What Is Policy and What Can It Be?

Andrea Westerinen

Senior Architect and Manager, Cisco Systems

VP of Technology, DMTF

andreaw@cisco.com

Topics

- Definitions
- What and Why of Policy
- What Policy Is and Is Not (or Policy Is Like a Snowflake)
- Automated Management and Other Policy Synonyms
- SLAs
- An Ideal World and How to Live There
- Policy, Pigs and Ponder

Merriam-Webster’ Definition

- **1 a :** prudence or wisdom in the management of affairs **b :** management or procedure based primarily on material interest
- **2 a :** a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions **b :** a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body

IETF Terminology RFC3198

- "Policy" can be defined from two perspectives:
  - A definite goal, course or method of action to guide and determine present and future decisions
  - Policies as a set of rules to administer, manage, and control access to network resources [RFC3060]
- These two views are not contradictory since individual rules may be defined in support of business goals

Storage Networking Industry Assoc’s (SNIA) Definition

- “The measurable, enforceable and realizable specification of method, action and/or desired state that meets service requirements in a storage-based information infrastructure."

Paper from Univ of Surrey

- “Design and Implementation of a Policy-Based Resource Management Architecture”
- A means of extending the functionality of management systems *dynamically*
- Guides the behavior of a network or distributed system through high-level declarative directives
- That are dynamically introduced, checked for consistency, refined and evaluated
- Resulting typically in a series of low-level actions

Why Policy?

- “Extend” management infrastructure
- Move from passive monitoring and human based intervention to active management
- Intervene as problems are occurring at compute speeds, not human reaction times
- Enable reuse and duplication of an expert’s knowledge and processes
  - This is the real “sound byte”
  - “Knowledge for knowledge’s sake” is not enough

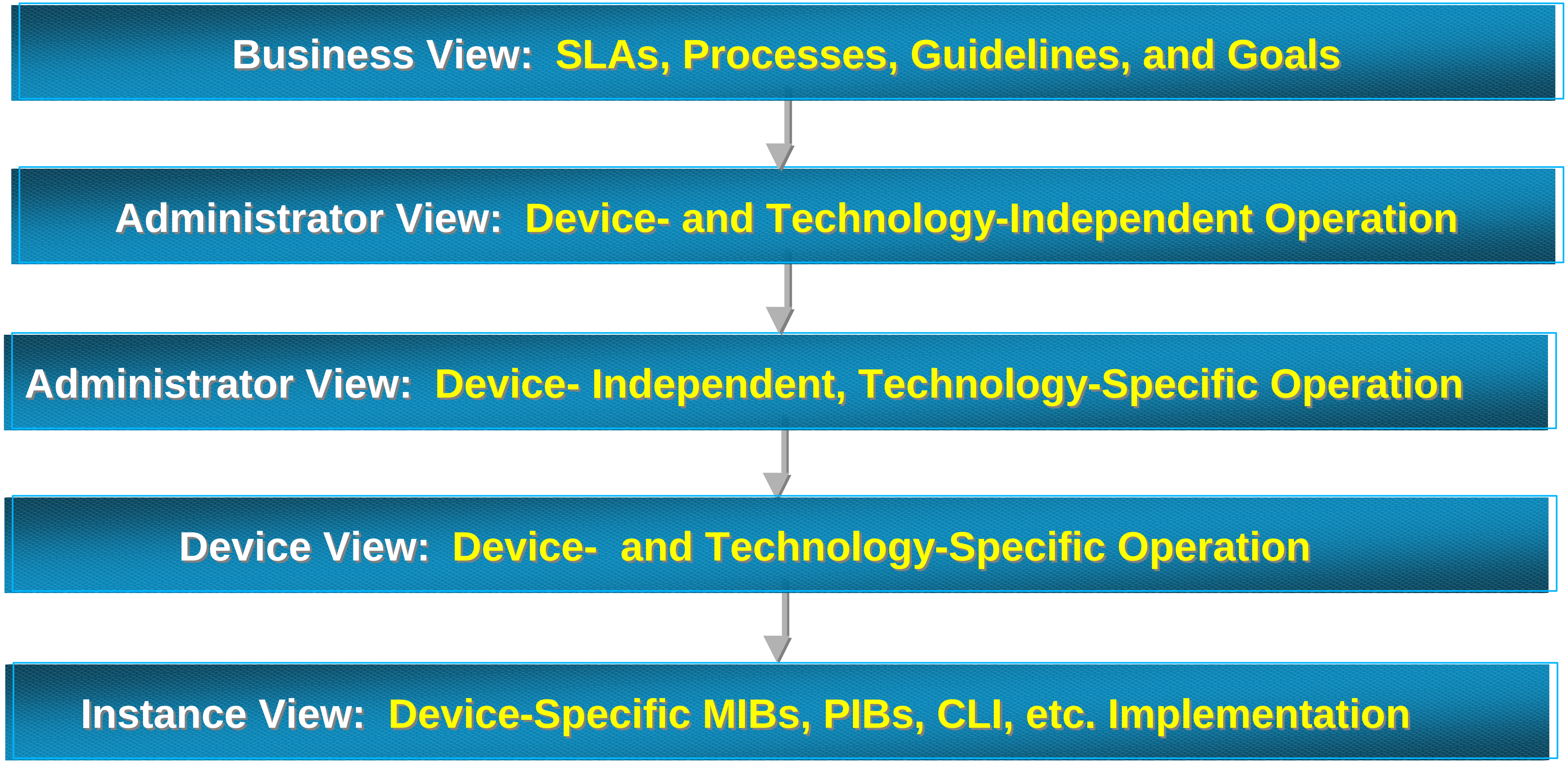
Knowledge and Policy

- Knowledge is much more than data
- Is the manipulation and correlation of data and higher level information (for example, trend analyses) to define patterns, draw new conclusions, create more information, and determine courses of action
- Is based on analysis, and yields strategy and "best" practice
- Is the reasoning regarding "how to" accomplish something based on the "who, what, where and when" of lower level data

Levels of Policy

- Goals -> Rules -> Device Commands
- Considering constraints (What can’t be allowed or can’t be done)
- Purpose to allocate and guide the operation of computing and networking resources
- Manages and is driven by business- and mission-critical data and operations

Policy Continuum (J. Strassner)



Business View: SLAs, Processes, Guidelines, and Goals

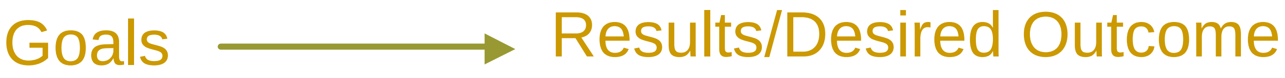
Administrator View: Device- and Technology-Independent Operation

Administrator View: Device- Independent, Technology-Specific Operation

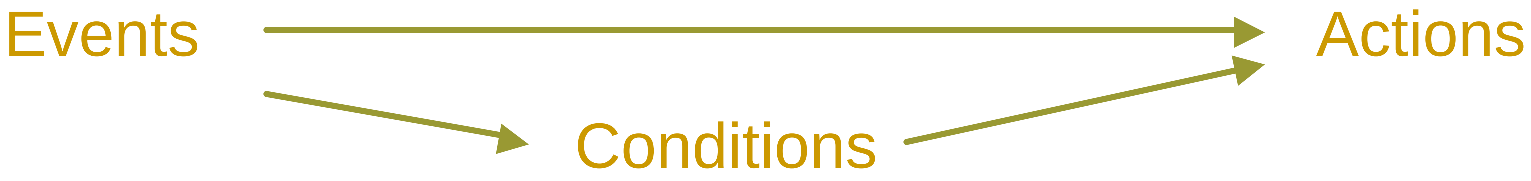
Device View: Device- and Technology-Specific Operation

Instance View: Device-Specific MIBs, PIBs, CLI, etc. Implementation

Policy “Rules”



If Administrator password entered and validated using appropriate shared secret, then assume that trust is established



If FileSystemThreshold event generated, AND (Unused storage is available on the System on which the FileSystem resides AND That storage space is > 1G), then allocate <company-specific amount> of storage and add this to the FileSystem’s StorageVolume

Anti-Characteristics of Policy

- Static
  - Predefined conditions and actions, determined by the vendor, able to be combined in predefined ways
  - Logical conclusion: Any if-then-else statement in a program becomes policy IF the customer’s input is used in the if clause
- Single level
  - Typically low-level device actions
- Policy aligned with the vendor or product, not with the business/company using the product

Anti-Characteristics of Policy

- Not about an end-to-end business process but about a single “domain”
  - Network QoS, storage arrays or security
- Why worry about setting this or that traffic flow when the network is shutting down?

Other “Policy Problems”

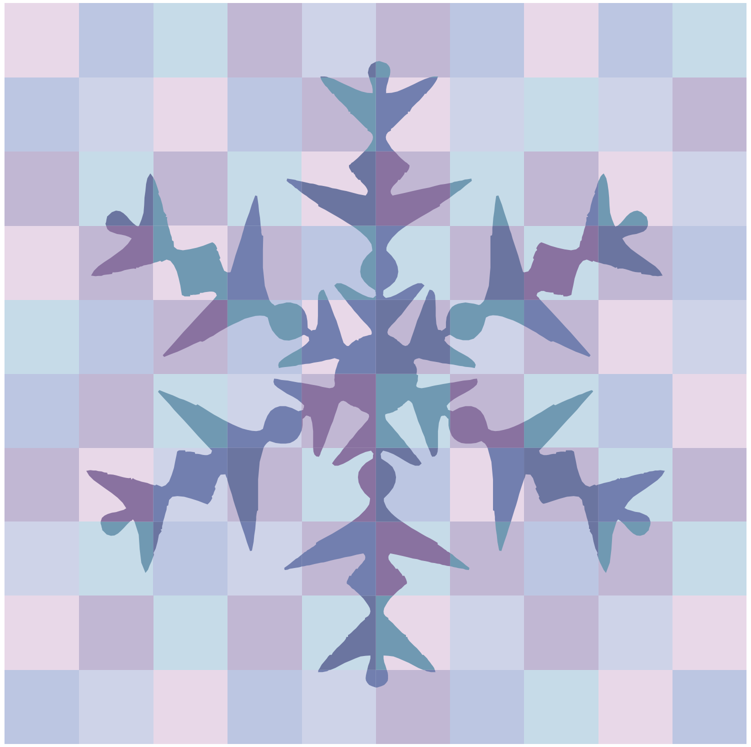
- Tendency to classify any data used in a policy infrastructure as “Policy”
  - Data and operations are used BY policy OR by humans (the operators of the systems and networks)
  - Definitions and semantics should not change
- Focus on infrastructure
  - More trackable problem than multi-domain, multi-vendor, interoperable policy
  - But only a means to an end

Policy Infrastructure

- Much time spent on how policies are stored, distributed and enforced
  - Policy repository and GUI
  - Protocols
  - PDPs
  - PEPs
- Really are matters of implementation
- Less important than defining, refining, translating, and performing conflict detection on policies in a multi-vendor, interoperable fashion

Policies Like Snowflakes

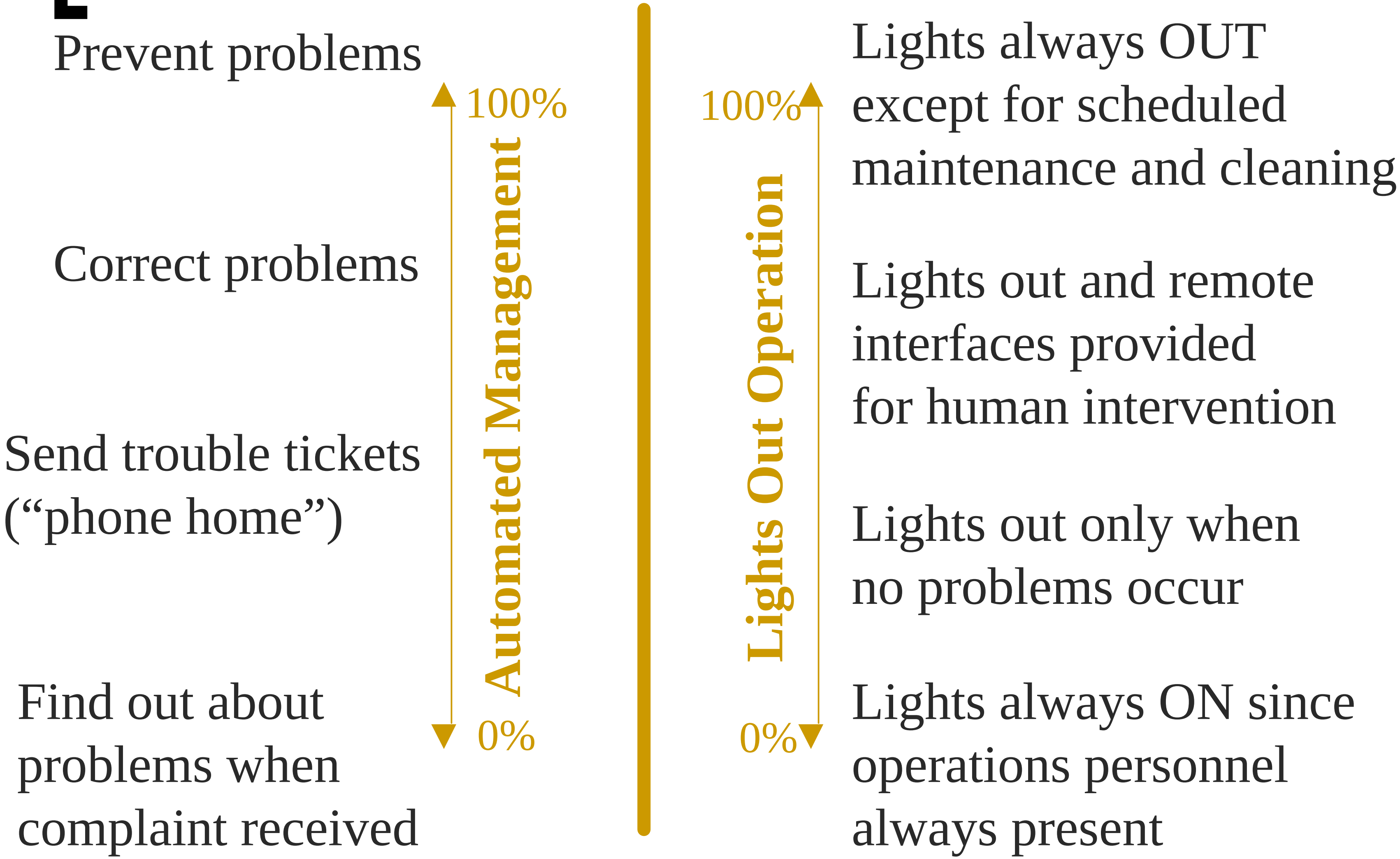
- Dynamically changing as they form and melt
- All different
- Float down from the clouds taking a broad view of the earth to a specific patch of ground
- Do you care how they formed or what cloud that they came from, when you want to build a snowman?



Synonyms for Policy, Yesterday and Today

- Automated management
- Self-healing, self-managing systems
- Autonomous systems
- Autonomic computing
- “Lights out” computing
- Intelligent networks and systems
- “Active” networks

Analyzing Automated Mgmt



Prevent problems

Correct problems

Send trouble tickets (“phone home”)

Find out about problems when complaint received

Lights always OUT except for scheduled maintenance and cleaning

Lights out and remote interfaces provided for human intervention

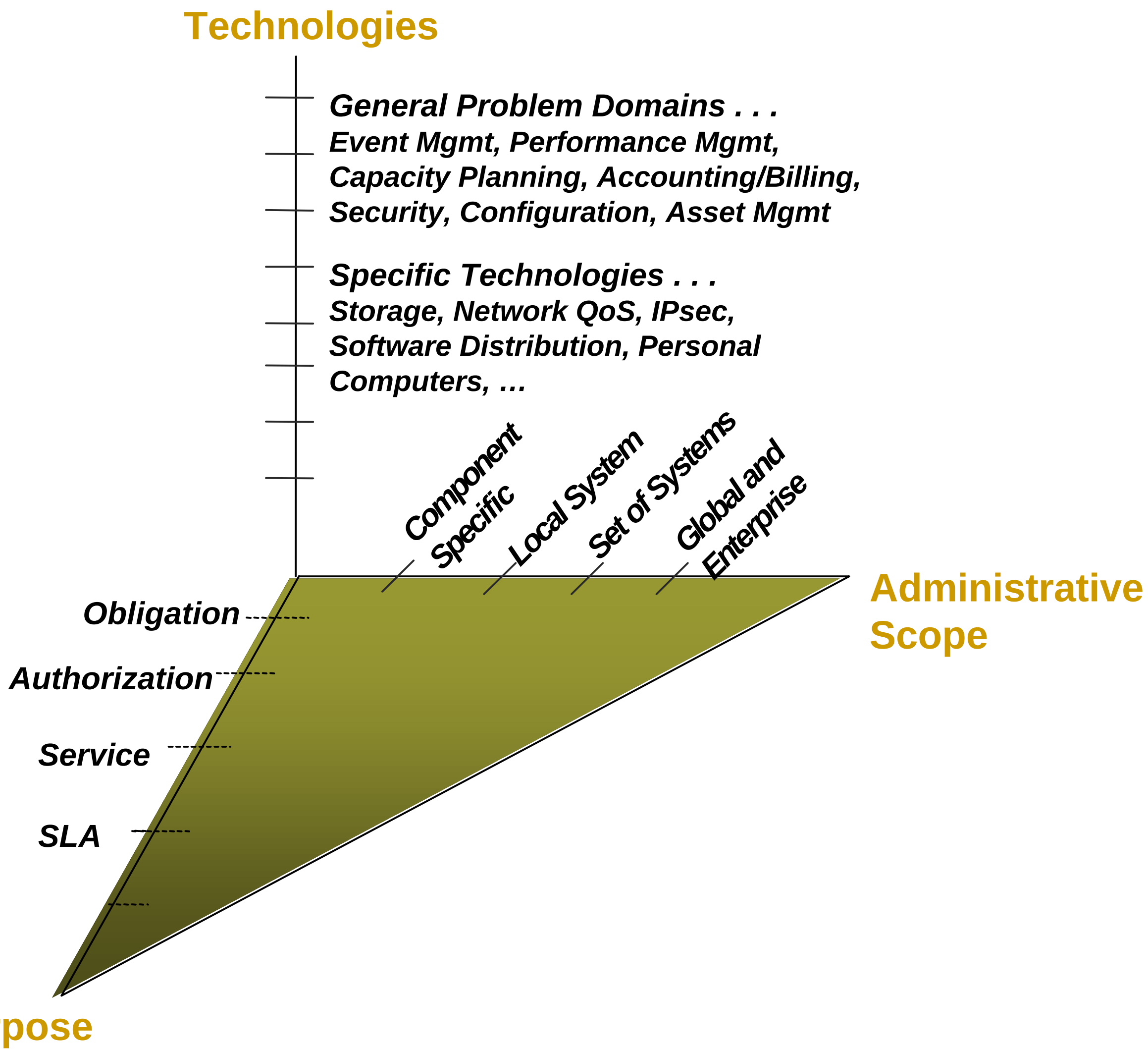
Lights out only when no problems occur

Lights always ON since operations personnel always present

Achieving Automated Mgmt

- Requires a complete and consistent definition of a business' processes, guidelines and procedures
- Requires the capture and distribution of the knowledge of the product and business' experts
  - Describing which trends and conditions are important versus which are trivial, and what to do when these trends and conditions are observed
- Requires sufficient tools and infrastructure to monitor state and the current environment, and to integrate data for all vendors, possibly across the entire enterprise

Policy as a 3D Space



Technologies

General Problem Domains . . .
Event Mgmt, Performance Mgmt,
Capacity Planning, Accounting/Billing,
Security, Configuration, Asset Mgmt

Specific Technologies . . .
Storage, Network QoS, IPsec,
Software Distribution, Personal
Computers, …

Component Specific

Local System

Set of Systems

Global and Enterprise

Administrative Scope

Obligation

Authorization

Service

SLA

Purpose

But Where Are We Today?

- Overprovisioning instead of policy
- Single-vendor
- Single problem space
  - What good is high-priority, high-throughput network traffic if the storage array on the receiving end loses the data?
- Lack of trust in the solutions
  - When humans make mistakes all the time, would a policy-based system make the mistakes faster?

“Self-Repairing Computers”

- Scientific American, June 2003
- Researchers from Stanford and Berkeley
- Lots of talk about self-repairing systems, but not policy
- “Digital computing performance has improved 10,000 fold in the past two decades … We pay a price for these enhancements, though. As digital systems have grown in complexity, their operation has become brittle and unreliable. Computer-related failures have become all too common.”

ROC-Computing

- “Inconvenience aside, the situation is also an expensive one: annual outlays for maintenance, repairs and operations far exceed total hardware and software costs, for both individuals and corporations.”
- Recommendation: ROC-computing
  - Recovery-oriented computing

ROC-Solid ☺

- Quick comeback / rapid recovery
- Pinpointing problems / failure analysis
- Wiping away errors / “un-do”
- Injecting test errors

- Uh-oh, no policy except in a sidebar and then the reference is to “computational and storage resources that manage themselves”
- Ideally both prevent problems AND recover quickly

Service Level Agreements

- Much business interest in SLAs and their specific objectives (SLOs/metrics)
- There are two aspects of an SLA:
  - The business negotiation and contractual elements of an SLA and its incentives/recourses
  - The management and maintenance of the individual objectives
- Consider this:
  - Couldn’t the SLOs just be the specific “goals” maintained by a policy-based management infrastructure?

SLA Management

- Monitoring and maintenance
  - Maintenance performed via manual intervention and/or policy
- SLA monitoring and maintenance handled consistently with other management tasks
  - IE, any concepts or attribute can be used independently, or within the context of an SLA
- Necessary concepts:
  - SLA contract for reporting
  - Individual SLOs and definitions of compliance
  - Current values and ability to determine compliance with objectives

SLA “Automated” Maintenance

- Ability to invoke a policy action in the event of non-compliance with a service objective -> Tie to notification and indication mechanisms
- Ability to identify specific entities where rules apply and actions are enforced
- Consistent and coordinated notion of the managed environment
  - An element may be managed under multiple SLAs and within several problem/technology domains

An Ideal World

- Complete description of managed environment
- Emphasis on applying “interoperable knowledge” to the managed environment
- Requires:
  - Common information model to describe and organize the managed environment
  - Unambiguous policy definition/language to convey information and to manage the system
  - Extensible expression of policy as a continuum of policy rules

More of the Ideal World

- Policy is a *declarative* system that controls computing and networking resources (configuration and operation) end-to-end
  - At the highest level, describes desired state and constraints of the business and managed elements
  - At lower-level is translated to the individual device inputs (CLI?, SNMP?) to “make it so”
  - Monitors resources to verify conformance to business and operational goals, and adjusts as necessary

Ideal Worlds & Semantic Webs

- Is this possible?
- Scientific American, May 2001
- "The Semantic Web"
- Berners-Lee, Hendler and Lassila
- "Information is given well-defined meaning, better enabling computers and people to work in cooperation … For the semantic web to function, computers must have access to structured collections of information and sets of inference rules that they can use to conduct automated reasoning."

Ideal Worlds & Semantic Webs

- “Human language thrives when using the same term to mean somewhat different things, but automation does not.”
  - Clowns, business addresses and PO Boxes
- “Human endeavour is caught in an eternal tension between the effectiveness of small groups acting independently and the need to mesh with the wider community. A small group … produces a subculture whose concepts are not understood by others. Coordinating actions across a large group, however, is painfully slow and takes an enormous amount of communication.”

How Do We Accomplish Policy-Based Management?

- Keep communicating and standardizing across products, vendors & problem domains
- Establish "trust" in policy
  - Start with detailed best-practice workflows and walk them manually
  - Once validated, automate a portion or all of the workflow
  - Repeat as necessary
- Work through the standards organizations and not individually
  - DMTF, IETF, SNIA, GGF, …
- But, all the standards bodies should be working *together*

Tackling the Tough Problems

- Information modeling for end-to-end semantics
    - That can decompose from the general to the specific
- Standardization of information and mechanisms to translate rules
    - Between abstraction levels, products, vendors and problem domains
- Ease testing burden by using standard semantics in trigger and condition clauses, and define actions as the invocation of standard methods and operations
    - Also begins to address conflict detection since standard data, methods and operations can be analyzed together

Policy, Pigs and Ponder

- Hard problem: "If at least two of a famer’s pigs are squealing, then he/she must feed one of the pigs that isn't squealing.“
- Another constraint: Graft policy onto an information model by introducing references to the suitable objects in the model
  - PigKeeper and Pig classes, KeeperKeepsPig association, SquealingPig notification, and FeedPig method on the PigKeeper

Policy, Pigs and Ponder

- oblig feedNotSquealingPig {
- On CIM_SquealingPigIndication(Pig1) && CIM_SquealingPigIndication(Pig2);
- // 2 squealing pigs
-     subject /pigkeepers;
- // i.e., all pig keepers
-     do (t = self.KeeperKeepsPig->reject (isSquealing)) -> self.feedPig(t);
-     when Pig1!=Pig2   // they are different pigs
-     and Pig1.KeeperKeepsPig =
-         Pig2.KeeperKeepsPig = 'self';
-           // and I am the keeper