SYSTEM CENTER 2012 CONFIGURATION MANAGER: COMPLIANCE SETTINGS

John J. Rayborn

East Carolina University

Author Note

This paper was prepared for course ICTN 6865, Fundamental Network Security, taught by Dr. Phil Lunsford.

Abstract

The intent of this paper is to provide a discussion on what compliance means as it relates to desired configuration, why it is important to organizations to ensure systems on the enterprise / corporate networks are compliant, and provide information on how an organization can look to ensure desired configuration compliance is being obtained. It is meant to be informational as well as educational for awareness purposes. I will be looking to explain how desired configuration for compliance is accomplished as well as provide information / screenshots on the use of the Compliance Settings component available in Microsoft System Center 2012 Configuration Manager. The paper will also provide information on how compliance standards requirements among various Industries can be accomplished through the use of System Center 2012 Configuration Manager.

Contents

Introduction

As threats from attackers persist on corporate networks, the management and monitoring of assets becomes a recurring theme. Whether it's meeting guidance provided by Industry standards organizations or looking to stay proactive in the ever-present and ongoing struggle of maintaining a "patched" network. While in most cases this aspect would deal with updates, hotfixes, quick fix engineering patches, etc… the standardization of system settings and configurations also must be taken into consideration as a part of an overall management and monitoring solution. The ability to determine whether systems on the network are compliant with corporate determined standardized settings and configuration assists in providing an overall picture as to the state of health of the network itself. While there are a variety of tools available on the market, we will be reviewing the Compliance Settings features and capabilities within the System Center 2012 Configuration Manager technology by Microsoft. Before providing an example on how this technology works, we must first need to understand what compliance is and its importance in a network environment.

What is Compliance?

As provided by the Merriam-Webster website, the definition of compliance is **"*the act or process of doing what you have been asked or ordered to do*"**. [1] While this provides the definition in broad terms, when it comes to compliance within the realm of computer systems; compliance is determining whether devices are configured in a manner such that the correct operating system version, required applications, or optional applications are installed and configured appropriately, as well as whether prohibited applications are installed on systems. [2][12][13] Compliance of systems might also include determining various registry settings, software updates installed, and security settings in accordance with corporate policies or

directives. Next we will look at why compliance is an important achievement to strive for in a network environment.

Why is Compliance Important?

Compliance of a system's configuration and settings are important for several reasons in a network environment. First, an organization having documentation on compliant settings and configurations provides a standard baseline across these systems. Utilizing this standard should alleviate configuration "drift" – where settings are changed on systems based on troubleshooting, fix actions that change configurations, and hotfix installations - from what the standard is.[12] Second, when systems are compliant with a standard configuration and settings, the likelihood for a vulnerability to be exploited will be minimized. Last, it provides a foundation for which discussions on how, when, and what configurations are changed going forward. This would be accomplished through the use of a Change Control Board in being able to determine what the current configuration and settings for compliance is and what the impact is in the implementation of a change would be to this baseline.

How Does the Compliance and Settings Feature Work?

System Center 2012 Configuration Manager is a Microsoft technology that provides the ability to manage devices, deploy software and operating systems, as well as inventory both hardware and software information of assets on the network. Compliance Settings is the new name of the feature within System Center 2012 Configuration Manager that provides the ability to create, assess, remediate, and report whether a system is compliant with pre-determined configurations and settings. Prior to the 2012 version release, this was referred to as Desired Configuration Management (DCM).[8][11][12][13] In order to gain a better understanding of the Compliance Settings feature and how it accomplishes these actions we will need to first dissect

the various pieces that makes up this feature. However, before beginning this dissection, we will need to have an overview understanding of the System Center Configuration Manager technology. Afterwards, I will provide an example of the Compliance and Settings process with screenshots.

System Center Configuration Manager.

System Center Configuration Manager is a server-client product that is currently on version release 5 or more commonly known as "2012". In providing a brief history of the product; the initial release was named Systems Management Server (SMS) for the first 3 versions (1.0, 2.0, and 2003), the version 4 release (2007) was when the name changed to Configuration Manager (ConfigMgr), and version 5 is the most recent release of the product. "A member of the Microsoft System Center suite of management solutions, System Center 2012 Configuration Manager increases IT productivity and efficiency by reducing manual tasks and letting you focus on high-value projects, maximize hardware and software investments, and empower end-user productivity by providing the right software at the right time. Configuration Manager helps you deliver more effective IT services by enabling secure and scalable software deployment, compliance settings management, and comprehensive asset management of servers, desktops, laptops, and mobile devices." [3]

Server-Side Roles and Client Component.

While there are various roles available for use with the product, most of them are outside the scope and the intent of this paper. There are three server-side roles and one client-side component that are specific to the ability of Compliance and Settings to function. The three server-side roles are the Site Server, Management Point, and Reporting Services Point. The system with the Site Server role is "a computer from which you run Configuration Manager

Setup and that provides the core functionality for the site" [4]. The main thing to understand about this role is this is where all of the configurations for the site and client systems occurs accomplished by the ConfigMgr Administrators on this server through a management console. The system with the Management Point role is "a site system role that provides policy and service location information to clients and receives configuration data from clients" [4]. In relation to Compliance and Settings, this role provides the policy data to the client system as to whether it's a targeted system to run the Baselines and Configuration Items as well as the system that the client results are sent to for processing by the Site Server for reporting purposes.

The Reporting Services Point role is "a site system role that integrates with SQL Server Reporting Services to create and manage reports for Configuration Manager".[4][6] This provides the enterprise-wide view as to the state of systems with relation to whether clients are compliant or non-compliant with the Baselines and Configuration Items deployed in the environment.

Similar to the server-side roles available for use in ConfigMgr, there are a number of client components that can be enabled and utilized in environment. The Compliance Settings component must be enabled within the management console in order for client systems to download the Baseline and Configuration Item policies, run them for assessment, and report their state of compliance or non-compliance. [6] The client system can also be referred to as a targeted system, which will be discussed next.

Targeted Systems.

Before we get into the Compliance Settings specific components, we need to discuss how the compliance settings are targeted to systems in the environment. Within System Center 2012 Configuration Manager there is an object referred to as a Collection. Within this Collection can

be user or device objects; however, the main concept to know is that a Collection is a group of users or devices that have some common trait. [12][13] For example, a Collection of "All Windows 8 Workstations" would have a query that annotates all systems in the System Center 2012 Configuration Manager database with an Operating System Caption of "Windows 8 Workstation" within the various systems hardware inventory table would become a member of this Collection. The members of this Collection would then be targeted systems eligible for Compliance Settings checks by Configuration Items and Baselines.

Configuration Items.

The core piece of the Compliance Settings feature is the Configuration Item. There are four main Configuration Item types [2]:

Configuration Item Type	Definition
Application	Used to check and determine an application's settings for compliance.
Operating System	Used to check and determine a particular Operating System's version or settings for compliance.
Software Update	Used to check and determine Configuration Manager clients for Software Update compliance.
General	Used to check and determine settings of objects that do not fall under any of the other categories listed above.

Table 1 Configuration Item Types.

Within the General Configuration Item type, there are a variety of Configuration Item setting types available for use [14]:

Configuration Item Setting Type	
Active Directory query	**LDAP prefix** - Specify a valid prefix to the Active Directory Domain Services query to assess compliance on client computers. You can use either LDAP:// for a or GC:// to perform a global catalog search.. **Distinguished Name (DN)** - Specify the distinguished name of the Active Directory Domain Services object that is assessed for compliance on client computers. **Search filter** - Specify an optional LDAP filter to refine the results from the Active Directory Domain Services query to assess compliance on client computers.

	Property - Specify the property of the Active Directory Domain Services object that is used to assess compliance on client computers. **Query** - Displays the query constructed from the entries in **LDAP prefix**, **Distinguished name (DN)**, **Search Filter** (if specified), and **Property**, which are used to assess compliance on client computers.
Assembly	**Assembly name**: Specifies the name of the assembly object that you want to search for. The name cannot be the same as other assembly objects of the same type and must be registered in the Global Assembly Cache. The assembly name can be up to 256 characters long.
File System	**Type** – In the list, select whether you want to search for a File or a Folder. **Path** - Specify the path of the specified file or folder on client computers. You can specify system environment variables and the %USERPROFILE% environment variable in the path. **File or folder name** - Specify the name of the file or folder object to search for. You can specify system environment variables and the *%USERPROFILE%* environment variable in the file or folder name. You can also use the wildcards * and ? in the file name. **Include subfolders** – Enable this option if you also want to search any subfolders under the specified path. **This file or folder is associated with a 64-bit application** - Choose whether the 64-bit system file location (*%windir%*\System32) should be searched in addition to the 32-bit system file location (*%windir%*\Syswow64) on Configuration Manager clients running a 64-bit version of Windows.
IIS Metabase	**Metabase path** - Specify a valid path to the Internet Information Services (IIS) Metabase. **Property ID** - Specify the numeric property of the IIS Metabase setting.
Registry Value	**Hive** - In the list, select the registry hive that you want to search in. **Key** - Specify the registry key name that you want to search for. Use the format key\subkey. **Value** – Specify the value that must be contained within the specified registry key. **This registry key is associated with a 64-bit application** - Specifies whether the 64-bit registry keys should be searched in addition to the 32-bit registry keys on clients that are running a 64-bit version of Windows.
Script	**Discovery script** – Can use Windows PowerShell, VBScript, or Microsoft JScript scripts.

SQL query	**SQL Server instance** – Choose whether you want the SQL query to run on the default instance, all instances, or a specified database instance name. **Database** - Specify the name of the Microsoft SQL Server database against which you want to run the SQL query. **Column** - Specify the column name returned by the Transact-SQL statement that is used to assess the compliance of the global condition. **Transact-SQL statement** – Specify the full SQL query you want to use for the global condition. You can also click Open to open an existing SQL query.
WQL query	**Namespace** - Specify the Windows Management Instrumentation (WMI) namespace which is used to build a WQL query that is assessed for compliance on client computers. The default value is Root\cimv2. **Class** - Specifies the WMI class which is used to build a WQL query that is assessed for compliance on client computers. **Property** - Specifies the WMI property which is used to build a WQL query that is assessed for compliance on client computers. "WMI provides a uniform interface for any local or remote applications or scripts that obtain management data from a computer system, a network or an enterprise". [5]
XPath	**Path** - Specify the path of the .xml file on client computers that is used to assess compliance. Configuration Manager supports the use of all Windows system environment variables and the *%USERPROFILE%* user variable in the path name. **XML file name** - Specify the file name containing the XML query that is used to assess compliance on client computers. **XPath query** - Specify a valid full XML path language (XPath) query that is used to assess compliance on client computers. **Namespaces** - Opens the **XML Namespaces** dialog box to identify namespaces and prefixes to be used during the XPath query.

Table 2. Configuration Item – Setting Types

Depending on the above setting type and what an organization or Industry Standard determines as important in maintaining a standardized system in their environment, the Configuration Item contains the rules associated as to whether or not a system is compliant with the setting. Once the Configuration Item(s) have been defined they will be linked to a Baseline for deployment to a target collection of systems to determine compliance with the Configuration Items. [11][12][13]

Baselines.

A Baseline is the piece of Compliance Settings feature that contains one or many Configuration Items for assessment against the systems within the targeted collection of systems. Baselines can be used to target different collections as well as multiple Baselines can be targeted to multiple collections. For example, you could have a Windows Server Baseline with Configuration Items that are specific to the Windows Server Operating System as well as another Baseline with SQL-specific Configuration Items and target both of these Baselines to a Collection of SQL Servers. [11][12][13]

Remediation.

A new capability within System Center 2012 Configuration Manager that wasn't available in previous versions described as Remediation. Depending on the setting type used in the Configuration Item, there is a possibility of accomplishing "Remediation On-the-Fly". "Remediation is supported for WMI, registry, and script settings that are noncompliant". [2] This means that as the system is running the compliance rule against itself, if the "Remediation" checkbox is enabled on the Compliance Rule and the system determines that it's out of compliance – it can then run the remediation script or in the case of a registry value, change the registry value to what it should be based on the Compliance Rule parameters. [10] This provides a capability to lessen the window of opportunity for attackers to take advantage of misconfigured settings of systems on the network.

One item to note is that while the ability to "Remediate On-the-Fly" is a good concept, a review of enabling this feature needs to be accomplished in order to verify that the setting being changed won't cause other issues with the applications or services being provided by the non-compliant system.

Reporting.

Once a system receives policy that it is targeted by a Baseline (or multiple Baselines), the system will download the Baseline with the Configuration Items and assess the Compliance rules against itself and whether it is compliant with these settings. Based on the verbiage of the Compliance rule(s) of the Configuration Item(s), the system will then log as well as provide a local report as to the state of compliance the system is in with relation to the Configuration Items within the Baselines targeted against the system.

The system will also send this compliance state information to the System Center 2012 Configuration Manager Site Server for processing and reporting. This capability provides administrators and management with an overall view of what the compliance state of the environment is of the systems targeted by the Baselines and Configuration Items. [11][12][13]

Compliance Settings Example

The following example will be a simplification of the process to provide an overview as to how the Compliance Settings feature works. I will use a compliance rule that checks the registry key "HKEY_Local_Machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName" for a value that "contains" the words "Server 2012". The reason for the creation of this compliance rule is that I've been provided information from a colleague stating that all of the systems within my lab environment have been upgraded to a version of Server 2012 (which could be R2, Datacenter, Standard, etc…). This value isn't something that I would utilize the remediation capability of the Compliance Settings feature. Since systems that would be non-compliant with this Configuration Item would likely require having the Operating System upgraded, rather than setting the registry key value "On-the-Fly" to meet compliance and provide a false-positive.

The first step is to create a collection of targeted systems for the compliance rule to run against.

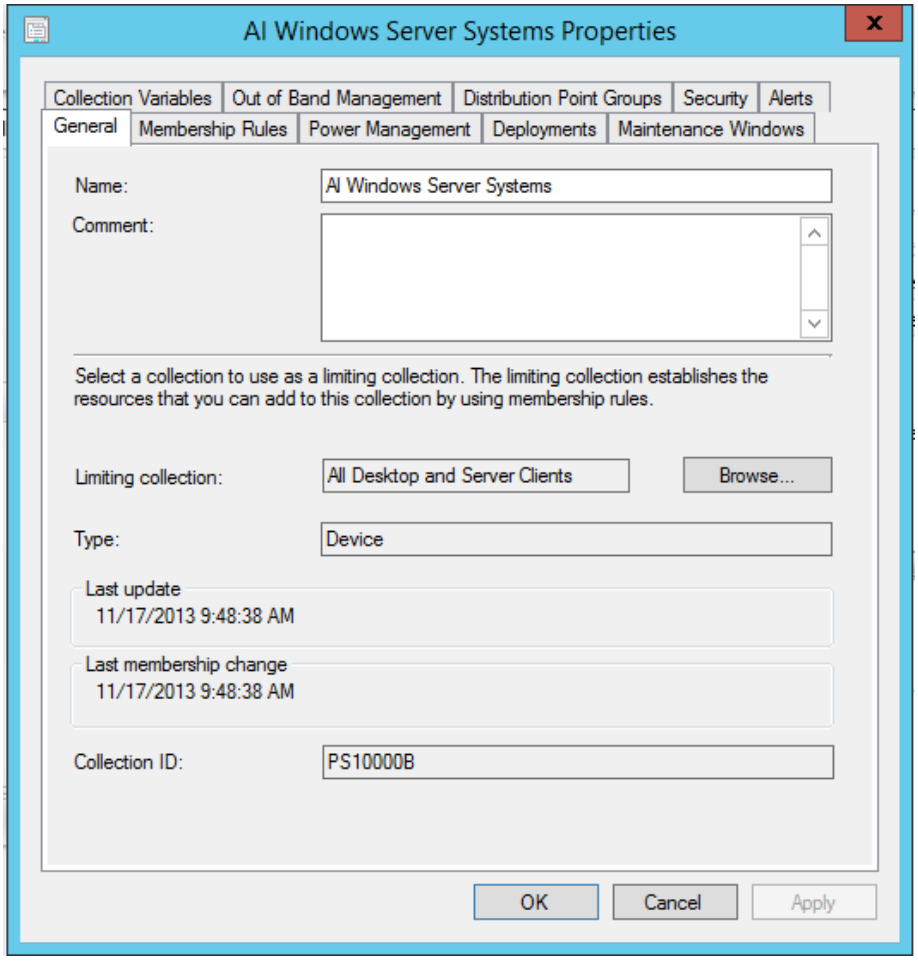

Figure 1. Collection – General Tab

For this example, we will use a collection query that uses the Operating System Caption information in the database to determine the members of the collection.

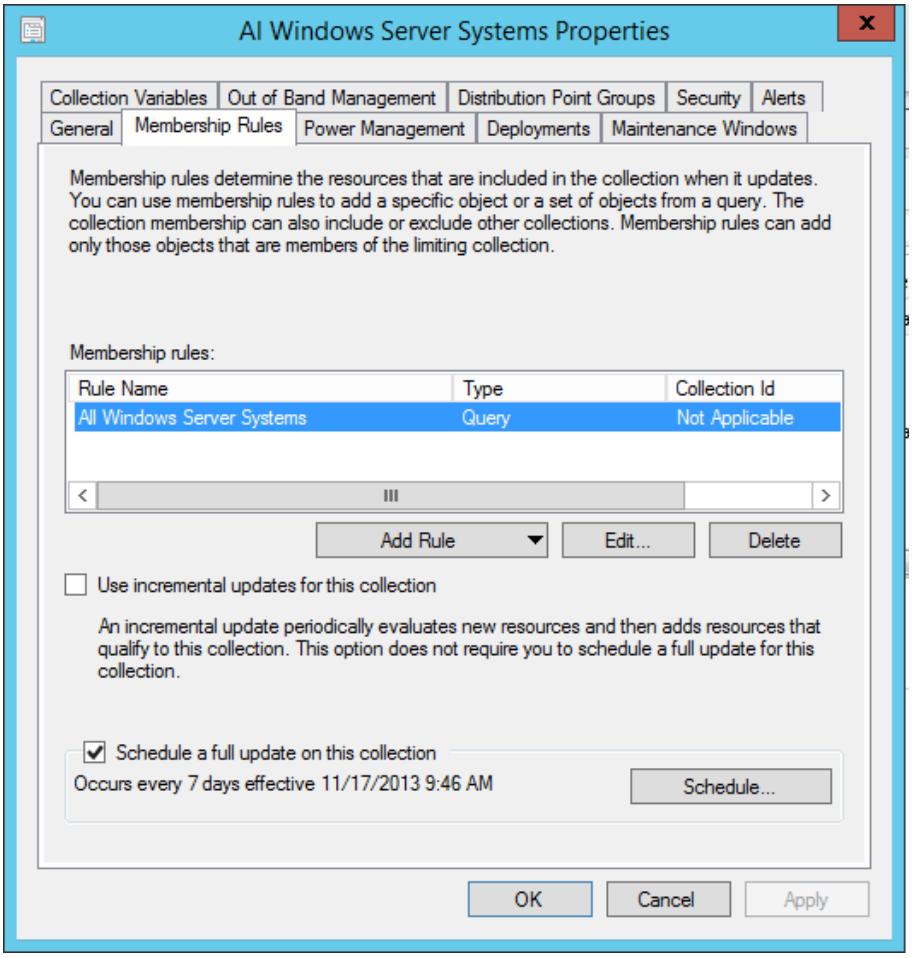

Figure 2. Collection – Membership Rules

On the Membership Rules tab we have adjusted the query to ensure that all Windows Server systems will be members. This collection utilizes a Windows Management Instrumentation (WMI) Query Language (WQL) query, which is shown below:

select

SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.

Name,SMS_R_SYSTEM.SMSUniqueIdentifier,SMS_R_SYSTEM.ResourceDomain

ORWorkgroup,SMS_R_SYSTEM.Client from SMS_R_System inner join

SMS_G_System_OPERATING_SYSTEM on

SMS_G_System_OPERATING_SYSTEM.ResourceId =

SMS_R_System.ResourceId where

SMS_G_System_OPERATING_SYSTEM.Caption like "%Server%"

The second step would be the creation of the Configuration Item within the System Center 2012 Configuration Manager console. The below series of screenshots provides the steps within the Configuration Item Wizard during the creation process.

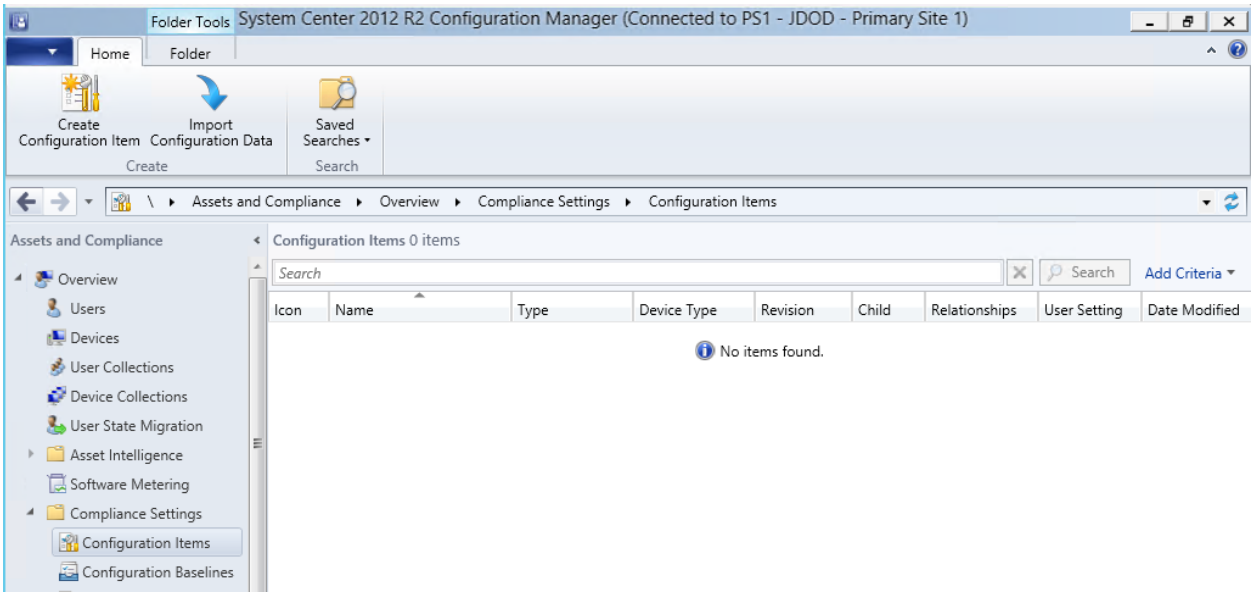

Figure 3. Compliance Settings Node

Select the “Create Configuration Item” at the Compliance Settings node within the Configuration Manager console to start the wizard.

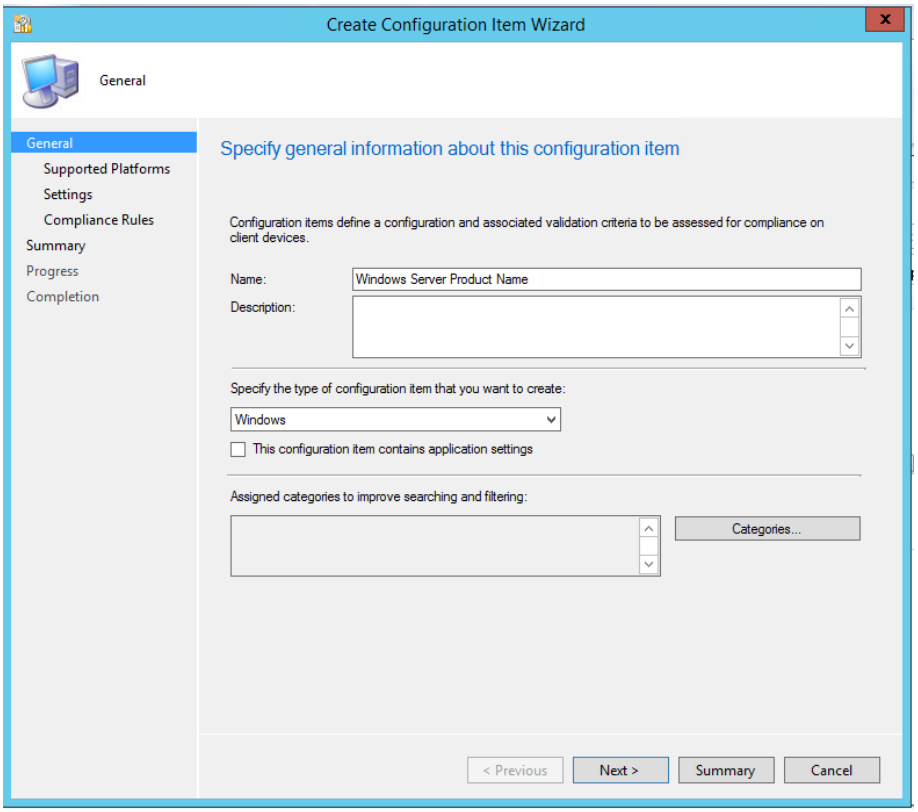

Figure 4. General Tab

This configuration tab provides details such as the Name of the Configuration Item being created. We will use “Windows Server Product Name” for this example.

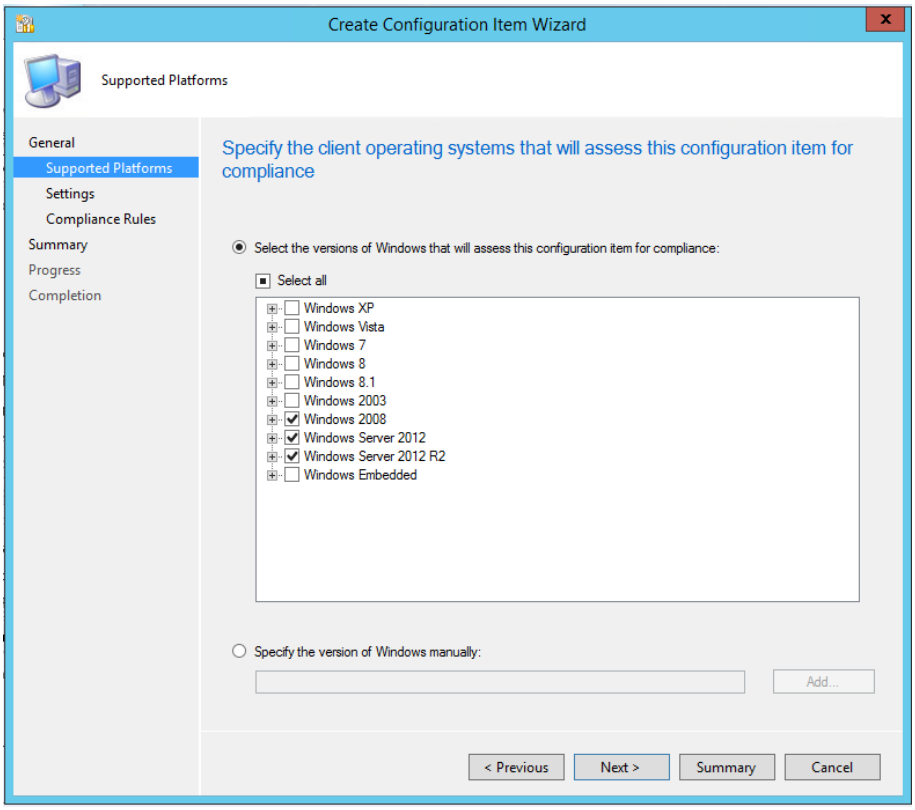

Figure 5. General Tab - Supported Platforms

This setting provides the granularity as to which platforms the Configuration Item will assess for compliance. In this example, we will be targeting Server 2003, Server 2012, and Server 2012 R2 client systems.

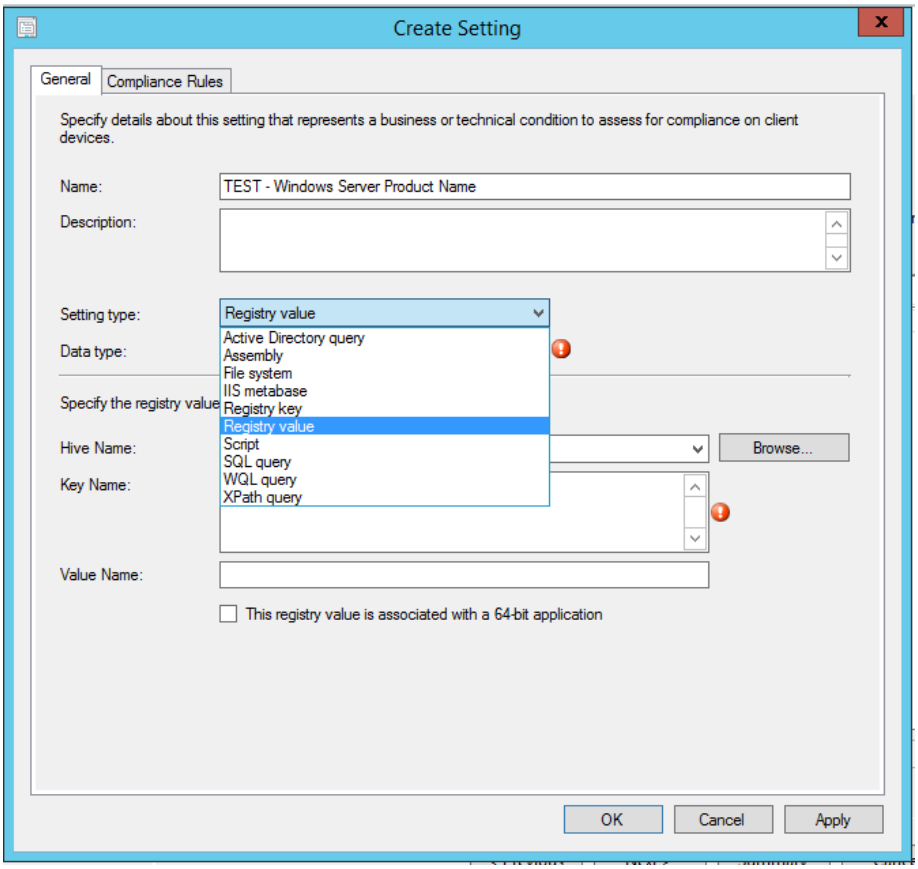

Figure 6. General Tab – Settings Type

This is the pop-up created when creating the actual setting that will be assessed for compliance. We named this Setting "TEST – Windows Server Product Name" and will be one of potentially multiple Settings that can be assessed as part of one Configuration Item. As you can see there are a variety of Setting Types available for use which were discussed earlier.

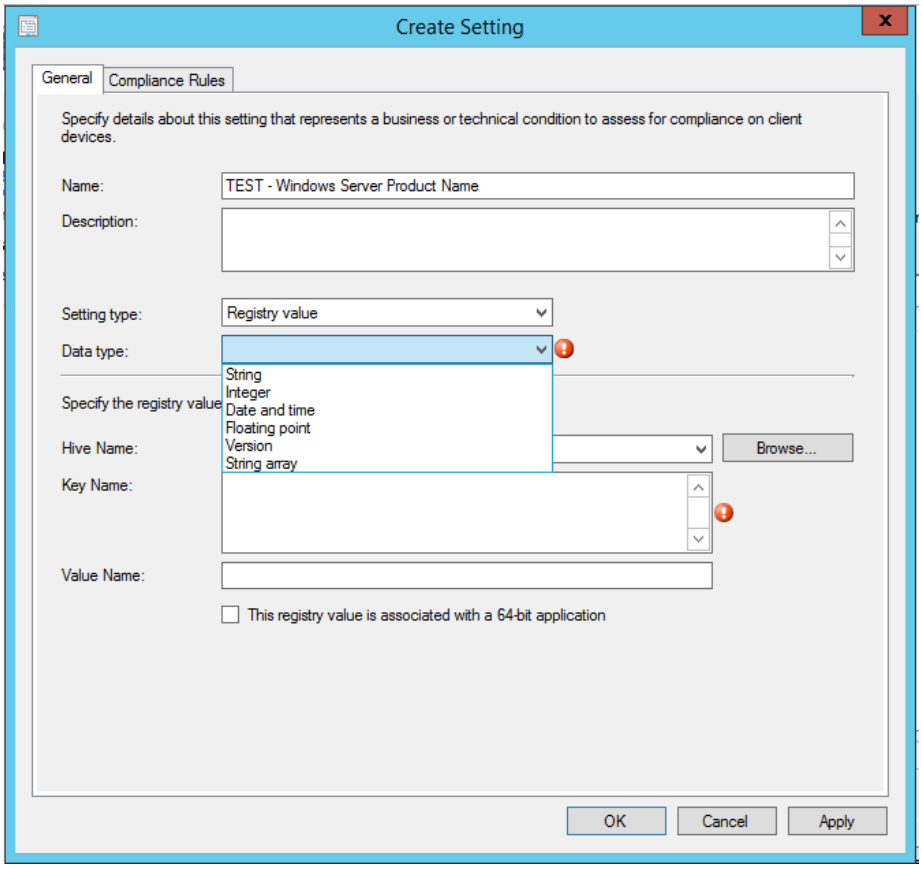

Figure 7. General Tab - Data Type

Since our example will be accomplishing a registry check, we have several Data Types to choose from specific to potential registry values available. I'm going to Browse to find the registry value for Product Name.

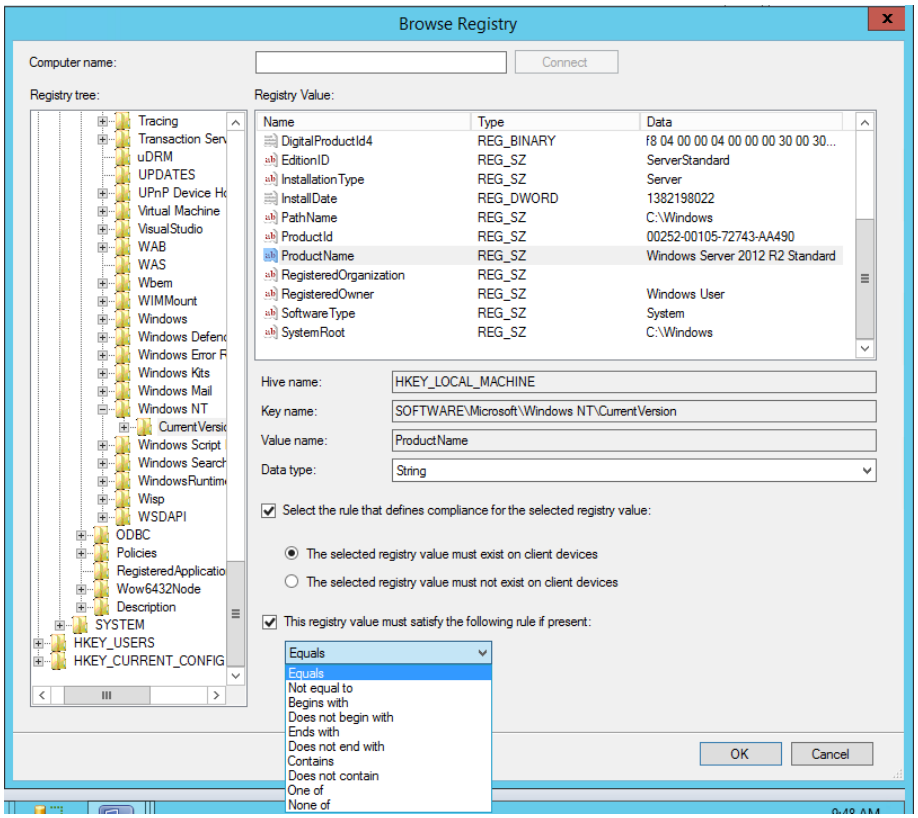

Figure 8. Compliance Rules - Browse Registry

I have the capability to either browse the registry of the system I'm on or a remote system. While I'm looking at the Product Name Value Name, I will be adjusting the operator at the bottom of the screenshot to use "Contains".

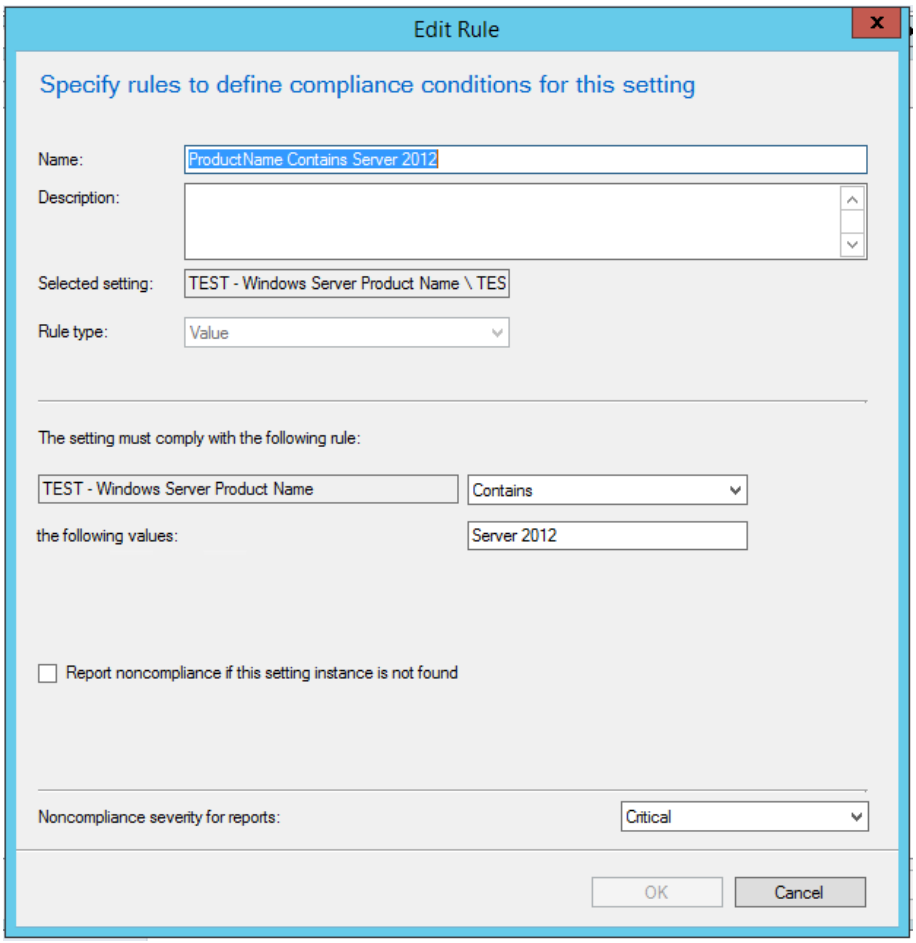

Figure 9. Compliance Rules

This is where we would look to set the value for the registry key as to what we would deem as compliant for the rule. This is referred to as the Validation Rule. In this case the value for Product Name would need to contain "Server 2012" to be compliant. This is also where we would be able to adjust the severity of the non-compliance to either None, Informational, Warning, Critical or Critical with event.

This process completes the creation of the Configuration Item for this example.

The third step would be to add the Configuration Item to a Baseline for targeting systems in a Collection.

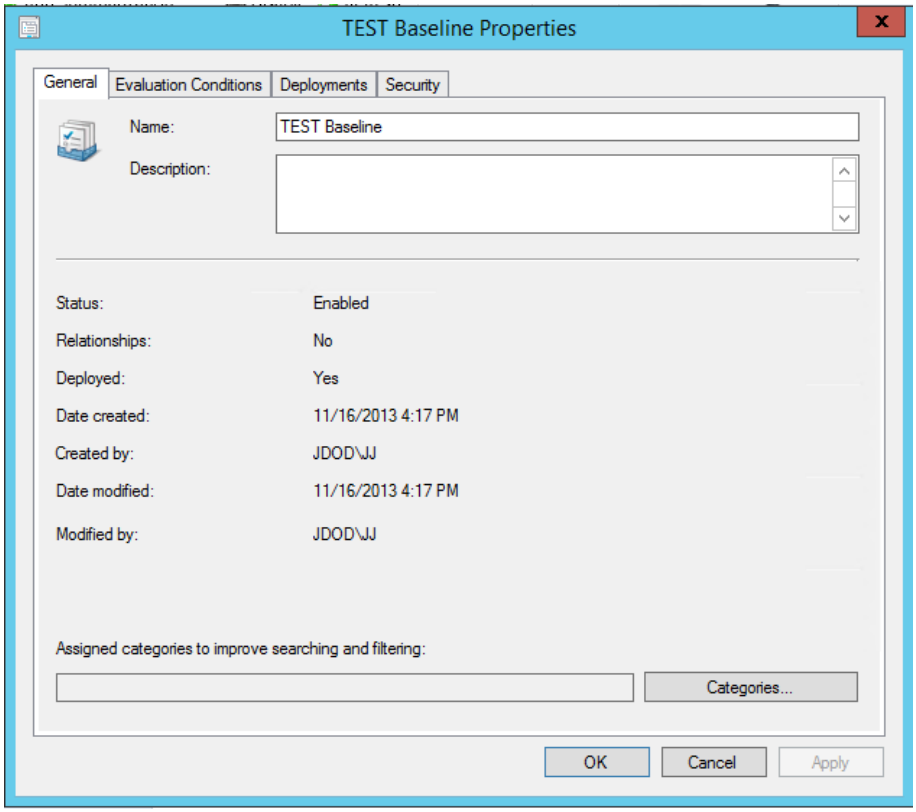

Figure 10. Baseline – General Tab

In this example we will add the Configuration Item to the "TEST – Baseline" Baseline for deployment.

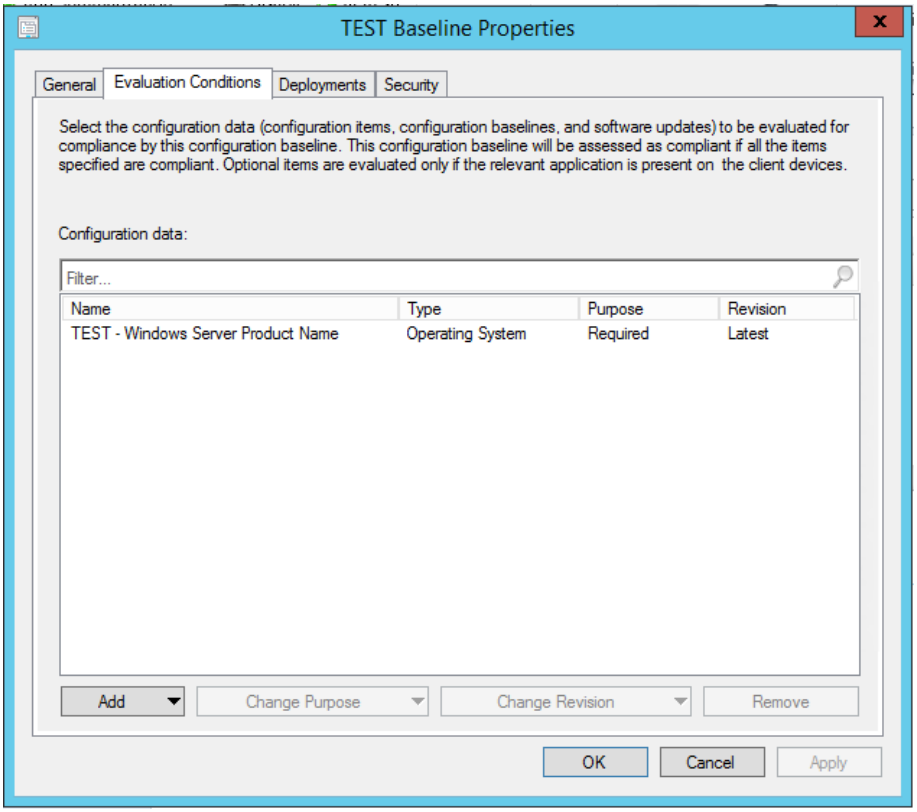

Figure 11. Baseline – Evaluation Conditions

On this tab, we will ensure that we've added the Configuration Item created earlier.

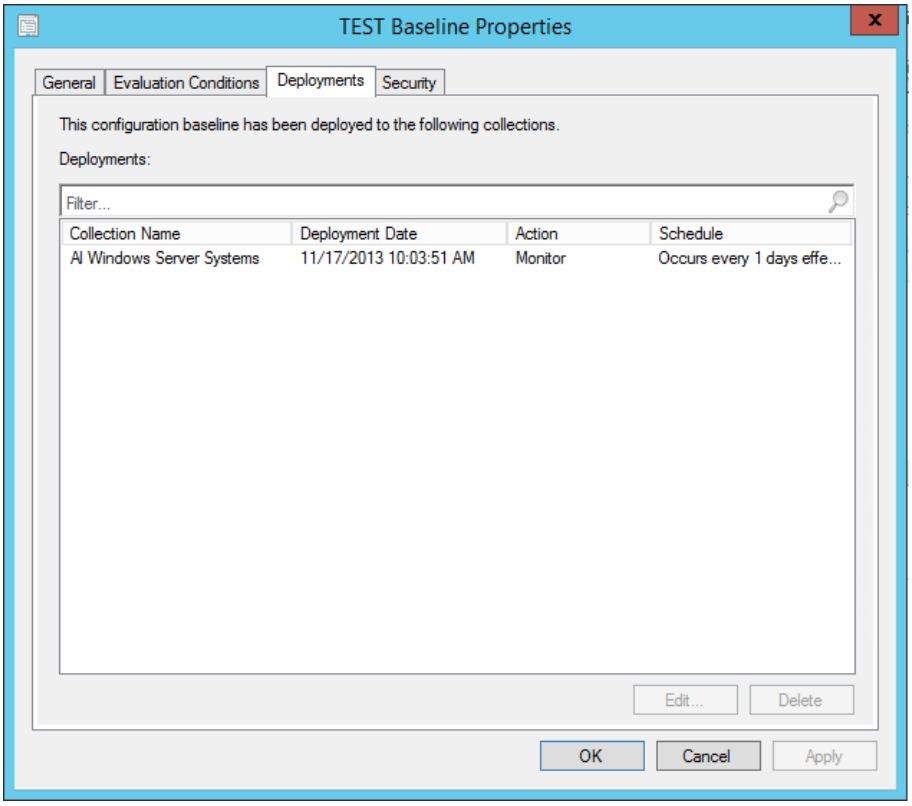

Figure 12. Baseline - Deployments

The next step would be to deploy the Baseline to a Collection (or multiple collections). For this example, we will use the "All Windows Server Systems" collection (which was created earlier) and will have the assessment evaluation occur on a daily schedule.

Once the Baseline is deployed, it is a matter of time (60 minutes, by default), that the client systems within the Collection receive policy that a new Compliance Settings Baseline is now required to be ran against the system. After the Baseline is downloaded locally to the client system and assesses the compliance rule(s) and creates a local report for review.

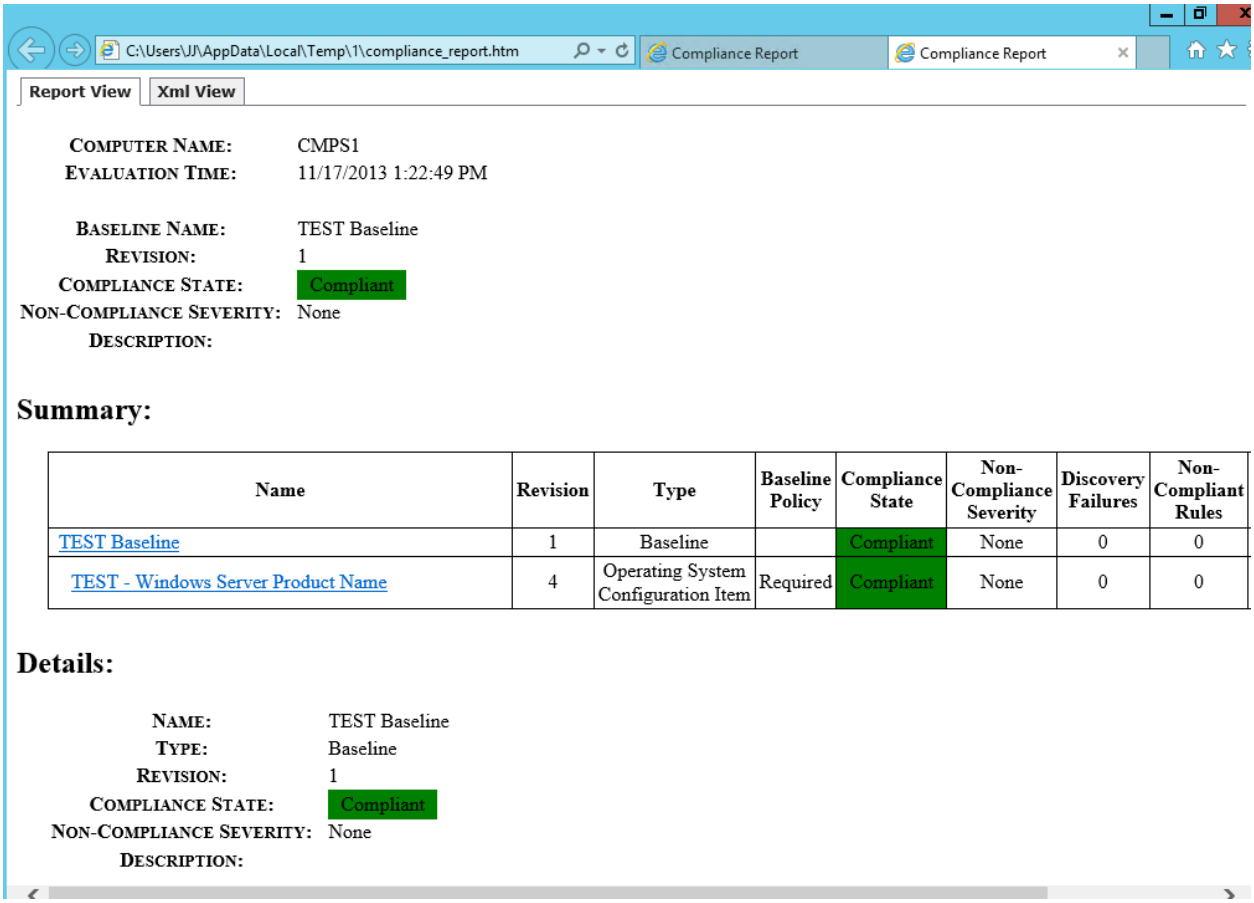

Figure 13. Local Report – Compliant

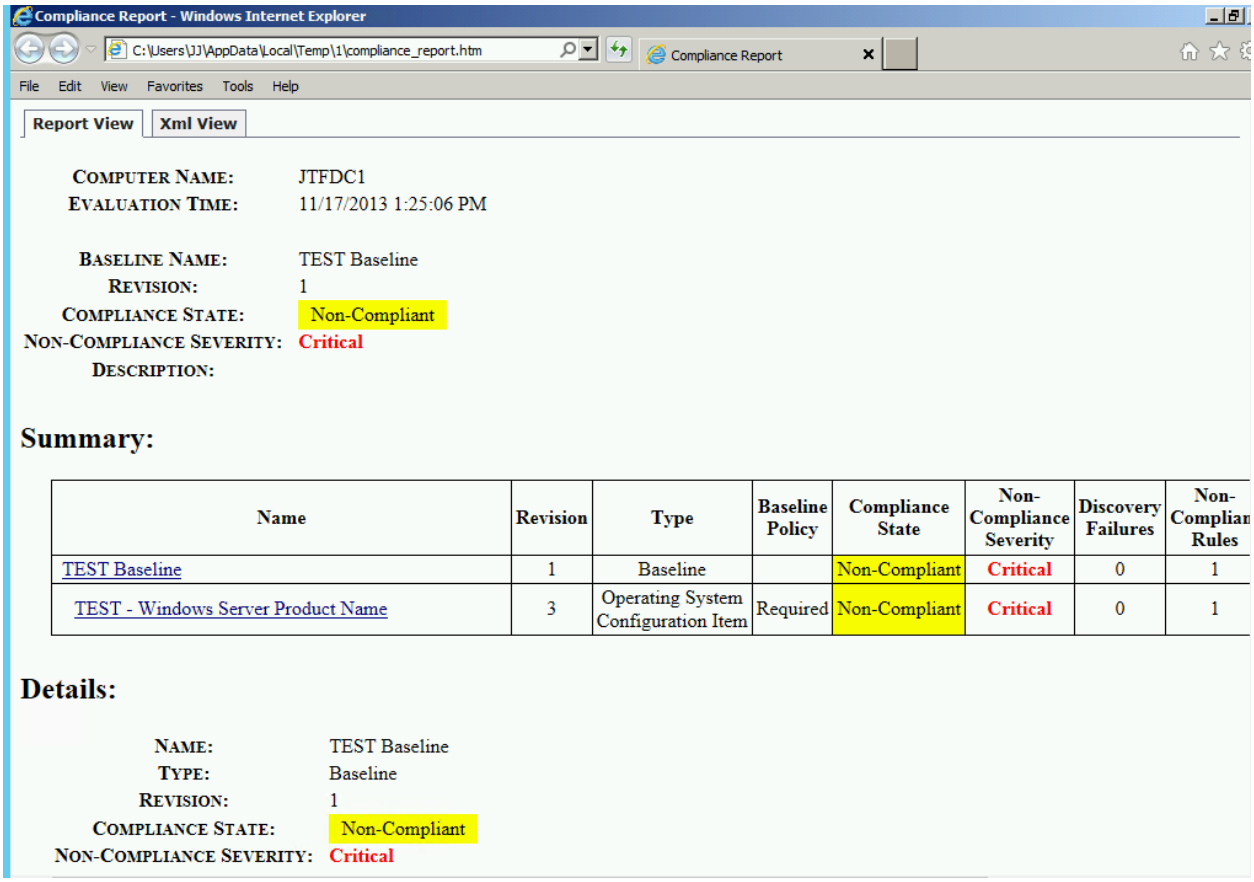

Figure 14. Local Report – Non-Compliant

At the same time that this local report is created, a state message is sent back for processing back to the System Center 2012 Configuration Manager for processing. Once this information is processed and stored in the database, it is made available for use by the Reporting feature. There are multiple "canned" Compliance and Settings reports available within the System Center 2012 Configuration Manager console which provides an overall, enterprise view of the systems that are targeted by the various Baselines that would be deployed in the environment and what their compliance state is.

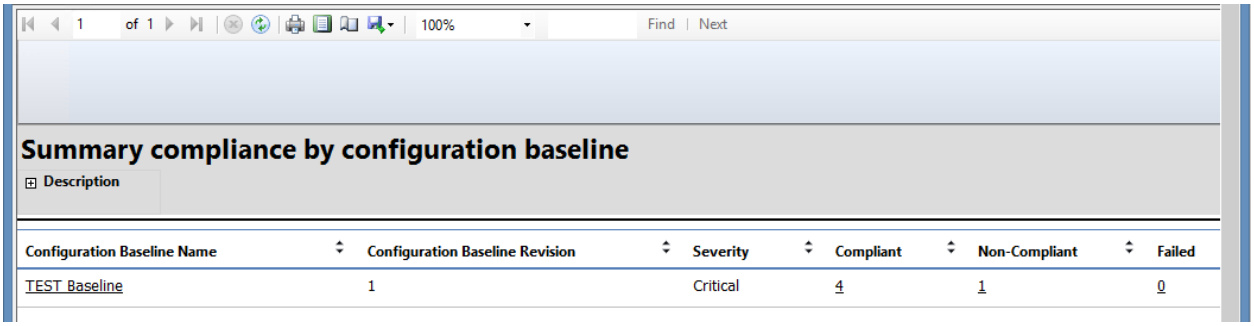

Figure 15. Overall Summary Compliance Report

As you can see, there is one system that is non-compliant with this Baseline and we can drill-down further to see the details of this system by clicking on the hyperlink associated with the "1".

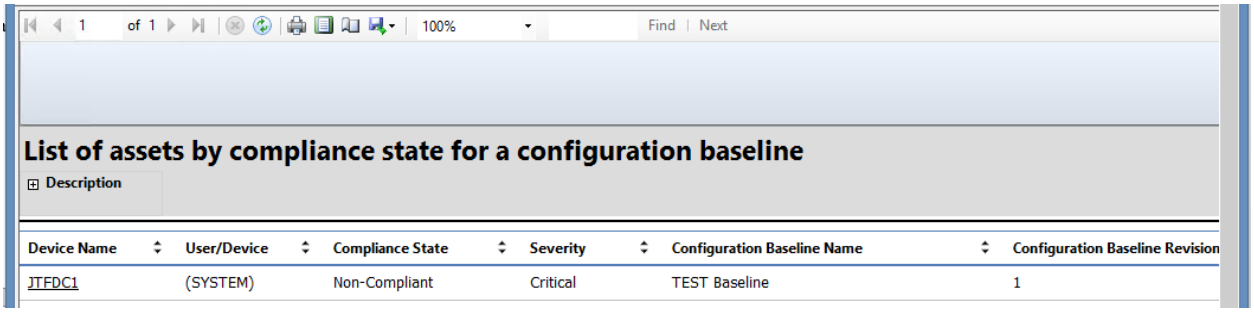

Figure 16. Non-Compliant System

The system that is non-compliant with the Baseline (as well as the Configuration Item associated with it of Product Name contains "Server 2012") is my Domain Controller for my lab environment. It is actually a Server 2008 system, which you would be able to determine by drilling down on the hyperlink of the system name JTFDC1.

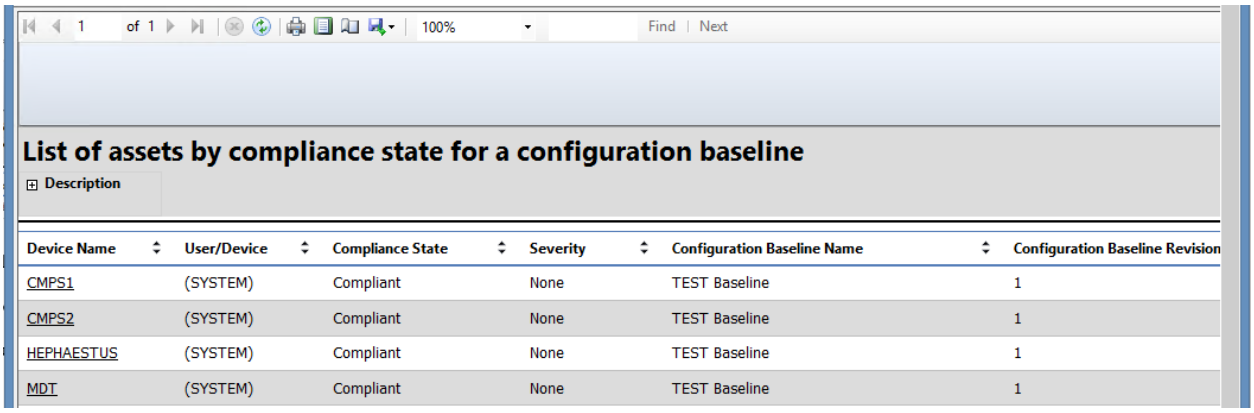

Figure 17. Compliant Systems

The list of systems above range from Server 2012 and Server 2012 R2. Since my compliance rule utilized the "Contains" operator, they are all seen as compliant since the Product Name value contains Server 2012.

I now have the capability within a report in a central location that will assist me (as an Administrator) or my management in determining how many Windows Server systems are not at the Server 2012 version on the network (or are non-compliant with the pre-determined standard). [8][9][11]

Industry Standards and Compliance Settings

While the ability to create custom, organizational-specific Configuration Items and Baselines for use, yet another benefit is having the capability to import pre-configured Configuration Items and Baselines (referred to as Configuration Packs) reduces the time and resources spent in the creation of these items for separate System Center 2012 Configuration Manager environments. "Those standards can be company policies regarding how a computer is configured, policies for compliance with regulations such as Sarbanes-Oxley (SOX), or best practices defined by a vendor or based on your internal IT department's experience"[2]. Various organizations can share what they've created themselves through the export of the Configuration

Items and Baselines into CAB files, though there is the ability to import configuration packs from a website provided by Microsoft which has numerous configuration packs available as well, ranging from HIPAA to FISMA to GBLA.[7][12][13] "This configuration data can be imported from http://pinpoint.microsoft.com in Microsoft System Center Configuration Manager configuration packs, defined as best practices by Microsoft and other vendors, defined within Configuration Manager, or defined externally and then imported into Configuration Manager"[2]. While some of the configuration packs aren't updated on a specific lifecycle and the Configuration Items that are assessed don't typically change, many of the configuration packs found on Pinpoint can still be used in System Center 2012 Configuration Manager with minimal changes or review required.[10]

Conclusion

As organizations struggle to not only ensure that systems are patched with various software updates (per Operating System, application, services, etc…), as well as determine whether systems on the network are compliant with organization-specific and Industry-specific settings, there is a real need to standardize these systems on the network. Part of this process is the determination by the organization as to what settings and configurations need to be standardized as well whether there are any Industry and regulatory requirements. Through the use of the Compliance Settings feature within System Center 2012 Configuration Manager, organizations can utilize their pre-determined standardized configurations and settings as a method to mitigate "drift" by ensuring compliance is being met on targeted systems. The example provided within this paper is a small sample of the capabilities available for use.

With the ever-changing and fast pace of vulnerabilities and exploits available to attackers against organizations, this document provides the information needed for administrators (as well

as management) to understand not only what compliance and standardization is, but also the importance these topics have as a mitigation against potential attacks. Utilizing a technology such as the Compliance Settings feature within System Center 2012 Configuration Manager, an organization will be able to proactively determine what the state of their systems are. Based on compliance assessment information provided back from the client systems, an enterprise view can be provided through the use of reports and assist in the effort to remediate the non-compliant systems. This could be through the use of the remediation "on-the-fly" capability or through other methods available through System Center 2012 Configuration Manager like Software Deployments or Software Updates, but those are topics for another time and discussion altogether.

References

[1] Compliance. (n.d.). In Merriam-Webster Online. Retrieved on November 9, 2013, from http://www.merriam-webster.com/dictionary/compliance

*[2] Rachui, S., Agerlund, K., Martinez, S., & Daalmans, P. (2012). Chapter 13 Compliance Settings. In Bennett B. (Ed.), *Mastering System Center 2012 Configuration Manager* (573-601). Indianapolis, Indiana: John Wiley, & Sons, Inc.

[3] Microsoft Corporation. (July 1, 2012). Introduction to Configuration Manager. *Microsoft TechNet*. Retrieved on November 9, 2013, from http://technet.microsoft.com/en-us/library/gg682140.aspx

[4] Microsoft Corporation. (June 1, 2013). Fundamentals of Configuration Manager. *Microsoft TechNet.* Retrieved on November 9, 2013, from http://technet.microsoft.com/en-us/library/gg682139.aspx

[5] Faldu, R., Raval, M., Linton, B., Pandey, K. (2013). Chapter 1 Introduction to WMI in Configuration Manager 2012. In Tulloch, M., (Ed.), Microsoft System Center: Configuration Manager Field Experience* (3-23). Redmond, Washington: Microsoft Press.

[6] Microsoft Corporation. (October 1, 2012). Prerequisites for Compliance Settings in Configuration Manager. *Microsoft TechNet*. Retrieved on November 10, 2013, from http://technet.microsoft.com/en-us/library/gg682073.aspx

[7] York, R. (February 13, 2010). Configuration Manager 2007 Desired Configuration Management Configuration Packs. *Microsoft TechNet Blogs*. Retrieved on November 11, 2013, from http://blogs.technet.com/b/manageabilityguys/archive/2010/02/13/configuration-manager-2007-desired-configuration-management-configuration-packs.aspx

[8] Griffin, D. (January 8, 2011). Desired Configuration Management in SCCM. *Blog at Wordpress.com*. Retrieved on November 11, 2013, from http://dbgriffin.wordpress.com/2011/01/08/microsoft-security-compliance-manager/

[9] Schloss, E. (November 27, 2012). Using DCM in SCCM 2012 to Report on BitLocker Encryption Compliance. *Blog at MyITForum.com*. Retrieved on November 12, 2013, from http://myitforum.com/myitforumwp/2012/11/27/using-dcm-in-sccm-2012-to-report-on-bitlocker-encryption-compliance/

[10] Zerger, P., (December 16, 2011). New ConfigMgr DCM packs available and thoughts on ConfigMgr vNext. *System Center Central*. Retrieved on November 14, 2013, from http://www.systemcentercentral.com/new-configmgr-dcm-packs-available-and-thoughts-on-configmgr-vnext/

[11] Desai, P., (February 14, 2013). SCCM 2012 Compliance Settings. *Blog at PrajwalDesai.com - Collection of Articles on SCCM, Lync, Exchange, and Other*

Technologies. Retrieved on November 16, 2013, from http://prajwaldesai.com/sccm-2012-compliance-settings/

*[12] Microsoft Corporation. (June 2008). Managing Data Center Server Compliance: Using Microsoft System Center (White Paper). Retrieved on November 15, 2013, from http://download.microsoft.com/download/6/6/5/665fcea2-89b2-4e5d-b80e-e7ac78a4968e/SC_Managing_Data_Center_Compliance_White_Paper.pdf

*[13] Silect Software. (October 2010). Simplifying the Deployment of Microsoft System Center Desired Configuration Management (DCM) "Open me first" (White Paper). Silect Software. Retrieved on November 16, 2013, from http://www.silect.com/sites/default/files/doc-assets/DCM_Deployment_WP_Oct2010.pdf

[14] Microsoft Corporation. (January 1, 2013). How to Create Windows Configuration Items for Compliance Settings in Configuration Manager. *Microsoft TechNet.* Retrieved on November 16, 2013, from http://technet.microsoft.com/en-us/library/gg712331.aspx

Key Terms

CI – Configuration Item

DCM – Desired Configuration Management

FISMA – Federal Information Security Management Act

GBLA – Gramm-Leach, Bliley Act

HIPAA – Health Insurance Portability and Accountability Act

SOX – Sarbanes - Oxley

SCCM or ConfigMgr – System Center Configuration Manager

SQL – Standard Query Language

WMI – Windows Management Instrumentation

WQL – Windows Query Language

XPath – XML Path Language