Chapter No. 1
"Planning for High Availability with Configuration Manager"
In this package, you will find:

A Biography of the author of the book

A preview chapter from the book, Chapter NO.1 "Planning for High Availability with Configuration Manager"

A synopsis of the book’s content

Information on where to buy this book

About the Author

Marius Sandbu is a Consultant, Advisor, and Trainer working at the VAD (Value Added Distributor) Commaxx in Norway. He has worked with Microsoft technology for over 8 years and has recently been awarded with a MVP title from Microsoft because of his high dedication to the Microsoft community. He is also a board member of the local Microsoft technology user group and spoken at many public events at both Microsoft and other events.

Marius has always had a high interest in technology, over the past few years he has taken over 20 certifications on different areas and technology, and also had a role within Microsoft as a V-TSP. He is also a certified Microsoft trainer and has held different courses, within System Center and Windows Server.

For More Information:

As an experiment to improve his learning skills, he started blogging in 2012 and now has over 2000 visitors to date. He also contributes to Born To Learn which is a Microsoft community website for training and certification.

I thank my lovely other half, Silje, for supporting and having patience with me, this is what made the book possible! Wouldn't be possible without you!

I also thank the people at Packt Publishing for a clean and efficient process with the book writing. It was a good experience and I've learned a lot during the process.

**For More Information:**
Microsoft System Center Configuration Manager High availability and performance tuning

Microsoft System Center Configuration Manager is a book that covers all of the aspects from planning to deploying a redundant Configuration Manager environment.

What This Book Covers

Chapter 1, Planning for High Availability with Configuration Manager, covers what you need to plan for when you want to set up High Availability for your site. For instance, it shows how to plan a layout for SQL Server, what kind of networking technology to use, and so on.

Chapter 2, Configuring Roles for High Availability, covers how you can deploy the different Configuration Manager roles that are highly available. For instance, it shows how we can deploy the application catalog service redundantly and the different forms of distribution points, and how they can affect the performance on our site.

Chapter 3, Deploy Highly Available Backend Services, covers how you can deploy backend services, such as DNS and AD that are highly available and how they operate together. It will also cover services such as SQL and using a redundant PKI solution.

Chapter 4, Backup and Recovery, covers what you need to take into account and how you can back up and restore a Configuration Manager environment. It also covers how the content store is built up and what we can use to back it up.

Chapter 5, Performance Tuning, covers various performance tuning tips such as OS deployment, virtualized environments, and SQL deployments. This chapter will also go into different OS tuning tips such as identifying bottlenecks using different tools.

For More Information:  
Planning for High Availability with Configuration Manager

Configuration Manager can be a complex solution to grasp, as it can span from thousands to tens of thousands of different clients placed all around the globe on different platforms. And with the large number of features it contains, it also requires a well-planned infrastructure in place to serve all the different clients.

The whole concept of a system being highly available is that a service (or services) will still be available to serve the users in case of a general failure of a single component or components in the infrastructure. If a system is not Highly Available and a critical component goes offline, your service might go offline, and depending on the priority and service level agreement (SLA) of that service, this situation might be damaging for the entire business and its users.

And of course you always want to plan ahead to make sure your solution is available at all times to serve your users. We will begin by going through the various components that makes up a Configuration Manager site and how they work to serve the clients.

In this chapter we will be covering the following topics:

- Planning for High Availability
- Different roles and components within Configuration Manager
- Planning for database configuration
- Network usage Configuration Manager
- What’s new with Service Pack 1

For More Information:
Planning

When planning for High Availability you need to look at every aspect of your infrastructure; spanning from the underlying hardware to the software running on top of the different servers that serve the clients.

Some general points that can be highlighted when setting up a design and that need to be taken into account are as follows:

• Is my network adequately built for redundancy and will it be able to service all the different clients with the large amount of incoming data?
• Do I have enough storage to store my data and what will happen in case of a disk failure?
• Do my servers have enough compute performance to serve the number of clients available, or do I need to roll out more servers or invest in more hardware?
• Is my database solution scaled to handle the data flow? What happens if one of the database servers fails?
• What will happen if one of the servers in the site suffers a hardware failure?
• What happens if any other critical component in our infrastructure fails?

All these questions need to be taken into account and looked over, and taken into the planning phase. We always need to look over a design and think is there any single point of failure with this design? Because, it does not matter if we set up a massive and redundant SQL cluster in every way and we put the cluster on the same network switch. Because, then we know that if that particular switch goes down, the cluster goes down.

For More Information:
Coming back to Configuration Manager let us take a look at a simple site design for Configuration Manager and how it might look:

With a simple design shown in the previous diagram we have the general feature set for Configuration Manager available to our clients. All our Configuration Manager Clients will contact the Management point for policies, advertisements and reporting of data, and so on. The Management point in return will populate the site database with information received from the clients.

When the clients need to download a source file from an advertised deployment or for an operating system deployment it will contact the Distribution point within the site. For this site the data is stored in a single database server, which is collocated with the Primary Site Server. This design also includes a Software Update Point role as well as Endpoint Protection Role for the management of endpoint protection and patch management.

Let us look into problems with this type of design. For instance, let us see what would happen if the Management point server in the site stops functioning:

1. The clients will try to contact the Management point to get info about policy updates or report in data.
2. Since the Management point is unavailable, the clients will look at the list of available Management points in the site to see if there are any others available.

For More Information:
3. Since this site contains only one Management point, it will stop sending data back to the site and will start to cache the data locally and run using the last known configuration.

4. The clients will do so until the Management point is back online.

Let us see what would happen if we had two Management points in the site we just saw.

The clients would try to contact its first Management point; if it is offline it would look at its list of available Management points and try to contact the other one. This way we would have maintained site functionality for the clients. This gives us a Highly Available Management point solution for the clients, but this is only one of the components that need to be taken into account.

If the database stops working or suffers from a faulty hard drive at the server site, it would reflect outcomes that appear in the upcoming sections. As I mentioned earlier, clients will cache data locally until the site server is restored, but historical data will be lost. For instance, software metering information can be used for reporting licensing usage.

These were just a few examples of what might go wrong with this design. It is important to stay ahead when planning. There are also other components besides the ones we just covered in my example that need to be taken into account and they will be covered later in the book.

Networking

Does my core network have redundant paths to my switches? So in case a switch goes offline my servers are still available on network. Same goes for NIC teaming on the physical hosts.

Hardware

A solution such as RAID allows redundancy in case of a disk failure on physical servers, and depending on the RAID level, it might boost the server’s performance. If you are unaware of what RAID does, we will go through this in greater detail later in the chapter.
Database server
Configuration Manager is highly dependent on a Microsoft SQL Server to store site data and client data. Microsoft has many built-in solutions for High Availability and they will be covered in a later chapter.

Virtualization hosts
Depending on where you want (either physical or virtual) to deploy Configuration Manager, you need to make sure that you have a Highly Available virtualization solution on the underlying hosts.

Other Configuration Manager roles
There are multiple roles in Configuration Manager that can be deployed as Highly Available, which are mandatory for most of the features (I will come back on this subject in a later chapter).

Backup
In case there are roles that cannot be set as highly available, what options do we have to back up the data and the role information, and how can we restore the service it offers to the users as quickly as possible?

Other components
Configuration Manager is highly dependent on other components such as DNS and Active Directory, and also Active Directory Certificate Services and DHCP. Are there any High Availability options for them? I will cover this topic more in detail in a later chapter.

But many of these roles are not a part of the design phase for a Configuration Manager solution, and in most cases are already set-up redundant. Further on in the upcoming chapters we will discuss how we can deploy each role and back-end services like Microsoft SQL Server using High Availability and load-balancing features, SQL Server. It is important to note that there are no services in Configuration Manager that happen in real time and that no clients require continuous communication with any of the site roles.

Configuration Manager always works on a predefined schedule for each operation; therefore you must expect some latency even if you set up High Availability for your sites.

For More Information:
Before we continue, we will take a look at how Microsoft IT deployed Configuration Manager for the environment, just to give a clearer image on how a large enterprise Configuration Manager deployment might look for a business. The following diagram gives its overview design:

Microsoft IT deployed Configuration Manager 2012 for more than 250,000 systems and more than 150,000 users worldwide. Using this design and much of the logic that they use when deploying should be used in other scenarios as well as when planning.

The entire project can be found at the following site:


A point to note here is that there are only six physical servers in the entire design. They are used on the site server roles, which have SQL Server installed (In this case, there is one each in the different Primary Sites and the CAS server).

At the time Microsoft IT implemented Configuration Manager, Windows Server 2012 was not available and therefore, they chose not to virtualize the database servers in this design because of the hardware requirements for CPU.

**Database planning**

All of the servers which have Microsoft SQL Server installed are set up with different forms of RAID in order to gain redundancy and performance. This is needed because all the clients report back a large amount of data to the site, depending on what features are enabled in the client policy.

For More Information:

For instance, some examples of what the clients might report back to the site and the database are as follows:

- Software inventory
- Hardware inventory
- Software metering
- Baselines and configuration items

And depending on the information and the schedule this might result in a large amount of data.

But let us delve into the different forms of RAID and how it can give us better performance and redundancy for our database server. The whole purpose of RAID is to group together physical disks into a group and then form virtual disks on top to gain performance and redundancy. Now, there are different levels of RAID that we can setup.

RAID 1 is a solution based on two disks where data is mirrored on both disks (so in case of a disk failure the service will continue to run on the other disk) when you replace the faulty disk the RAID controller will rebuild the data on the new disk until both disks have the same content again. This type of RAID will in theory give us 2x the read performance since the data is available on both disk, but this is very dependent on having an adequate RAID controller.

RAID 5 is a solution based on minimum three disks and it uses parity bits on each disk. Here data is split up in different chunks where two of the disks contains the data and the third disk contains the summary of the data on the other disks (known as a parity bit) For instance, if disk one contains the data bit, 1, and disk two contains the data bit, 1, then the parity disk would contain the data, 2. Since, it will always contain the sum of the different data from the other disks. If disk 1 should fail, it would take the parity and extract the data on disk 2, which will add up to 2 - 1 = 1. So it knows that the bits that are missing on the faulty disk is 1. Depending on the data the parity might be on different disks, so we do not use a dedicated disk for parity.

RAID 1+0 (or 10) is a combination of RAID levels 1 and 0 which does mirroring and splitting the data. All disks are members of two groups, where one group does the mirroring and the other group is for splitting the data. This can, in theory, give us 4x read and 2x write performance gain and redundancy in case of a disk failure and depending on the disks that fails, it can allow for two disks to fail.

For More Information:
If you are unable to use RAID there is an alternative within Windows Server 2012, called Storage Spaces. This feature is set to be supported in SQL Server 2014. Support for SQL Server 2014 will come with Configuration Manager 2012 R2.

When Microsoft IT set up the CAS SQL Server, they used different levels of RAID depending on the purpose of the volume.

So let us take a better look on Microsoft setup and the layout of their database server. To explain in detail how Microsoft set up their database servers, have a look at the following volumes:

- **Volume C:\**: This contains the OS setup with RAID 1)
- **Volume H:\**: This contains the SQL Databases setup with RAID 1+0)
- **Volume D:\**: This contains the SQL Database logs setup with RAID 1+0)
- **Volume E:\**: This contains the backups setup with RAID 5)
- **Volume T:\**: This contains SQL Database TempDB, which is setup with RAID 5)
- **Volume I:\**: This contains the Configuration Manager files and is setup with RAID 1+0
- **Volume F:\**: This contains the page file and the WSUS updates that is setup with RAID 1

Some factors that are worth taking note are that they split the database setup so that they place the transaction logs on one volume, TempDB on one, and the regular databases on another one. With this type of setup you get better performance on the database service because of the way the different components and SQL work.

The TempDB database is responsible for storing all the temporary tables, temporary stored procedures, and internal objects created by the database engine. So any procedure in Configuration Manager that you use to create a temporary table will be stored in the TempDB.

The transaction logs store all the data transactions and database modifications. After these transactions are stored they are truncated to the database. These logs files will grow in size until a full backup has been done. This requires a lot of write activity and by placing them on a RAID 1+0 solution, we will have adequate performance.

It is also a best practice to store the swap file on a disk other than the regular OS disk. This will also boost our performance, since the swap file does not need to share IO with the regular system services. The other SQL Server on the primary sites are set up in an equal way as the CAS SQL to ensure that performance is not an issue for the large amounts of data.

For More Information:

It is important to note that you do not need to split up your database servers like this unless you require the extra performance and redundancy. But this type of deployment is according to best practice and should be used when possible, since Configuration Manager relies heavily on its database server.

We can also see in the design that Microsoft IT decided to use Secondary Sites in some of their regions. This is mostly because of the geographical gap between different countries. With Secondary Sites you can control the flow of data going back and forth between the sites.

Since secondary sites install a Management point and a Distribution point automatically, clients have what they need to get policy updates and content. As we can see from the site design, Microsoft uses a simple design for their solution. To sum up, following bullet points show how they deploy their service:

- Use CAS on the top of the hierarchy because of the large amount of clients, less than 400,000 clients
- Microsoft split up large geographical regions (Europe, Asia, and so on) as their own Primary sites
- Use secondary sites within primary sites to control the flow of data
- Multiple instances of each role within each site are used to have multiple instances available to the clients

Now, let's take a look into the different roles within Configuration Manager and see what kind of features they give and what they support. This will give you a better understanding on how you should scale and where you should use the different roles and components.

**Central Administration site**

Central Administrator site is the role that sits on top of the hierarchy (It is not mandatory but if you need more than one primary site you need this role to manage the different subprimary sites).

The features it contains are as follows:

- It can be installed along with the database server
- It cannot have any clients directly assigned to it
- It does processing of data from all the other primary sites in the hierarchy
- It can manage all the clients in the hierarchy
- It supports only Primary Sites as child sites

For More Information:

This site does not support all the different roles. For instance, it does support Endpoint Protection, Asset Intelligence, Reporting Services, Software Update point, Intune Connector, and System Health Validator point and some of these roles should be placed in top of the hierarchy.

This site supports the following:

- It can support up to 25 child primary sites
- When using SQL Datacenter or Enterprise it support up to 400,000 clients
- When using SQL Standard it supports up to 50,000 clients

Before Service Pack 1, you would need to install CAS first when you were going to set up your hierarchy with multiple primary sites. This has changed after Service Pack 1. You can now add CAS to an existing Primary Site to extend your hierarchy.

**Primary sites**

It is the most commonly-deployed site method and is a mandatory role when deploying Configuration Manager.

Now a primary site can have the following features:

- It can be standalone or part of a hierarchy either with a CAS and other Primary site or a Primary with subsecondary sites
- It is responsible for processing all data from its assigned clients
- It uses database replication to communicate with its CAS
- It can be installed with the database server
- It can have clients assigned to it

The primary site has support for the following:

- It can have up to 250 Secondary sites in its hierarchy
- It can manage up to 100,000 clients
- It can manage up to 10,000 Windows Embedded clients
- When having a SQL Server collocated with the site server it can have up to 50,000 clients
- A standalone primary site supports all the different roles. When a primary site is part of a bigger hierarchy, it no longer support having Asset Intelligence point, Endpoint Protection, or Synchronization point installed

For More Information:

• It can have up to 10 Management points connected
• Also, it can have up to 250 Distribution points connected

Secondary sites
This can only be set up as a child site to another primary site and participates in file-based replication to communicate with its parent Primary Site. This is not a mandatory role and should only be considered if you want to control the transmission of client data up the hierarchy. However, secondary sites do not have all the functionality of a primary site and must be a child site of an existing primary site.

A secondary site has the following features:

• It is installed with an SQL Express automatically if a SQL instance is not installed previously
• Installs a Management point and Distribution point on the same server
• Software Update point and State Migration point can also be installed
• Sends data to its primary site using file-based replication

Also, it can support the following:

• It can have only one Management point
• It can have up to 250 Distribution points
• It can manage up to 5,000 clients

It is important to note that Microsoft recommends that we try to avoid using secondary sites whenever possible, and just work with a regular primary site and use the different features which are included with the Distribution point. This will be covered in the next chapter.

Management point
A Management point has the following features:

• Primary contact point for clients within a site is present. You can also install a Management with a connection to a Site Replica database to reduce CPU cycles on the Site database server.
• Clients have to be connected to a Management point to communicate with a site.
• It can support having up to 25,000 clients.

For More Information:
If you have a remote location (for instance, on a low bandwidth WAN) you should not configure a Management point at the remote location. This is because a Management point is not aware of the site, unlike a Distribution point, which you can place within a boundary. If you place a Management point at the remote location, clients from another part of the site might actually use that Management point and cause more traffic on the WAN link. In this case, it would be better suited to use a secondary site.

**Distribution point**

The Distribution point is responsible for delivering data to the clients, both for applications and OS deployment and also, it has the following features:

- It allows streaming of applications using App-V
- It allows PXE connections using unicast or multicast
- It allows rate limiting and pull-based content deployment.
- It supports up to 4,000 clients
- It supports a combined total up to 10,000 applications and packages

**Software Update point**

Software Update point is integrated with Windows Server Update Services (WSUS) to deliver software updates to clients using Configuration Manager.

WSUS can be deployed on a regular Windows Server with either using a Windows Internal Database or using a regular Microsoft SQL Server. It supports the following features:

- It supports up to 25,000 clients (when installed with the site server)
- It supports up to 100,000 clients (when installed on another server that is not the site server)

Before Service Pack 1, you were restricted to having only one Software Update point in each site. Now with Service Pack 1, you can install multiple Software Update roles within a site.

**Fallback Status point**

The Fallback point allows clients to send status messages back to the site in case there is trouble with locating its Management point or for instance, trouble connecting to the site.
It is also useful if we want to use the client deployment report, which displays data received from the Fallback Status point. It is important to note that this role runs on regular HTTP and therefore it's not encrypted. This role supports up to 100,000 users and should be on a dedicated server.

**Application Catalog Website point & Web Service point**

These roles allow users to access a self-service portal for applications that are published to them. The portal itself is based solely upon Silverlight, both of these roles support up to 50,000 clients each.

**Reporting Services point**

The reporting role is attached to a SQL reporting instance to generate Configuration Manager Reports from the console.

This role copies over Configuration Manager Reports and applies security policies based upon the security settings in the site. It is important to note that only one reporting role can be attached to a SQL reporting instance.

There are other roles that can also be a part of the installation, which I’m not going to cover in detail in this chapter, but the following points might be worth looking into:

- State Migration point
- System Health Validator point
- Intune point
- Enrollment point
- Enrollment Proxy point
- Asset Intelligence synchronization point


But there are some components that are important and are required for most of the roles in Configuration Manager. They are as follows:

- **Internet Information Services (IIS)**: This is a web server role, which is included in Windows Server. The majority of the roles in Configuration Manager require having this role installed, since it allows clients to communicate with the server using HTTP or HTTPS.
• **Background Intelligent Transfer Service (BITS):** This is a component, which is included in most of the operating systems from Microsoft. It allows asynchronous, prioritized, and throttled transfer of files between machines using available network bandwidth. BITS is used by Configuration Manager to deliver content to the clients.

• **Remote Differential Compression (RDC):** This is an algorithm, which is used to analyze a situation where a file exists on two computers and that file is modified. Only the differing sectors need to be sent to the other computer. Site Servers and Distribution points use this to generate package signatures. So when we update a package it will only send over those sectors that have changed.

### Network flow

In a moment, you will see how the different roles and clients communicate with each other. This information will be useful when setting up or planning firewall rules between servers and clients, and roles that can be load balanced.

Network communication flow is described in the following table:

<table>
<thead>
<tr>
<th>Description</th>
<th>Protocol</th>
<th>Client/Server</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client DHCP to PXE point</td>
<td>UDP</td>
<td>Distribution point with PXE</td>
<td>67, 68 69 (TFTP)</td>
</tr>
<tr>
<td>Client to Distribution point</td>
<td>TCP</td>
<td>Distribution point</td>
<td>80 or 443</td>
</tr>
<tr>
<td>Client to Fallback Status point</td>
<td>TCP</td>
<td>Fallback Status point</td>
<td>80</td>
</tr>
<tr>
<td>Client to Management point</td>
<td>TCP</td>
<td>Management point</td>
<td>80 or 443, 10123(Client Notification)</td>
</tr>
<tr>
<td>Client to Software Update Point</td>
<td>TCP</td>
<td>Software Update point</td>
<td>80 &amp; 8530 or 443 &amp; 8531</td>
</tr>
<tr>
<td>Client to Cloud Distribution point</td>
<td>TCP</td>
<td>Azure Distribution point</td>
<td>443</td>
</tr>
<tr>
<td>Client to State Migration point</td>
<td>TCP</td>
<td>State Migration point</td>
<td>80 or 443 and 445</td>
</tr>
<tr>
<td>Client to Application catalog</td>
<td>TCP</td>
<td>Application catalog</td>
<td>80 or 443</td>
</tr>
<tr>
<td>Client to Global Catalog</td>
<td>TCP</td>
<td>Domain Controller</td>
<td>3268 or 3269</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>TCP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For More Information:

<table>
<thead>
<tr>
<th>Description</th>
<th>Protocol</th>
<th>Client/Server</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Manager Console to Client (Remote tools)</td>
<td>TCP</td>
<td>Clients</td>
<td>2701 for Remote Control and 3389 for Remote Assistance</td>
</tr>
<tr>
<td>Management point to Site Server</td>
<td>TCP</td>
<td>Management point to Site Server</td>
<td>135, 445 and Dynamic ports in RCP range</td>
</tr>
<tr>
<td>Management point to Global Catalog Domain Controller</td>
<td>TCP</td>
<td>Active Directory</td>
<td>3268 or 3269, 135, 445 and Dynamic ports in RCP range</td>
</tr>
<tr>
<td>Management point to SQL Server</td>
<td>TCP</td>
<td>SQL Server</td>
<td>1433</td>
</tr>
<tr>
<td>Site Server to SQL Server</td>
<td>TCP</td>
<td>SQL Server</td>
<td>1433</td>
</tr>
<tr>
<td>SQL Server to SQL Server</td>
<td>TCP</td>
<td>SQL Server</td>
<td>1433 and 4022 SQL Service Broker</td>
</tr>
<tr>
<td>Application Catalog Web Service point to SQL Server</td>
<td>TCP</td>
<td>SQL Server</td>
<td>1433</td>
</tr>
<tr>
<td>Application Catalog Website point to Application Catalog Service point</td>
<td>TCP</td>
<td>Catalog website to Catalog Service point</td>
<td>80 or 443</td>
</tr>
<tr>
<td>Site Server to server roles</td>
<td>TCP/UDP</td>
<td>Site Server connects to another server role</td>
<td>445 (TCP) 135 (TCP/UDP) and Dynamic Ports in RPC range</td>
</tr>
<tr>
<td>Software Update point to Internet</td>
<td>TCP</td>
<td>Software Update point to connect to Microsoft</td>
<td>80</td>
</tr>
<tr>
<td>Software Update point to Upstream WSUS Server</td>
<td>TCP</td>
<td>Software Update point to internal WSUS server</td>
<td>80 and 8530 or 8531</td>
</tr>
<tr>
<td>Exchange Server Connector to Exchange Online</td>
<td>TCP</td>
<td>Site Server to Exchange Online, for instance, Office365</td>
<td>5986</td>
</tr>
<tr>
<td>Exchange Server Connector to Exchange on premise</td>
<td>TCP</td>
<td>Site Server to Exchange server</td>
<td>5985</td>
</tr>
</tbody>
</table>
Some important factors regarding port usage within Configuration Manager are as follows:

- Most of the traffic is either based upon HTTP (port 80) or HTTPS (port 443) depending on whether you have deployed a PKI infrastructure or not.
- Some roles require the use of port 445 based on SMB traffic (regular file transfer protocol).
- Some roles also require the use of a dynamic range of ports from the RPC protocol. The range for RPC is between port 49152 and 65535.
- RPC also uses port 135.
- Most SQL connections use port 1433, which is the standard SQL port for SQL to SQL connections. SQL also uses port 4022, which is used by the SQL function service broker, which is used to replicate between parent and child SQL Server.
- Different client installation methods use different ports, where manual installation can use either HTTP/HTTPS 80 or 443 and SMB 445. Client push installation uses a combination of the previous ports and dynamic RPC ones.

New in Service Pack 1

Before we continue on how to deploy High Availability, it is important to note some of the changes that have been done to the Service Pack 1 release. Some of the new features are large hierarchy changes that can affect the site design. It has the following features:

- Support to update client notifications from the Console
- Support for Windows Server 2012 for Site Systems and clients
- Support for Microsoft SQL Server 2012 for Site databases
- Support to place a Distribution point in Windows Azure
- Support for multiple Service Update points within a site
- Support to expand a primary site into a hierarchy including a CAS
- Support for PowerShell
- Support for pull-based Distribution points
- Support for agents on Mac clients, Linux servers, and UNIX servers
- Support to configure users’ profile settings such as folder redirection, offline files, and roaming profiles

For More Information:
• Support for applications that has been created using Microsoft Application Virtualization Version 5.0
• Support for thin clients using Windows Embedded
• Support for endpoint protection for Mac clients, Linux servers and UNIX servers
• Support for Intune integration for mobile device management

During the writing of this book, System Center 2012 R2 is in the making and is expected to be released October 18, 2013, the release will focus more on Intune and mobile device management.

Also it will support the next wave of operating systems Windows 8.1 and Windows Server 2012 R2.

Summary
In this chapter, we have gone through the different components and roles within Configuration Manager, what their functions are, and how they scale. We looked into different components which need to be taken into account when planning for High Availability such as networking, hardware, and other critical infrastructure components such as AD, DNS, and DHCP.

We also took a closer look at how Microsoft IT has deployed their Configuration Manager solution to get a better overview on how a site design with High Availability might look like.

In the next chapter, we will start by going through how we can set up the different roles and features to become highly available.

For More Information:
Where to buy this book


Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our shipping policy.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.