Best Practices for Designing and Consolidating Group Policy

August 2012

Darren Mar-Elia

CTO & Founder, SDM Software, Inc. (www.sdmsoftware.com)

About the Speaker

- First started using GP in 1998
- Group Policy MVP for the last 8 years
- Contributing Editor to Windows IT Pro Magazine since 1997
- Maintain popular GP resource site www.gpoguy.com
- CTO & Founder: SDM Software www.sdmsoftware.com

Agenda

- What are the criteria for good GP design?
- GP Design Decisions Explored
- Balancing AD and GP design requirements
- Understanding GP processing
- Tips to Maximize GP Performance
- Tools to help you measure & optimize your GP design
- GPO Consolidation – The “Whys” and “Hows”

Definition of Good Group Policy Design

- Characteristics:
  - Minimal impact to end user
  - Security/lockdown goals of organization are met
  - Management overhead and complexity minimized
- These can often work against each other
- Certain GP behaviors can impact this as well
- For me, the best design is like “Goldilocks”
  - Not too many GPOs, but just enough
  - Not too much complexity, but just enough

sdmsoftware

GP DESIGN DECISIONS EXPLORED

sdmsoftware

GPO Design Approaches

- Monolithic GPOs
  - Contains settings from a variety of GP areas (e.g. software installation, folder redirection, etc.) in a single GPO
- Functional GPOs
  - Contains one or more settings from a single GP area and typically targeted at a single function (e.g. domain password policy)

Which to Choose?

- Most environments have a combination of both monolithic and functional GPOs
  - Driven by factors such as delegation needs, complexity requirements and security mandates
- Each type makes sense in certain situations, but from a performance perspective, one may be better than the other... (more later)

sdmsoftware

Functional GPOs

- Functional GPOs are used to isolate a single setting or group of settings
  - Account Policy can/should be stored in a single GPO (e.g., Default Domain Policy) that does nothing else
- You can go overboard here though—100 GPOs, each with a single setting, is *probably* not a good idea…

Monolithic GPOs

- Ideal for delegating to OU administrator
- Keeps all settings in a single, manageable and delegated GPO
- Eases troubleshooting by having to look in one place to find and fix problems

GP Design Considerations

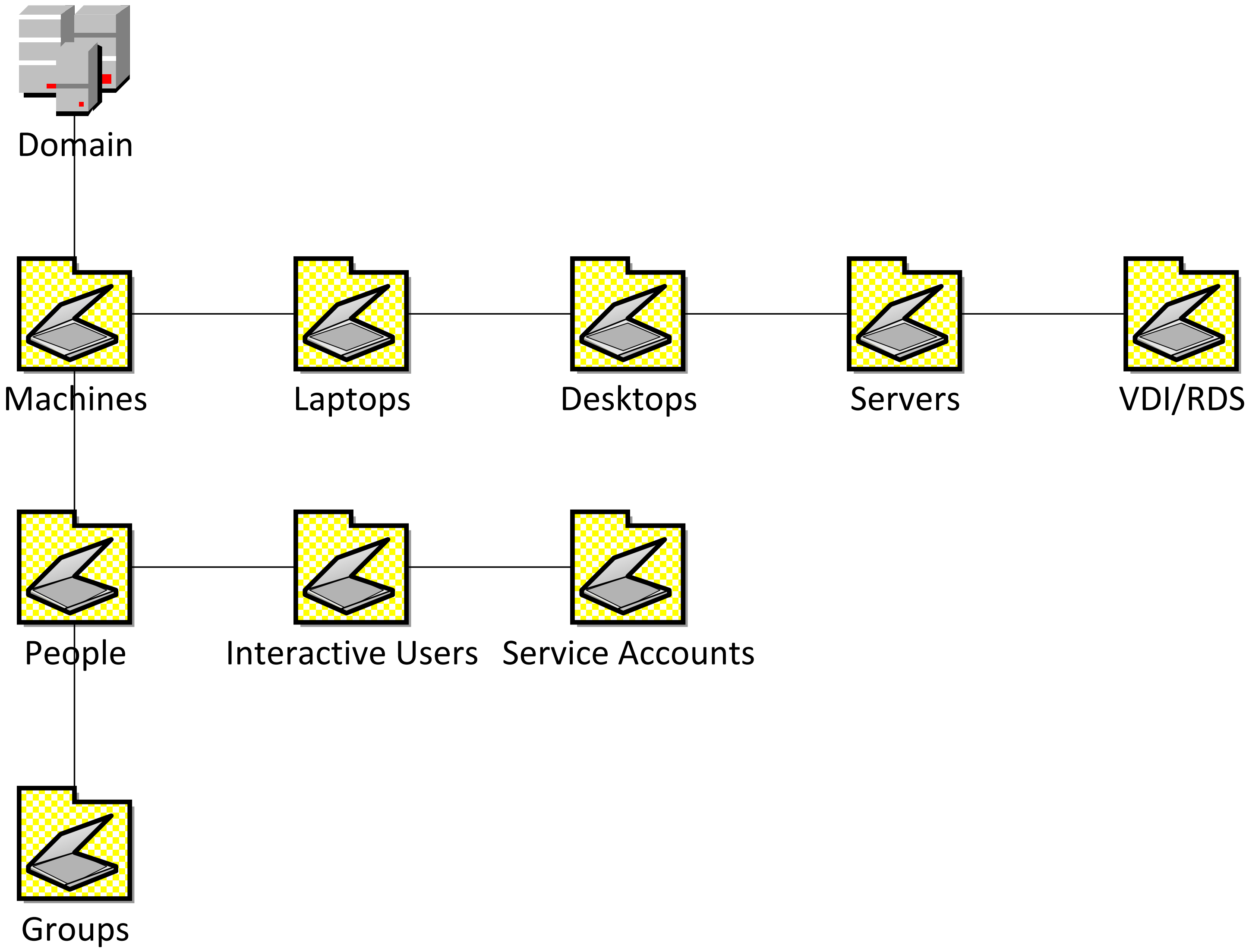
- GPO Linking vs. Filtering
  - Another design point with potential performance impacts
  - Decision Point:
    - Link a GPO close to its intended target (and potentially link it to multiple OUs if needed) or…
    - Link it “higher” and filter using WMI and/or Security Group Filters
- Group Policy Preferences has bigger implications, as each setting in a GPO can have its own filter!

BALANCING AD AND GP DESIGN REQUIREMENTS

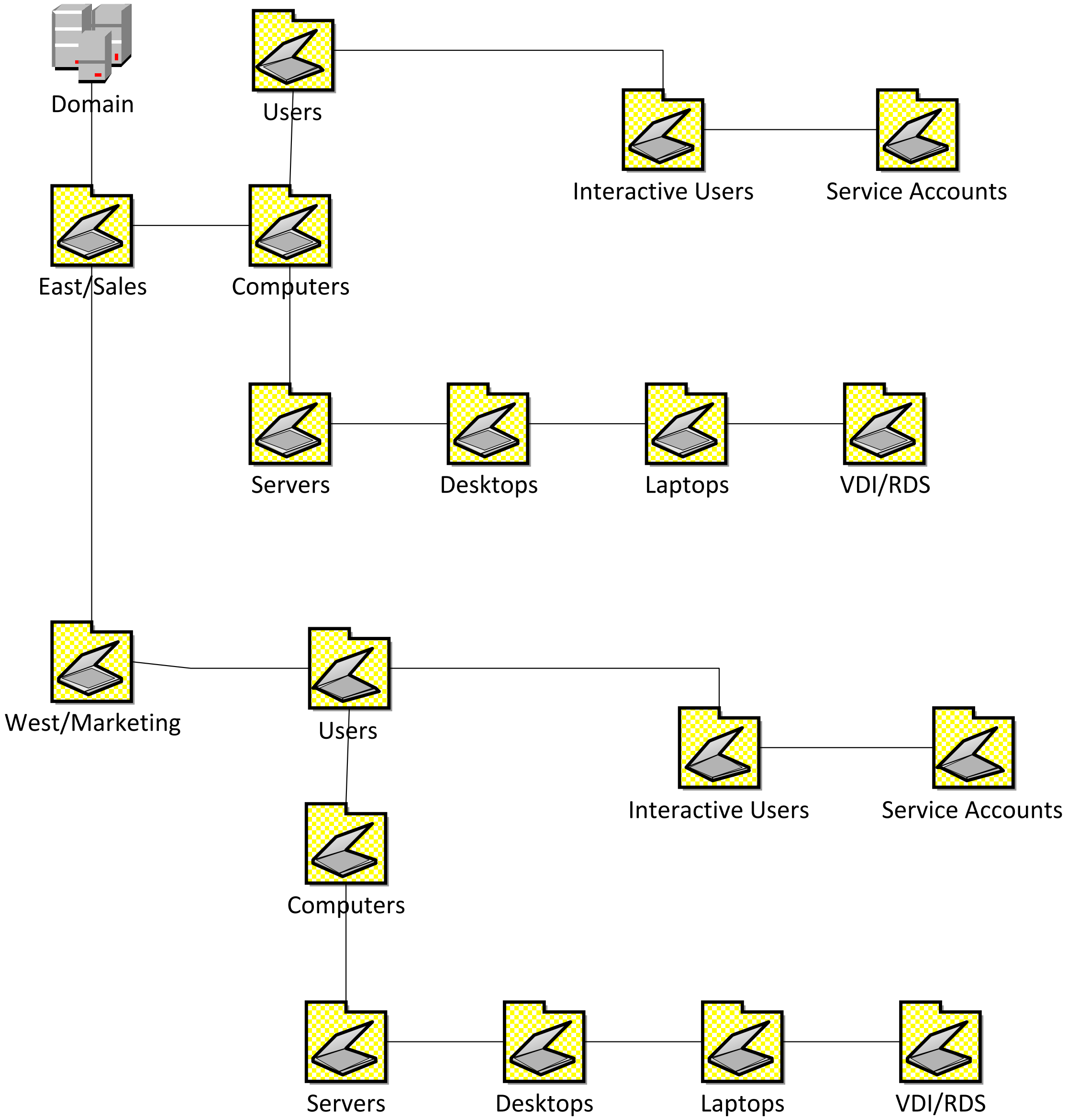
The Challenges of Balancing Conflicting Needs

- The challenge: AD design—particularly OU design, is driven by different goals than GP design
  - AD: Driven by security, delegation, application and administration needs
  - GP: Ease of targeting, differentiation by platform (e.g. server vs. workstation) and sometimes by delegation

AD Designs That Complement GP- “Type-Based”



AD Designs That Complement GP- “Biz/GEO-Based”



AD/GP Design Goals

- Keep in mind the rules about linking and filtering– 80/20 rule applies:
  - Find an OU model that let’s you link as close to the target for 80% of your scenarios
  - The other 20% will require compromises, not AD re-designs
- Avoid designs where you’re forced to link and enforce at the domain level
  - Reduces your options downstream
- Avoid overly flat OU structures (e.g. all users in one OU) if you plan to use per-user policy in any significant way.
- Avoid designs that **require** loopback for all computers

UNDERSTANDING GP PROCESSING

Group Policy Processing – Background & Foreground

- Two kinds of GP processing
  - Foreground (e.g. during machine startup or logon)
  - Background (e.g. periodically based on computer role — DCs every 5 min., workstations and member servers every 90 min. with randomizer)
    - Vista/Win7 introduced the “NLA Refresh”

Group Policy Processing—Synchronous vs. Asynchronous

- Foreground processing can run asynchronously or synchronously
  - XP/ Vista/Win7/Win8 is asynchronous by default, aka “Fast Logon Optimization”
  - You can change this:
    - Computer Configuration\Policies\Admin Templates\System\Logon\Always wait for network at computer startup and user logon set to Enabled to make all foreground processing synchronous
  - Server SKUs always run synchronously

Group Policy Processing – The Impact of Change

- Keep in mind that normally, policy processing only occurs on the client if there is a change to “something”
- What determines if “something has changed?”
  - The list of GPOs that apply to user or computer has changed
  - Security group membership of user or computer has changed
  - WMI Filter link has changed
  - Version number of GPO(s) are different than that stored in the registry
- Note that GP Preferences Item-Level Targeting does not impact this determination

Security Policy is Different

- The Security CSE will process in the background every 16 hours by default, even if nothing has changed
- This ensures that users who try to undo their security settings will be thwarted automatically
- But keep in mind that this is going on—could have performance impacts if you're doing "expensive" things in your security policies
- The interval can be changed
  - – http://support.microsoft.com/kb/277543

Client Side Extension (CSE) Impacts on Performance

- Certain CSEs are more “expensive” than others when it comes to performance impact
- The Security CSE and particularly file and registry security can be expensive when it runs
  - Permission changes to large file trees or many registry keys can impact system performance
  - Runs every 16 hours even if no changes occur
- The Scripts CSE (or more specifically, script execution) can cause problems
  - Hung or long-running scripts don’t timeout for 10 minutes, by default

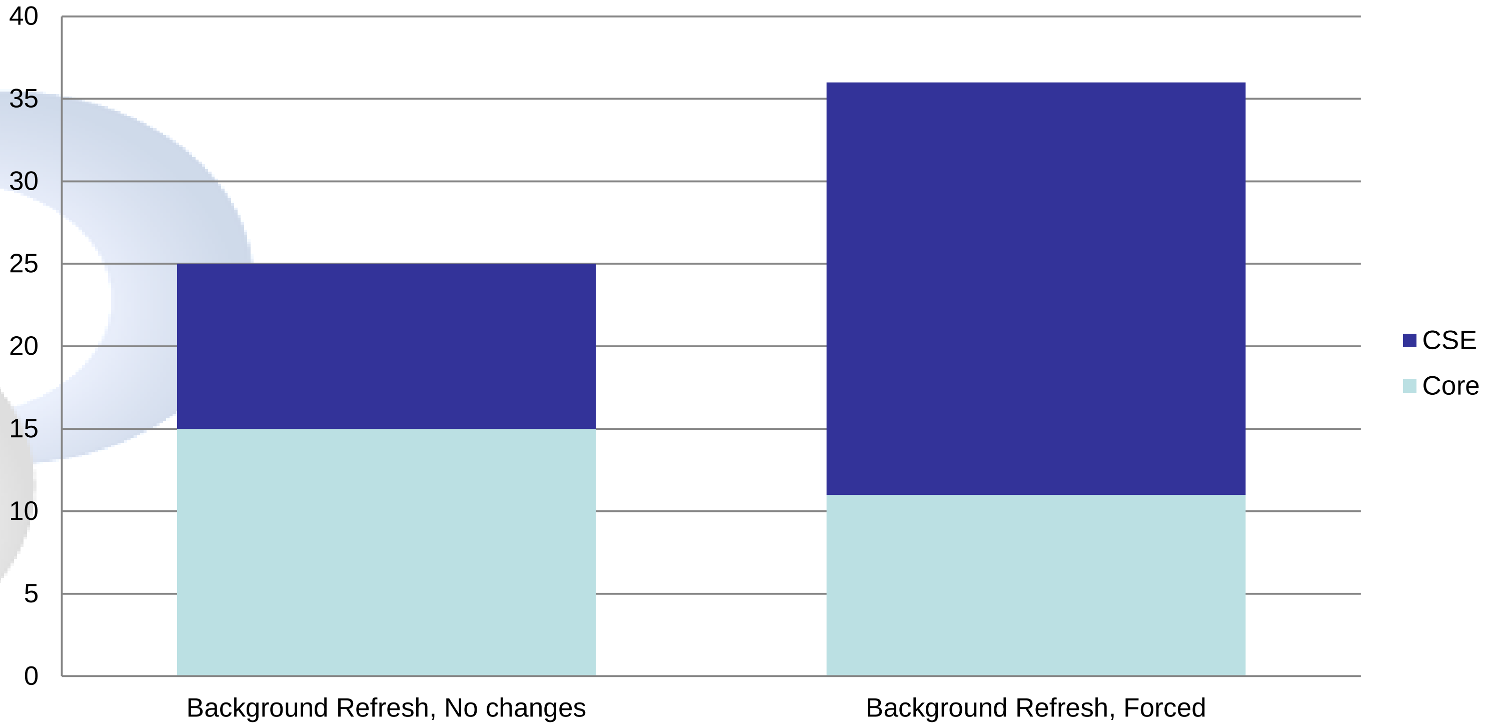
Synchronous CSEs & Performance

- Several CSEs can only be run during a foreground, synchronous processing cycle:
  - Software Installation
  - Folder Redirection
  - Disk Quota
  - GP Preferences Drive Mappings
- Careful consideration should be given around where you place settings from these CSEs (more on this later)

How GP Processing Affects Performance

- Darren’s Axiom of GP Performance:
  - Whenever a client is processing GPOs, and CSEs have to do work (i.e. something has changed in the GPOs), then CSE processing will typically take much longer than the enumeration of GPOs (i.e., “Core Processing”)
- The Corollary to this Axiom:
  - If no processing is going on, then Core and CSE processing takes roughly the same amount of time

GP Processing Times Compared



GP Performance Modifications to Avoid

- Avoid these if possible:
  - You set policy under Computer Configuration/Administrative Templates/System/Group Policy to force one or more CSEs to process even if there are no changes
  - You use security group filters extensively. Large ACLs on a GPO will take longer to evaluate
  - Many GPOs are linked to a given container. Links are stored as a concatenated string on the gpLink attribute of the container, and must be parsed out.
  - Complex WMI filters or excessive WMI filters. Evaluating WMI queries can be “relatively” expensive. (see my free WMI Filter Test Utility on www.gpoguy.com)

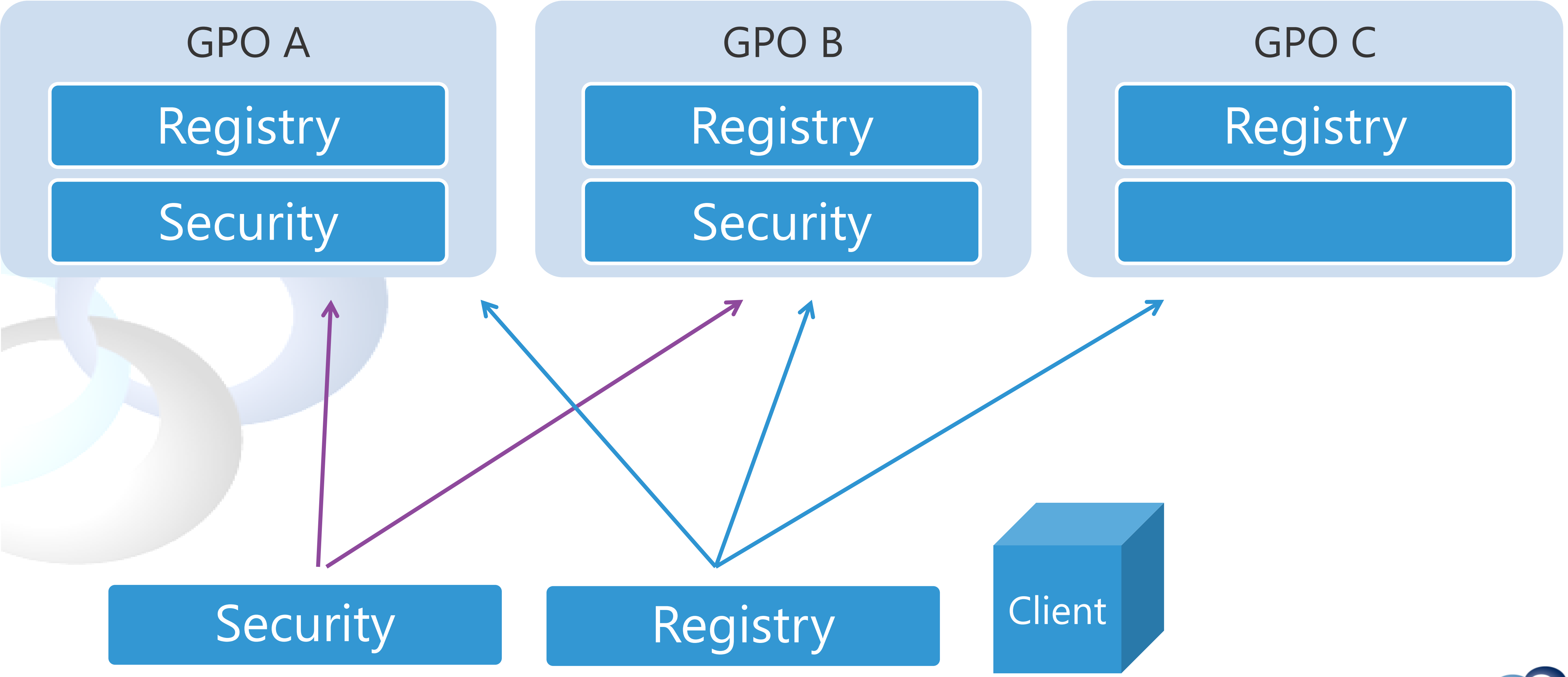
How Many GPOs is Too Many?

- There is no “best practice” on the number of GPOs to have (other than a theoretical maximum that a given user or computer can process of <1000)
- So, the number of GPOs is probably less important to performance than other factors, such as:
  - How often GPOs are changing
  - What those GPOs are doing (expensive vs. cheap settings)
  - How they are structured (changes to Monolithic GPOs can cause more processing than Functional ones)

Designing a GPO with Performance In Mind

- The GP Engine does not keep per-CSE version information
  - Why does this matter?
    - Example: GPO A implements both Admin. Templates and Security Policy. Computer account processes 5 GPOs, including GPO A. You make a change to GPO A’s Security Policy. GP Engine knows that “something” has changed, but not what, so during the next processing cycle, both Security and Admin. Template CSEs re-process policy settings.
  - Moral of the Story: If using Monolithic GPOs with multiple CSEs implemented within them, minimize changes

How Grouping of CSEs Impacts Performance



How Grouping Synchronous CSEs Impacts Performance

- Synchronous CSEs like Software Installation or GP Preferences Drive Mappings will force the next GP processing cycle to be synchronous when there’s a change
- This slows down startups or logons
- Group Synchronous CSEs together to avoid changes to other CSEs within a GPO forcing a synchronous refresh

Loopback and GP Performance

- Loopback comes in two modes: merge and replace
- Merge mode has potential for performance impacts
- Need to be careful about how you define loopback machines
  - I like dedicating an OU(s) to machines that require loopback
  - Avoid doing it on the whole domain!
- Merge mode should only be used if your scenario requires it
  - Depending upon how GPOs are linked and filtered, you can get settings processing twice for a given user on a loopback machine

Linking and Filtering Best Practices

- I’ve already mentioned the linking/filtering choices:
  - Link as close to intended target as possible
  - Use security/WMI/GPP filters as an exception
- Avoid lots of Domain-linked, Enforced GPOs
  - Useful for truly domain-wide security policies that MUST be in place
  - Otherwise, to be avoided, because they limit options downstream and can impact security or other changes that you need to make on subsets of machines

Scripts and GP Performance

- Avoid logon/startup scripts – use GPP when you can
  - It’s more deterministic and easier to troubleshoot
  - If I’m faced with adding a new script or using GPP with Item-Level Targeting, I’ll choose the latter almost every time
  - The only exception is when complex conditional logic is needed within a script to perform an action.

TOOLS FOR MEASURING AND OPTIMIZING GP

sdmsoftware

The Role of Event Logs

- On Windows 7 (and 8) and Server 2008-R2 and Server 2012, GP-related events are held in two places in the Windows Event Log:
  - System Log
  - GP Operational Log (Under Applications and Services Logs\Microsoft\Windows\GroupPolicy
- These logs provide high-level detail on each step of GP Processing, including overall timings, which DC was used, which GPOs were found and which CSEs ran

GP Trace Logging

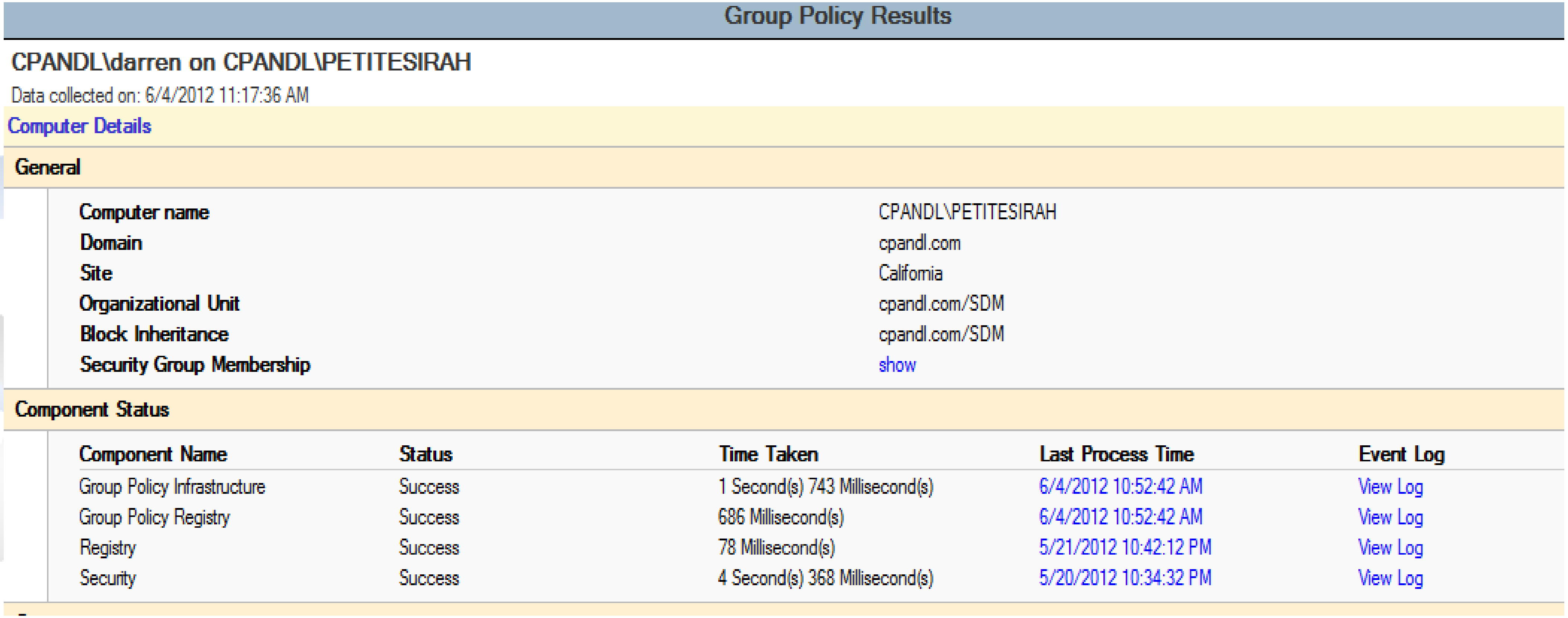
- GPSVC.log (used to be held in userenv.log in XP)
  - – Enabled using information in http://support.microsoft.com/kb/944043
- Provides VERY detailed trace logging of GP Processing
- Only useful if you can’t get enough info from Event Logs

sdmsoftware

Changes to RSoP Data in Windows 8/Server 2012

- RSoP (as seen through the GP Results Wizard in Windows 8 or Server 2012 GPMC) now provides timings on each CSE processed
- Also presents Operational Event log data in much better format

New RSoP Performance in Windows 8/2012



Group Policy Results

CPANDL\darren on CPANDL\PETITESIRAH

Data collected on: 6/4/2012 11:17:36 AM

Computer Details

General

Computer name	CPANDL\PETITESIRAH
Domain	cpandl.com
Site	California
Organizational Unit	cpandl.com/SDM
Block Inheritance	cpandl.com/SDM
Security Group Membership	show

Component Status

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	1 Second(s) 743 Millisecond(s)	6/4/2012 10:52:42 AM	View Log
Group Policy Registry	Success	686 Millisecond(s)	6/4/2012 10:52:42 AM	View Log
Registry	Success	78 Millisecond(s)	5/21/2012 10:42:12 PM	View Log
Security	Success	4 Second(s) 368 Millisecond(s)	5/20/2012 10:34:32 PM	View Log

Additional Tools

- My **GPTime** command-line utility
  - Returns overall GP processing time for local or remote computer/user
  - Download at http://www.gpoguy.com/Free-GPOGuy-Tools.aspx
- My GPHealth PowerShell cmdlet
  - Returns GP processing information, including timings, which GPOs & CSEs ran and overall status
  - Download at http://www.sdmsoftware.com/freeware
- My GP Health Reporter
  - GUI version of Health cmdlet
  - Download at http://www.sdmsoftware.com/freeware

GPO CONSOLIDATION—THE WHYS AND HOWS

Why GPO Consolidation?

- GP performance and ensuring that the right policies are getting delivered are further impacted by poorly deployed GPOs
  - Duplicate settings
  - Conflicting settings
  - GPOs that are no longer in use or are mis-targeted
- A consolidation exercise might be just the ticket if you've built up GP "clutter" over time

How to Approach a Consolidation

- Step 1: Assess What You Have
  - Take an inventory of your existing GPOs and their settings
  - Look at what’s linked where
- Step 2: Look for the low-hanging fruit
  - Look to remove unlinked GPOs, empty GPOs and GPOs that are obviously no longer in use
- Step 3: Look for GPO settings that can be eliminated due to redundancy, conflict, etc.
- Step 4: Test, test, test, then roll out changes
  - Provide yourself a fallback—this usually means creating new consolidated GPOs that can be linked or unlinked if needed.

Need Help with GP Consolidations?

- SDM Software can help!
- Check out our GPO Reporting Pak to get a handle on what you have:
  - GPO Compare
  - GPO Exporter
- Contact us at sales@sdmsoftware.com for more information on how we can help!

sdmsoftware

Additional Questions?