

System Center User Group
Columbus, Ohio
July 21, 2009

Implementing Custom Management Packs

Presented by: Jon Kaloz



Sponsored by:

BENNETT ADELSONsm
Microsoft® Solution Center

Overview

- Overview of Environment/Project
 - Problems
 - Technologies
 - Requirements
- Implementation examples
 - 3rd Party Management Packs
 - Overview of Management Packs
 - Custom Management Pack Development
 - Demo of various Management Pack components and usage
 - Security Roles and Support Delegation
 - Overview of Security and Support Delegation and integration into environment

SCOM Management Packs

- What is a Management Pack?
 - Model containing a comprehensive set of pre-defined rules that define how an application or service functions
 - Describes what data to examine and performs live analysis via workflows of that data
 - The instructions that SCOM uses to tell the clients what and how to monitor a system

Management Packs

- Management Packs are XML documents that contain the monitoring instructions
- Management Packs can be “Sealed” and made read only
 - This is a read-only encrypted version of the XML document
 - Most 3rd Party Management Packs are provided in a Sealed State
- Management Packs are easy to work with
 - Provides central management
 - Rapid deployment of monitoring enhancements and changes
 - Easy to Import/Export for testing and deploying

3rd Party Management Packs

- There are numerous 3rd Party Management Packs available for use
- Benefits of 3rd Party Management Packs
 - Written by the developers and technology experts of the application or service being monitored
 - Rapid deployment with minimal management overhead
 - Can be customized with externalized Overrides to meet implementation/environment specific needs (discussed later)

3rd Party Management Packs

- Examples:
 - Microsoft Operating Systems (Server/Client)
 - Microsoft Applications (SQL/IIS/DNS/Active Directory/Exchange/etc)
 - Hardware (Dell/HP/etc)
 - Good Sources for 3rd Party Management Packs
 - Microsoft Library –
 - <http://technet.microsoft.com/en-us/systemcenter/cc462790.aspx>
 - Quest Software –
 - <http://www.quest.com/quest-management-xtensions-operations-manager/>
 - <http://management-extensions.org/monitorextensions.jsp>

Custom Management Packs

What if there is not an existing 3rd Party Management Pack available for my application, service, or business process?

- Often times there will be in-house developed applications or processes that will not have a 3rd Party Management Pack available
 - Custom Management Packs must be created to facilitate the monitoring of these applications, processes, and services
 - Operations Manager provides the ability to rapidly develop, test and deploy custom monitors to meet these needs

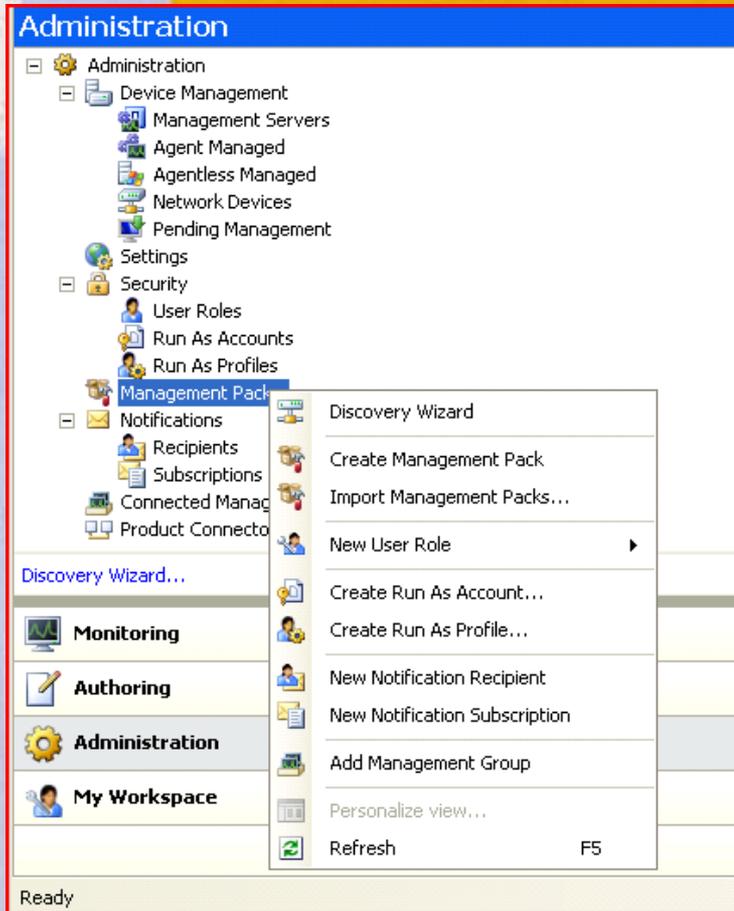
Developing Custom MP's

- Anatomy of a Management Pack
 - Monitors
 - Rules
 - Attributes/Discoveries
 - Tasks
 - Groups
 - Overrides
 - Views
 - Knowledge Base Articles
 - Others (Templates)
 - Web Application, Windows Service, TCP Port, OLE DB
 - Distributed Application

Developing Custom MP's

- Management Pack Creation tools
 - Operations Manager Console
 - Operations Manager Authoring Console
 - Any Text editor
- Demos will be performed in Operations Manager Console
 - Authoring Console can be used to perform these functions as well
 - Operations Manager Console will provide instant deployment to agents without the need to import and export
 - Overhead using SCOM Console vs. Authoring Console

Creating a New Management Pack

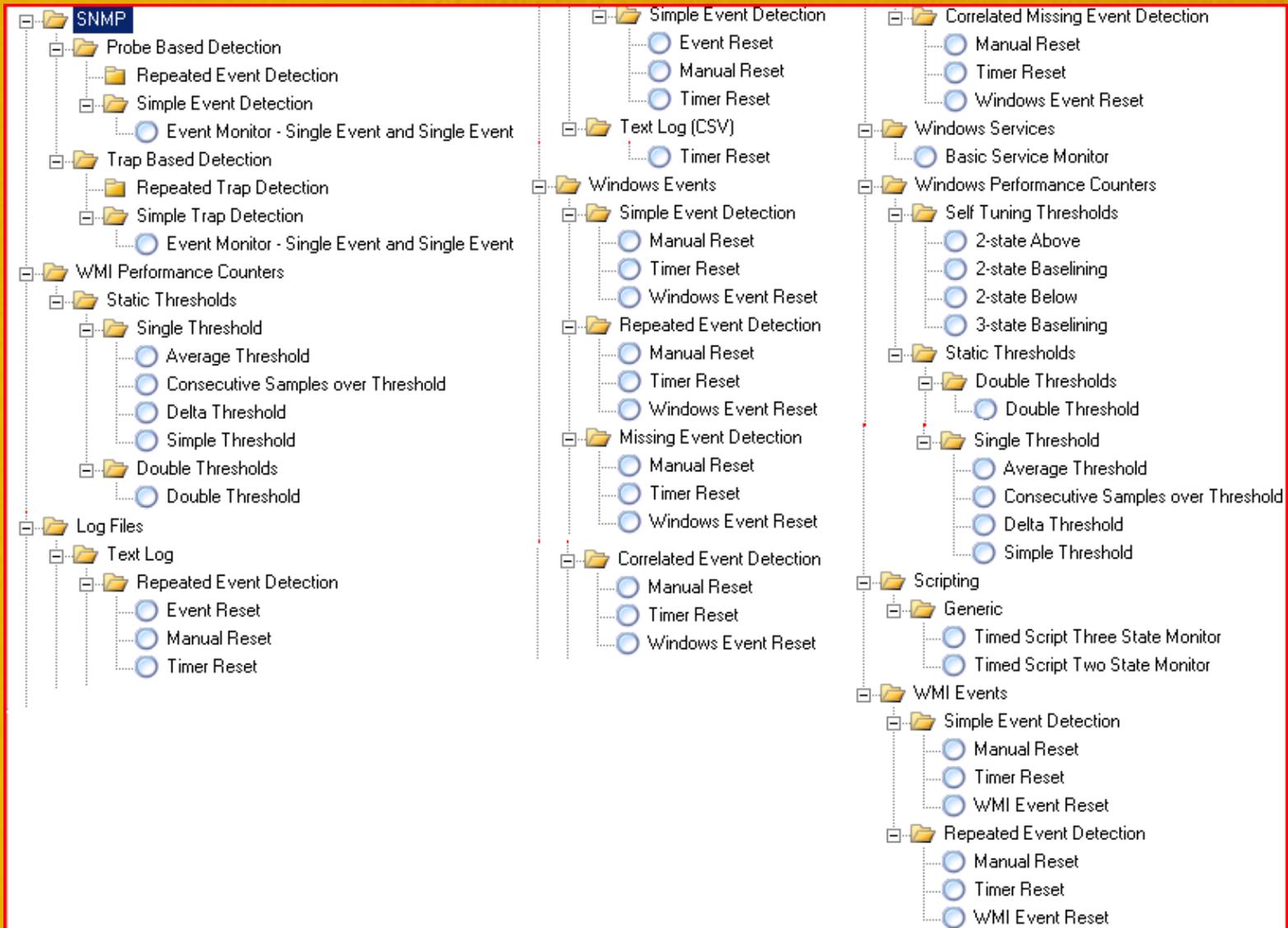


- From SCOM Console
 - Administration Section
 - Management Packs
 - Right Click → New “Create Management Pack”
 - Specify Unique Name and version for Management Pack
 - Add Description and KB
 - MS Word XP or greater
 - 2005 Visual Studio Tools for Office Required

Monitors

- What is a Monitor?
 - Checks for certain events and occurrences on the system
 - Windows Events, SNMP Traps/Probes, Log Files, Services, Custom Scripts
 - Monitor typically has known Healthy and Unhealthy information to key off of
 - Event X = Unhealthy (Problem Occurring)
 - Event Y = Healthy (Problem Resolved)
 - Impacts the system's "State of Health"
- System Health
 - Indicates the overall status of the system rolled up through individual monitors
 - Levels of System Health/Monitor Health
 - Healthy
 - Warning
 - Critical

Monitors Types



Monitor Samples/Demo

Basic Service Monitor

- Windows Deployment Server service (**demo*)
 - Diagnostic and Recovery Tasks

Timed Script Two State Monitor

- Scheduled Task - Could Not Start
 - MOM.ScriptAPI & State Property
 - More info on MOM Scripting Objects
 - <http://msdn.microsoft.com/en-us/library/bb437621.aspx>

Consecutive Samples Over Threshold (Performance)

- ShopperTrak - CPU Utilization

Event Reset (Log File)

- Credit - FiPayrte - Head Office Down

Correlated Missing Event

- Disk Mirroring - Mirror Rebuild

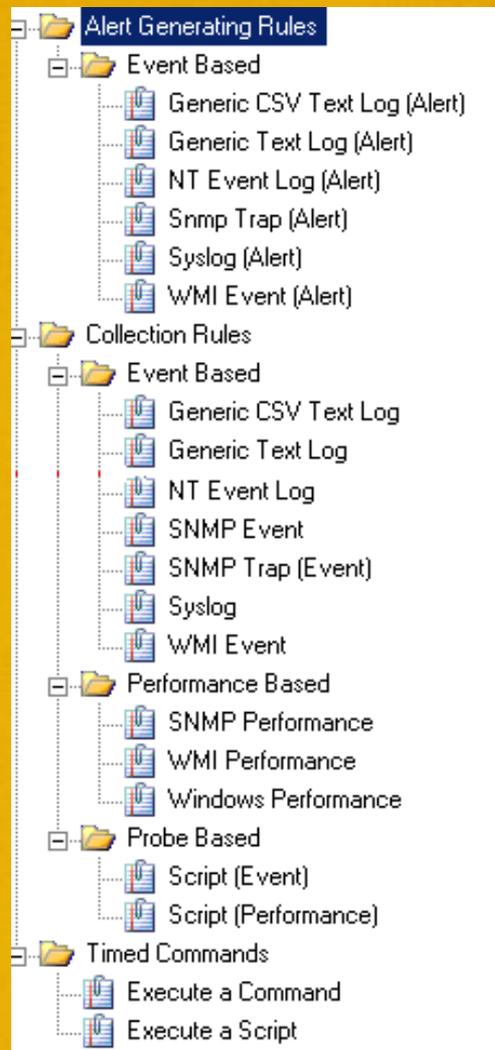
Windows Event Reset

- Store Account Management - File Processing

Rules

- What is a Rule
 - Checks for certain events and occurrences on the system
 - Windows Events, SNMP Trap/Probe, Log Files, Services, Custom Scripts
 - Does NOT impact the "State of Health" for the monitored system
 - Typically has a known error event, but not correlated correction event
 - Associated Alerts must be manually closed

Rules Types



- Alert Generating
 - Generate Alerts in the SCOM Console
- Collection
 - Gather specified events centrally in SCOM
- Timed Commands
 - Execute regularly scheduled scripts or programs on the systems

Rule Samples/Demo

Alert Generating

- RCS - Scanner Not Programmed Correctly
 - Windows Event Driven
- Credit - CrdLog - Pending, Timeout, Authorizer Not Up, or Bad Pin Block
 - Log File Driven

Timed Commands

- DSW - Set Deployment Group
 - Timed Script
- DSW - Start DCM Scan and Evaluate Results
 - Timed Script

Collections

- DSW - Security Event Log Collector
 - Event Collection

Attributes and Discoveries

- What is a Discovery?
 - Provides the ability to interrogate the system for a registry key or WMI information and store it in an Attribute that is tied to a monitored object
 - Useful for defining and identifying specific applications or system processes on monitored systems dynamically
 - Can define a new object class/target for monitoring or extend an existing class/target

Attributes Sample/Demo

Discovery for System Information

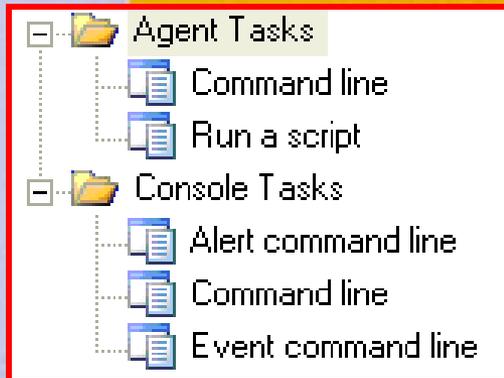
- System Time Zone/Deployment Group
 - Registry entries on all systems (**demo*)
 - Used to create views in SCOM to better support and validate SCCM advertisements
 - Target Tasks and Monitors based on Role

Tasks

- What is a Task?
 - A task is an action that is executed on the system or on the support engineer's system to perform specific support or management operation
 - Provides historic run information and results
 - Task Status – Run time/Results/Output
 - Excellent tool for consolidating common support and system management functions into single interface

Tasks Types

Agent Tasks



- execute on the monitored system in the context of the SCOM agents account or specified action account for the task
- can be executed via the SCOM Console (Actions) or automatically by monitors or rules (Recovery and Diagnostic Tasks)
- provide tracking of when and what the results were for the tasks fired

Console Tasks

- Executed from the SCOM Console, but run on the support users local system in the support context

Tasks Samples/Demo

Agent Tasks

- Recovery & Discovery
 - Windows Deployment Services (**demo*)
- Action Tasks
 - Starting/Stopping Services
 - Running SCCM DCM Scan
 - Logging off User/Displaying logged in users
 - Printer Management
 - Delete Local Profile
 - *Agent based with User Input*
 - DHCP Management

Tasks Samples/Demo

Console Tasks

- Run Active Directory Users and Computers
- SMS Remote Control (*Demo)
- RDP
- UNC/Map Drive to System
- Computer Management Console

Groups

- What is an Operations Manager Group
 - Provides the ability to create logical grouping of monitored objects based on object types and attributes of the monitored objects
 - Groups can have Explicit, Dynamic, and exclusion membership rules for flexible creation and maintenance
- Common Usage
 - Target monitoring and monitoring customizations to a specific object(s)
 - Customize views and organization of monitoring data in logical views

Groups Samples/Demo

Group by system Role

- ISP (Store Server)
- Register
- Manager Workstation
- PCI Validated Systems
- Pilot/Debug Group

Group by Object Type

- DHCP Scopes
 - Provide limited access to Help Desk
- Scheduled Tasks
 - Override Based on Discovery (EOD Task)

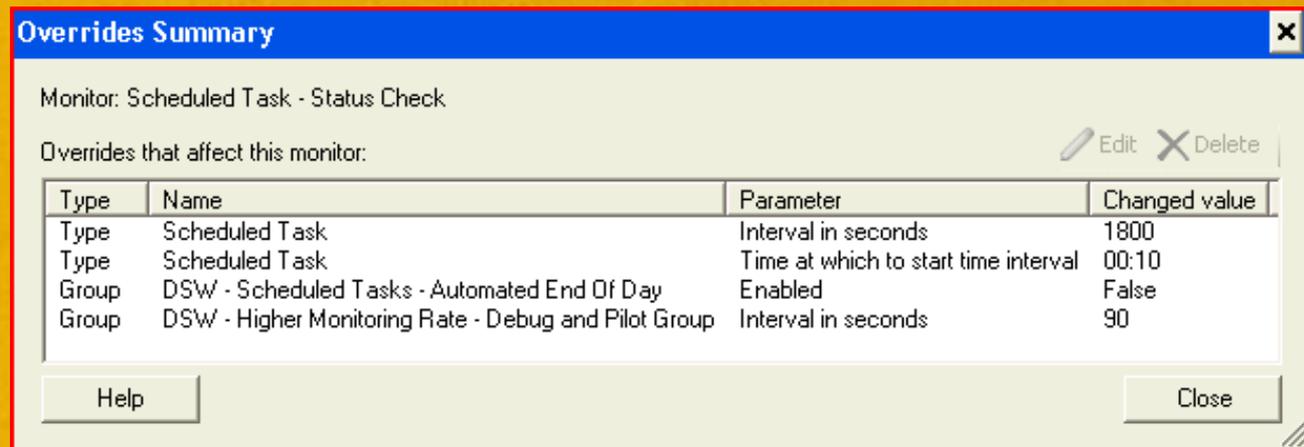
Overrides

- What is a Override
 - Provides the ability to further customize and target monitors from 3rd Party and Custom Developed Management Packs
 - Typically Override most all Rules and Monitors
 - Create Rule and Monitors as Disabled
 - Enable them via Override to targeted systems
 - Typically create a separate Management Pack for all 3rd Party Overrides
 - Unsealed Management Packs will force the override to be stored in its own Management Pack
- Common Usage
 - Enable or disable a monitor or rule
 - Change the frequency for which a timed command or performance monitor executes
 - Change the thresholds for when an alert is raised

Override Samples/Demo

Monitor Override

- Shopper Track – CPU Utilization
 - Enabled for ISP Systems Group
 - Other options (Frequency, Threshold, Priority, Severity, Auto-Resolve Alerts, etc)
- Automated End of Day Scheduled Task

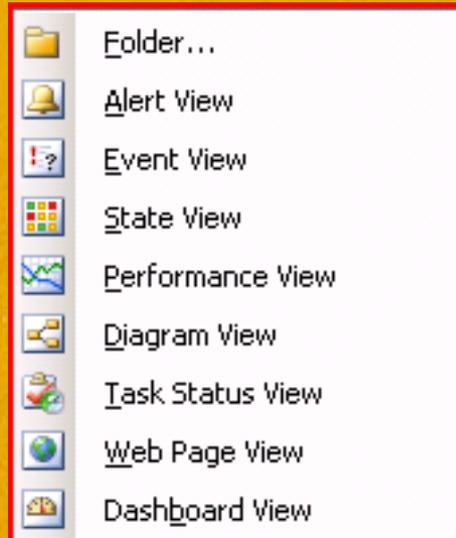


The screenshot shows a window titled "Overrides Summary" with a close button (X) in the top right corner. Below the title bar, the text "Monitor: Scheduled Task - Status Check" is displayed. To the right of this text are two buttons: "Edit" (with a pencil icon) and "Delete" (with an X icon). Below this is the text "Overrides that affect this monitor:". A table follows with four columns: "Type", "Name", "Parameter", and "Changed value". The table contains four rows of data. At the bottom of the window are two buttons: "Help" on the left and "Close" on the right.

Type	Name	Parameter	Changed value
Type	Scheduled Task	Interval in seconds	1800
Type	Scheduled Task	Time at which to start time interval	00:10
Group	DSW - Scheduled Tasks - Automated End Of Day	Enabled	False
Group	DSW - Higher Monitoring Rate - Debug and Pilot Group	Interval in seconds	90

Views

- What is a View
 - A view is what provides the logical view of all the monitoring data being evaluated and collected
 - There are several types of views that can be created based on the type of monitoring data you want to review



View Samples/Demo

- Views can only be created in the Monitoring Pane (From SCOM Console)
- DSW - Deployment Tracking
 - Pilot
 - Deployment Group 1
 - Deployment Group 2
- DSW - Help Desk
 - Computers
 - Active Alerts
 - DHCP Scopes
 - POS Event Log
 - Performance
- DSW - Store Systems
 - ISP Servers - Health Critical or Warning
 - All Open/Active - Backup Process Alerts
 - DCM - Compliance Results - Success and Failure
 - DCM - Compliance Failures - Items Out of Compliance

Knowledge Base Articles

- Knowledge Base Articles provide the critical support information that are related to the monitor, rules and other management pack components.
- Provides common information in multiple locations (Alerts/Health Explorer/Monitor Properties)
 - Summary
 - Configuration
 - Causes
 - Resolutions
 - Additional Information
 - External Knowledge Sources
- Allows for quick ramp up of support staff
 - Issue information is readily available within the alert
 - Quicker problem resolution time with steps on how to troubleshoot and correct the issue

Knowledge Base Articles

- Creation
 - Unlike all the other monitoring components, KB articles currently cannot be created within the SCOM console and requires the Authoring Console (maybe available in R2)
 - Also requires Visual Studio Toolkit for Office to be installed
- Sample
 - Windows Deployment Server (*Demo)

Other Custom Monitoring Options

- Management Pack Templates
 - Included monitoring templates to rapidly develop monitors for monitoring
 - Provide a framework to collect data and generate monitor alerts based on common aspects of common application components



Other Custom Monitoring Options

Management Pack Templates

- Web Application Sample
 - Store Portal Client
 - Web Service on all store servers
 - Transmits and Receives critical store data and configurations
 - Web Application Template used to create monitor
 - Automatically generates monitors
 - DNS Request
 - Download Time
 - Request Time
 - SSL Validation
 - Expiration/Valid/CN
 - Performance Counters
 - Simulated “Watcher Nodes”

Other SCOM Customizations

- Security Roles
 - Security Roles broken out and support views, tasks and access broken down in targeted fashion
 - HelpDesk
 - Level 2
 - Level 3
 - Web Support
 - Security
 - Provided the ability to provide target view and support tasks to appropriate support groups

Other SCOM Customizations

- Support Staff Lockdown via Roles
 - Some support activities require the support person to have elevated permissions on the system to perform their job
 - Stop and Start Services
 - Manage Printers
 - Delete Profiles
 - Log users off systems
 - Display and manager POS applications
 - Run various commands to gather information
 - Stop Specific Running Processes
 - Reboot a system
 - Unlock/Reset Passwords on AD account
 - Created a new Role in SCOM for the various groups
 - Help Desk was now able to perform over 90% of the daily support activities for the stores via the SCOM interface
 - Tasks Status logging of what actions were taken by who and when as well as the results
 - Views, Objects and Applications Scoped so they can only access what they need to support

Other SCOM Customizations

Product Connectors

- SCOM → LogLogic Connector
 - PCI Requirements to log and retain specific event log information long term
 - C# connector written with the managed code framework provided with SCOM
- SCOM → CA Service Desk
 - Automate Support Case Creation
 - Web Service
 - SCOM Connector (WIP)
 - E-Mail Eater
 - Send pre-formatted email to Service Desk mailbox
 - Generates support case based on alert criteria

Questions?

