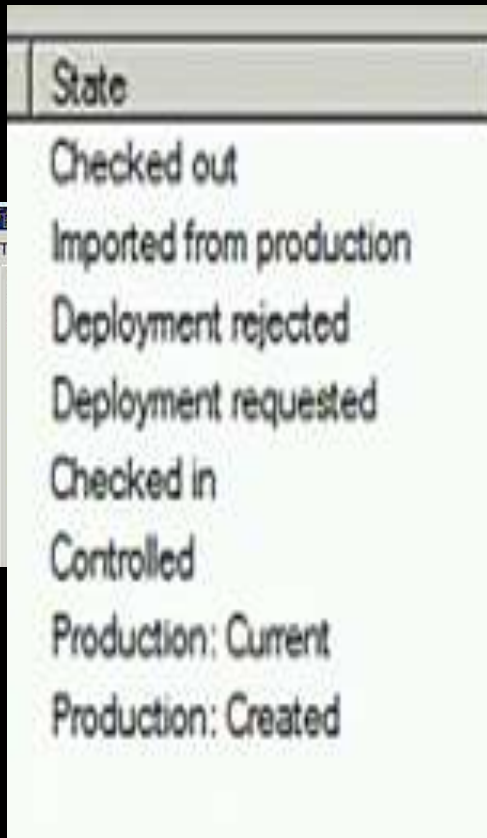
Define granular control without making everyone a Domain Admin

Role Delegation Demo

Workflow



Granular change tracking



Changed By	Comment	Deletable	Computer ...	User ...	GPO Status
Domain Admins (GPP...	e	Not applicable	0	2	Enabled
Editor Royce (EditorRo...	doobedoo	Yes	0	0	Enabled
Administrator (GPPM\A...	add another pref item	Yes	2	0	Enabled
Editor Royce (EditorRo...	everyone should have this ...	Yes	2	0	Enabled
Editor Royce (EditorRo...	look at that preference	Yes	2	0	Enabled
Administrator (GPPM\A...	bring it in	Yes	0	0	Enabled
AGPM Service (AGPM...		Not applicable	0	0	Enabled
-		Not applicable	-	-	-

Purge historical data

Contents | Domain Delegation | **AGPM Server** | Production Delegation

Specify the AGPM Server that manages the archive for this domain

Host: Port:

Delete old GPO versions

Delete old versions of each GPO from the archive. Retain only the current version and the preceding

Contents | Domain Delegation | **AGPM Server** | Production Delegation

Microsoft

Last Step Delegation

Contents | Domain Delegation | AGPM Server | Production Delegation

These groups and users have these permissions for controlled GPOs in the production environment:

Name	Allowed Permissions
AGPM Users (GPPM\AGPM Users)	Read
Domain Admins (GPPM\Domain Admins)	Edit settings, delete, modify security
Editor (editor@gppm.contoso.com)	Edit settings
ENTERPRISE DOMAIN CONTROLLERS	Read
SYSTEM	Edit settings, delete, modify security

Add... Remove Properties

Contents | Domain Delegation | AGPM Server | Production Delegation

Workflow Demo

Q & A

Partners to go to:



Microsoft®