Metropolia

Esa Kuusisto

Centralized Data Center Provisioning and Configuration in Managed Service Provider Environment

Helsinki Metropolia University of Applied Sciences
Degree (Master's Degree)
Degree Programme (Information Technology)
Thesis (Master's Thesis)
Date (22 May 2012)

Metropolia

PREFACE

This Master's Thesis contains information of servers and network management in a data center. I believe this gives the reader new ideas on how to do things in a data center environment more efficiently.

One of the biggest challenges of the study was to change my own thinking about how things could be done instead of how I have been doing them for many years. This study explains how much easier basic management tasks can be instead of repeating the same configurations and modifications multiple times.

I'd like to give a huge appreciation to a company called Crescom where they allowed me to do this Master's Thesis and a possibility to study and work at the same time.

I would also like to thank Ville Jääskeläinen at Metropolia for his instructions and support and Jonita Martelius for her help with the English language.

I also want to thank my friends and family who helped me with my Master's Thesis and gave a lot of good advice and support.

Espoo May 22 2012

Esa Kuusisto

Metropolia

ABSTRACT

Name: Esa Kuusisto

Title: Centralized Data Center Provisioning and Configuration in Managed Service Provider Environment

Date: May 22 2012 **Number of pages:** 77

Degree Programme: Information Techonology

Specialization: Multimedia Communications

Instructor: Ville Jääskeläinen, Principal Lecturer

Instructor: Pekka Rasi, Crescom Ltd

The topics of this Thesis were centralized data center server provisioning and management. Following are the questions the present study aimed to give answers to: Is it a correct solution to speed up installations server updates and big configuration changes in a data center? Can the provisioning software be used to automate support jobs which can take many hours to complete and do the same tasks repeatedly? Does the provisioning software take out possible errors in configurations which are done from one centralized location?

Provisioning application brings benefits to managing different operating systems and their updates. It allows selecting required update packages and distributing and installation of selected updates to the managed servers.

Provisioning enhances new server installation since the software can deploy new virtual machines rapidly. It can also provision new operating system installations to empty bare metal servers.

According to the study the provisioning application did bring noticeable time savings in the deployment process of the new operating system deployment to a bare metal server. It installed common settings automatically to a server under deployment. During the deployment process a server is added under a provisioning software management.

Using provisioning software to manage and deploy a server did bring time savings to the company. The use of the predefined installation process to deploy new installations helped to control servers in a Managed Server Provider (MSP) environment. BladeLogic provisioning software can be used to manage a server and to help to simplify a server management because only BladeLogic software is needed and all server management is centralized.

Key words: Provisioning data center management configuration server network

Metropolia

OPINNÄYTETYÖN TIIVISTELMÄ

Työn tekijä: Esa Kuusisto

Työn nimi: Keskitetty konesalin provisionti ja hallinta hallitussa palveluntarjoajan ympäristössä

Päivämäärä: 22.05.2012 **Sivumäärä:** 77

Koulutusohjelma: Tietotekniikka

Ammatillinen suuntautuminen: Multimedia Communications

Työn ohjaaja: Ville Jääskeläinen, Yliopettaja

Työn ohjaaja: Pekka Rasi, Crescom Oy

Tämän lopputyön aihe on keskitetyn konesalin palvelimien provisionti ja hallinta. Onko se oikea ratkaisu nopeuttamaan palvelinsalissa tapahtuviasennuksia palvelimien päivityksiä ja isoja konfiguraatio muutoksia. Onko ohjelmalla mahdollisuus automatisoida yleisiä ylläpito töitä joiden tekemiseen ennen on tarvittu monta henkilötyötuntia ja toistamaan sama tehtävä monta kertaa? Laskeeko provisionti ohjelmisto virhemahdollisuuden määrää kun voidaan yhdestä keskitetystä paikasta hoitaa konfigurointi?

Provisiointi sovelluksen tuoma etu hallittaessa eri käyttäjärjestelmien vaatimia päivityksiä. Tarvittavien päivityksien valitseminen palvelimille jakaminen jasentaminen.

Kuinka provisionti nopeuttaa uusien palvelimien asennuksia? Provisionti ohjelmistolla voidaan perustaa uusia virtuaalisia koneita nopeasti useita kappaleita. Samoin voidaan jakaa tyhjälle fyysiselle koneelle uusi käyttöjärjestelmä.

Provisiointi sovellus toi huomattavaa nopeutusta uuden palvelimen käyttäjärjestelmän asennukseen. Yleisimpien asetusten asettaminen onnistui automaattisesti jo asennusvaiheessa. Palvelimen hallintaan saattaminen pystyttiin toteuttamaan automaattisesti provisioinnin yhteydessä.

Yritykselle provisioinnin käyttöönotto toi huomattavaajan säästöä perinteiseen asennusprosessiin verrattuna. Käyttämällä BladeLogic provisionti sovellusta palvelimien hallinnan yhtenäistämiseen yhden sovelluksen alle nopeutti ja yksinkertaisti ylläpitotöitä.

Avainsanat: Provisiointi konesali Hallinta konfigurointi palvelin verkko

Metropolia

TABLE OF CONTENTS

Metropolia

LIST OF ILLUSTRATIONS

Metropolia

ACRONYMS

ACL	Access Control List
AD	Active Directory
API	Application Programming Interface
BL	BladeLogic
CD-ROM	Compact Disk – Read Only Media
CIFS	Common Internet File System
CLI	Command Line Interface
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Service
DRAC	Dell Remote Access Controller
DVD	Digital Versatile Disk
ERP	Enterprise Resource Planning
iDRAC	Integrated Dell Remote Access Controller
iLO	Integrated Lights-Out
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Mediaccess Control

MSI	**Windows Installer**
MSP	**Managed Service Provider**
NAT	**Network Address Translation**
NIC	**Network Interface Card**
OS	**Operating System**
PXE	**Preboot Execution Environment**
RAM	**Random Access Memory**
RPM	**Repository Package Manager**
RSCD	**Remote Server Call Daemon**
SSH	**Secure Shell**
TCP	**Transmission Control Protocol**
TFTP	**Trivial File Transfer Protocol**
UDP	**User Datagram Protocol**
UID	**User Identifier**
VLAN	**Virtual Local Area Network**
VPN	**Virtual Private Network**
VRF	**Virtual Routing and Forwarding**
WAIK	**Windows Automated Installation Kit**
XML	**Extensible Markup Language**

1 INTRODUCTION

A Managed Service Provider (MSP) is a company which offers Information Technology (IT) services, such as IT hardware and software, to corporate customers. It has become a practice for companies to outsource their IT services to MSPs to save costs. Companies which offer IT services are often described as Service Providers. MSP maintains IT related services which are outsourced and offers service which includes strategies to improve and maintain services the best way possible.

MSP environments are constantly changing as services are added and current services upgraded, modified or removed. Old services are removed from the system to give room for new services. The backbone of the services is servers and network equipment in MSP environments.

In the current situation it takes 15 minutes to deploy a new customer and to make the necessary network configurations. Deploying a new virtual server takes 30 minutes and additionally between one to two hours to the make the basic configurations. Deploying a new physical server it takes one to three hours to install a new operating system and in addition between one to two hours making the basic configurations. All this is time consuming.

The process now usually involves many employees and installation steps are made manually. This practice is very error prone. As a result some configuration parameters may be missed at the end when the number of the customers increases deploying servers to multiple clients and this is very time consuming. New deployments are usually not distributed equally but they come in bursts. For example there can be one week without any new installations and another week several customers need many new servers deployed at the same time. This is problematic for the technical personnel deploying new servers and project managers who need to manage and prioritize available resources.

Other problems take place when updating operating systems. Automatic updates cannot be used because all the servers cannot have all patches installed and reboots must be scheduled. Thus changing for example a common configuration parameter to all servers takes many days and becomes an extensive operation. A manual configuration change is a process where

one needs to login to every server and make same configuration to change manually. For example changing a password for a single username for one thousand servers requires one thousand logins and one thousand password changes.

A solution has been proposed to the constraints. Provisioning is a method of automatizing new server deployments. A normal server deployment includes many steps such as operating system installation application installation and basic configurations such as IP addresses and updates. A provisioning software can also make operating system upgrades and configuration modifications to servers using predefined configuration parameters. Some provisioning software such as IBM Tivoli Provisioning Manager and BMC BladeLogic include management tools which can be used to manage different types of servers.

There are a number of tools in the market to assist deployment and maintenance processes. One of them is BMC BladeLogic [1] which the case company has purchased. The aim of the present study is to respond to the following research questions.

Can provisioning software speed up new server deployments?

Can provisioning software support current server installations?

Is the BladeLogic provisioning software a good solution for provisioning and management?

These research questions are significant because this Thesis was done for a MSP company serving several customers. At the time of the study commonly referred to as ‘currently’ in the study the company had over one thousand servers both virtual servers and physical servers. The virtual servers were virtualized using two different virtualization platforms. The more widely used platform was VMWare Vsphere [2] and the other virtualization platform is called Citrix XEN virtualization software [3].

Network environment consist of over one hundred switches or routers. A new server deployment usually raises a need to make modifications to the network equipment. Customers have their own dedicated networks. The dedicated network is an Internet Protocol (IP) subnet where there is a server for only one customer. Network boundaries are restricted using virtual local area network (VLAN). Traffic crossing network boundary to Internet or to other customer needs to go through a firewall. Traffic flows are controlled using firewall rules.

The operating system (OS) for the target server must be selected before the installation process can begin. The most common server operating systems are Microsoft Windows and Linux. Microsoft Windows includes many different versions which are planned to be used for different purposes. The deployment of the different versions of Microsoft Windows does not differ from each other. An other very popular operating system is Linux. It was developed at the beginning of the 1990 by Linus Torvalds. Linux itself is only a small kernel which is a core component of a Linux and other components are installed around it. Linux is often derived under different distribution. The most common distribution in business environments is Red Hat Linux.

Operating system such as Microsoft Windows and Red Hat Linux differs completely from each other. Even if they provide same kind of services to users the configuration management and software are totally different. Both systems need to have the same predefined network parameters before they can access the network.

Hosted servers usually include managing the servers. Management includes keeping the server operating system and applications up to date by updating software regularly. At the same time the management software needs to keep up to date the list of the servers and their software levels. Then server administrators can easily see servers which require updating and which update packages are needed to be installed.

Today’s operating systems and applications offer options to automatic updates which often requires server reboots or at least the software service to be restarted. In business hours this may be catastrophic because users cannot access the application during the update. After upgrade there is also a possibility that the software does not start properly. Enterprise applications

depend heavily on the operating system version and when it is changed the application may refuse to work in some cases. Software upgrades need to be tested in a controlled environment simulating the current production environment. Controlling updates which are installed and when is one key feature in data center management software. It is also important that updates are installed in precise time and applications restarted under management software control. One of the key features is keeping a list which servers have been updated and which updates were installed.

2 BLADELOGIC AND COMPANY INFRASTRUCTURE INFORMATION

This chapter explains the background information of the BladeLogic server components and their relations to each other and basic functions. BladeLogic Server Automation application is not a single application, it is a distributed packet of software components where each component has a dedicated function.

The examples of the company's current environment and more detailed requirements for the management software are included. The examples consist of problems which are tested against BladeLogic features and its abilities to make management automated and more flexible.

Some of the software packages in BladeLogic are required for basic functions. If a given feature is required additional software packets are installed. BladeLogic uses wizard style configurations in multiple places, if for example configuration program only asks configuration parameters which only apply to selected task.

2.1 BladeLogic Provisioning Software

BMC BladeLogic Application Suite program is a Java based provisioning software. It can additionally manage configure and update server operating systems. The BladeLogic application contains three necessary components. First one is the application itself. The second required component is a database server which the application uses. The third component is a file server. All these three components can be located at same server or they can be distributed to different servers and locations. The 8.1 version of the BladeLogic software is currently deployed and under evaluation.

The BladeLogic application version 8.1 can be installed to a Windows or Linux platform. The installation platform needs to have at least one gigabyte of memory and 100 gigabytes of free disk space. Supported Windows versions are from Windows 2003 to Windows 2008. The supported Linux version is a RedHat Linux version five. Application server function can be used by graphical user interface (GUI).

The database server for The BladeLogic application is a required component. Supported database servers are a Microsoft SQL server and a Oracle Database. Microsoft SQL server can be run only in Windows platform. Oracle Database can be installed and operated in both Windows and Linux platforms. All BladeLogic information is stored in the database. The application gets all its data from database which it needs to function correctly.

A file server is a place where all necessary files are located which are needed in deployment and update processes. When deploying a new operating systems certain files are needed. Every version of the operating system has its own files in a certain format. This format is consistent with the BladeLogic file server and a deployment method. Same procedure applies to operating system updates. The updates for different operating systems and applications are all located in the file server when the update process deploys files to selected servers files are copied from the file server. The BladeLogic has its own process of the getting new versions of the updates and inserting them to the file server for future use. Instead of downloading operating system files from the Internet or other sources administrator of the BladeLogic system manually copies installation files from an installation media and insert those files in a correct format to the file server.

The BladeLogic has also other service components such as a TFTP (Trivial File Transfer Protocol) server and a PXE (Preboot Execution Environment) server. The TFTP server offers file transfer services over UDP (User Datagram Protocol). It has no user authentication and offers only file sending and file downloading functions. TFTP usually offers firmware configuration and boot files to the devices which do not have any static memory. Those devices will lose their configuration and boot files when power is lost or device is power cycled. PXE server is a service which offers information to clients which boot image it should request from TFTP server.

2.2 BladeLogic Three-Tier Description

BladeLogic Application is divided to three tiers. This is called three-tier architecture. Figure 1 illustrates the relations of the major components of BladeLogic (see Figure 1).

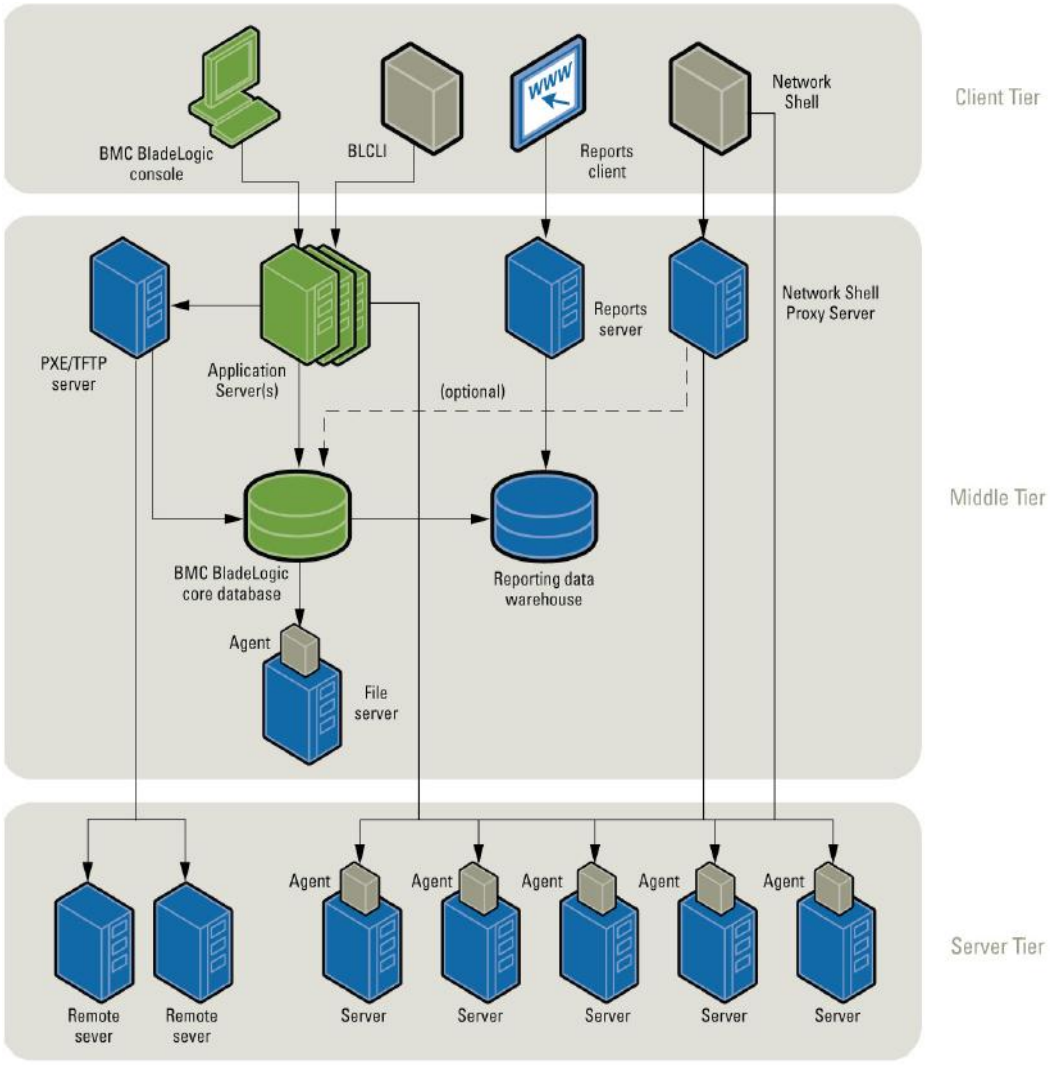


Figure 1. BladeLogic application tiers. [11]

The client tier includes BladeLogic console where users manage the system. This console is a platform for a sophisticated tool for managing and automating procedures in a data center environment. The client tier provides management for different supported operating systems such as Oracle Solaris Linux versions from Red Hat and Suse IBM AIX HP-UX and Microsoft Windows Servers. For customized use there is CLI (Command Line Interface) which provides API (Application Programming Interface) access to different functions and automating different processes. Network Shell is for administrating servers which are located in a server tier. [13]

The middle tier is the section of the BladeLogic components where Application Server is the primary component. It controls the rest of the BladeLogic components such as a database and a file server. In the middle tier there are other several components such as PXE and TFTP server which are required for provisioning. Reporting services are optional components in the middle tier. Also Network Shell Proxy Server is an optional component and it is required only if an application server is not equipped to work as Network Shell. Network Shell Proxy Server works as a proxy between application server and managed servers.

Server tier is a logical area where managed servers are located which have RSCD agents installed. An application server communicates with RSCD agents directly or through Network Shell Proxy Server.

2.3 Current Server Management Process

A company which has been MSP for a while probably has several servers under their management. Before obtaining a management or a provisioning software server management is usually done as a manual management process. The manual management is a process where the system administrator or a super user connects independently to all servers and performs all management functions such as updates and configuration changes manually.

A new server with an operating system can be brought in from another location. The server with existing applications needs to stay untouched for configuration changes. Adding new management components cannot disturb the existing applications and their configurations. Management components are called agents. A server can also be an existing production server in a company's data center but it has not any existing centralized management software.

The installation of the management components is a mandatory task in order to manage multiple servers in a reasonable time. It is needed so that status and configuration changes can be done from a centralized management center and those changes can be scheduled to be processed at a requested

time. The components manage and monitor a server continuously and return the status of the server and it components. Some server agents do not send any information to the management software. They provide only the interface for the management software to use to communicate with a server.

The company's current server management has three different components; software and a hardware monitoring service and a service poller. The monitoring components are centralized and they have two different methods for collecting information. The results must be converted to a form which the analyzer can process. Software monitoring includes monitoring operating system and application components which check the status of operating system components and also checks selected components and returns the status of selected parameters. A service poller uses an external software component which sends predefined requests to a server. A request is configured to connect to a service which is running on a server. All poller requests are made by an external server and the requests are returned to a poller server which processes answers and forwards the results to a monitoring service when a result parameter matches to the level it sets an alarm. These are forwarded to a server application where the alarms are processed.

For example a server has a web service listening on TCP port 80. A poller sends requests to a web service periodically and when a web service returns the answer to poller which sends the results to a management server. Based on the answer the management server sets an alarm if the answer is wrong or a web service fails to answer to the request.

A problem with the current management is that it can only monitor servers and the return statuses of those servers. Configuration changes and software updates are not possible. Server updates are done via separate centralized server update software. The current server update software only supports Microsoft Windows Server updates for Windows 2000 and 2003 servers. Currently latest Windows server version is 2008 and it was released 17th of February 2008 [7]. Since then most of the new Windows server installations have been 2008 versions. Updates to Windows 2008 versions are done manually which is a very time consuming process. The estimated time is that selecting updates to all currently managed servers take one 40 hour work week. The company's current process is that mandatory updates to

servers must be done at least four times a year. This brings extra overhead in the updating process.

When the new server management software is deployed and the management of the existing servers is moved under new management software certain steps are needed. Servers can be monitored externally by multiple sources. Installed management components agents are needed to be installed to the server. Multiple agents in one server can conflict with each other. This can produce unexpected situations to monitoring or even affect the performance of the server. Old agents must be removed before new agents can be installed. This can produce a service break which must be taken into consideration. After the new agent is installed a management server needs to be notified that a new server can be brought under its management.

Currently the company has many IP networks where the servers are located. When changing from a current network management agent to BladeLogic RSCD agent in some cases server IP address must be changed. In several cases there are servers located in the IP network where there are also other customer servers. In current deployments all customers have their own private IP network. When a server is moved from another network and it is taken under management software the IP address or network name is required. In some cases network changes require a new network to be deployed. If there is no currently existing network where a server could be located a new IP network configuration is deployed. In this case BladeLogic application needs to have an access to it so it can access the RSCD agent. If there is a suitable IP network available to the server network then no IP network deployment is needed.

2.4 Network Planning For a New Server

The process of a new deployment always begins with a plan. Currently a new client process begins with network planning. Different clients have different requirements for their network. Basic concepts which are common to every customer are located in their own separated virtual local area network (VLAN). Customers have their own dedicated Internet Protocol (IP) address network and network address is located in VLAN (see Figure 2).

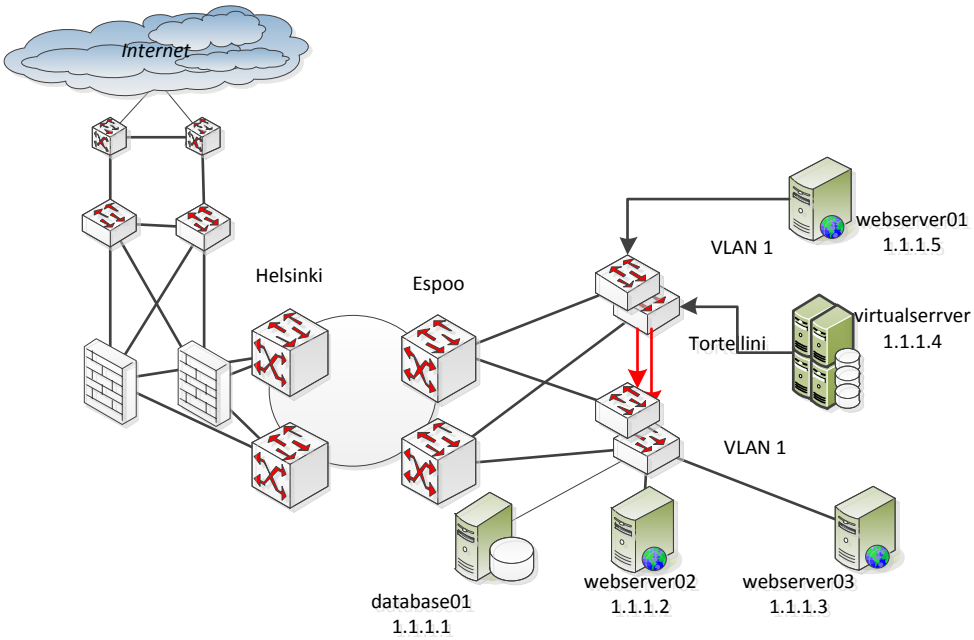


Figure 2. Crescom network example.

Figure 2 describes common network configuration which includes servers switches, firewalls and routers.

Each customer has a dedicated network profile which includes a public network and a private network. Public network is a network block where connections from Internet or other network sites connect. Public network offers connections to server services. Private network is a backup network which is used for server management and backups.

In several cases a server does not have direct connection to Internet but they use private network to connect the company's proxy server to get the necessary Internet connection or a simple mail transport protocol (SMTP) connection to SMTP proxy to send email.

Public network is dedicated to traffic directed to services running in a server. Connections through public Internet can use a routable IP address or a connection encapsulated in a virtual private network (VPN). VPN connections are de-encapsulated at the edge of the network and IP packets are forwarded to the server. Encapsulating packets inside IP-packets do not provide any protection to encapsulated data. Internet Protocol Security (IPSEC) provides authentication and encryption to the IP-packet. IP-packets are protected be-

tween end-points. End-points known as VPN gateways encapsulate and de-encapsulate IP-packets when they enter or exit VPN gateway (see Figure 3).

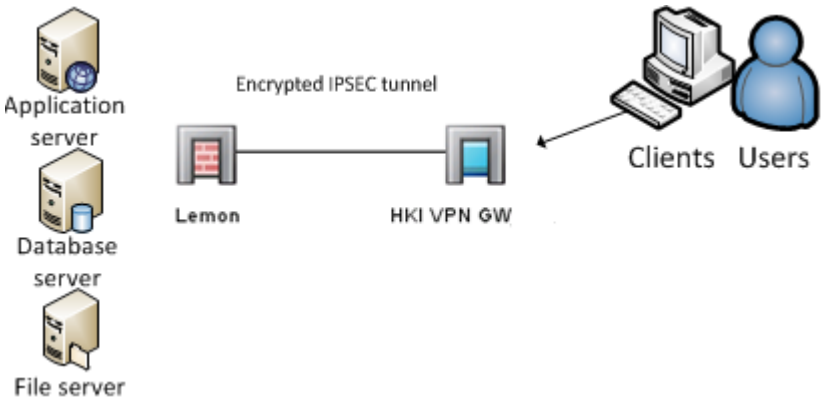


Figure 3. VPN tunnel example.

Public and private networks use IP addresses defined in the request for comments (RFC) 1918.[4]. Connections from public Internet would not work if the network address translation (NAT) mechanism (RFC 2663) [6] was not implemented. Traffic that arrives to a certain public routable Internet address needs to be translated to private IP address. This translation process is not visible to clients who connect over Internet. Response packets from the server also need to be translated back to a public IP address before the packet from the server can be routed to the client over Internet. This translation is done by firewalls or routers (see Figure 4).

Figure 4. Network Address translation example. IP 1.1.1.1 connecting to any IP address and any service is translated to 2.2.2.2 IP address.

There are pre-defined network blocks where new public and backup networks are selected. New network blocks are selected and assigned to customers. The network block contains 128 IP addresses. One IP address is re-

served for network address, the second address is broadcast address and the third address is reserved for a router. Now there are 125 IP addresses left from the network block which can be assigned to servers. Both public and backup network have 125 addresses free to be assigned to servers. In some rare cases a customer needs more than 125 IP addresses and additional public or backup networks must be deployed.

The network deployment process involves the creation of VLAN and its configuration. VLANs virtually separate traffic between different customers. Every VLAN has an numerical TAG, a number between one and 4094. In the current configuration the VLAN has an IP address which comes from the network plan. The IP address of the VLAN acts as a router for servers and must be assigned to correct switch ports.

Public and backup networks are physically separated networks. For customers who do not use company shared Internet but have their own connection only backup network is created.

Servers can communicate with each other using public network. It is recommended that the private network is not used to communications between servers. There are three reasons why private network should not be used in server to server communication. The first reason is that traffic is more easily controllable when designated to go only in one network. The second reason is that backup tasks are scheduled to run possibly through all night. The backup task can disturb other traffic and that is why backups have their dedicated network. Maintenance work to a private network is done during business hours and it is used to production traffic there would be production halts under maintenance. The third reason is that a private network has single point of failure points such as one switch, and switches have only one power supply. Public network devices have all components duplicated dual power supplies two or more switches routers and firewalls. Public network does not have single point of failure points (see Figure 5).

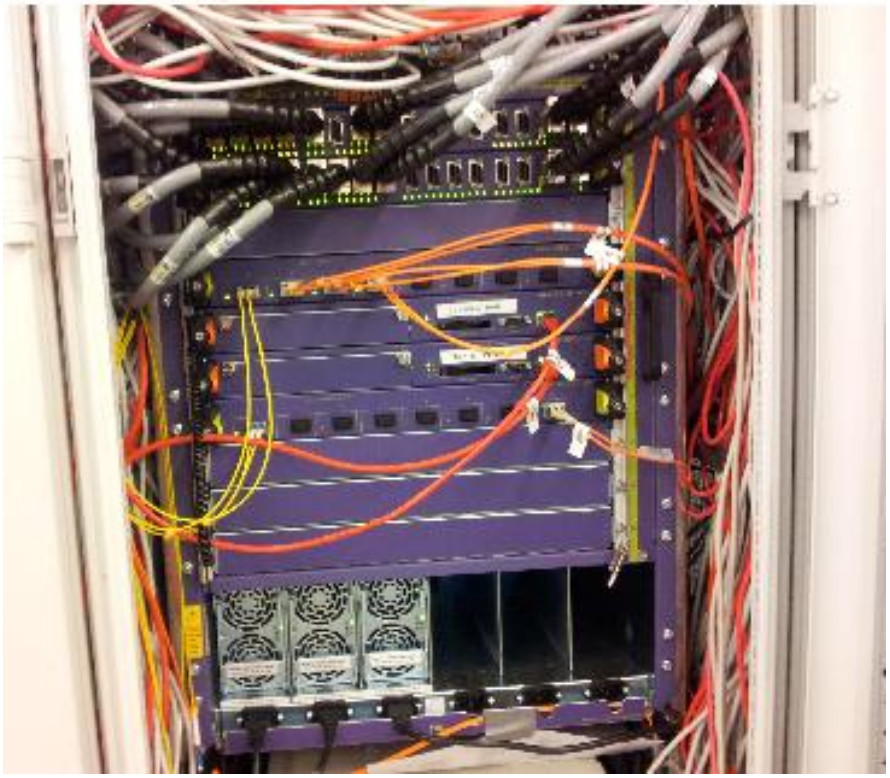


Figure 5. Core switch with triple power supplies and dual management modules.

The company has several TeliaSoneras Datanet network connection points in its data center. The Datanet is a concept where customer sites are connected together using VRF (Virtual Routing and Forwarding) technology. In VRF ISP (Internet Service Provider) or operator can use shared routers to route traffic. Shared routers in a core of the network are shared between multiple clients. The traffic between clients is separated by VPN and different customers cannot access other customer networks when the traffic is routed the routers need to keep routing information in memory. In a normal routing process all clients have their network traffic routed based on router's routing table and all clients have same the routing information. This brings up problems in a private network where different customers can have overlapping IP networks which prevents traffic to those networks. In VRF every customer has their own dedicated routing table in the routers and allow overlapping IP networks (see Figure 6).

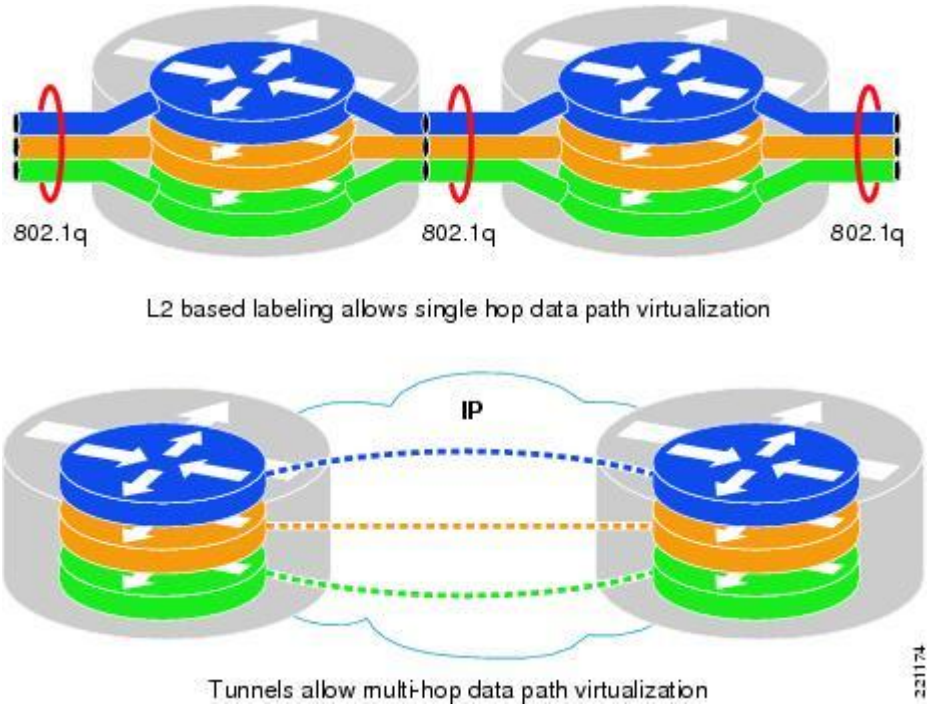


Figure 6. Logical VRF example [9[

A private network which is used to manage and backup servers has been done by using a technology called VLAN aggregation [6]. All servers share the same network subnet mask and router address. Customers are separated using VLANs. Customers in different VLANs cannot communicate over VLAN boundaries. In a VLAN aggregation there is a Super VLAN where the router is located which can communicate to all servers. Customers VLANs are created as sub VLAN where IP address the range of server is defined. This range defines IP addresses which the server IP can use to communicate to router or other servers.

2.5 Selecting between 32 Bit or 64 Bit Operating System

A server configuration includes an operating system (OS) version. The server operating system selection consists of several important choices which cannot be changed once the deployment has been completed. The only way to change the selection is to re-deploy the server which includes data loss. Before re-deploying, a really important step is to save backup data from the server. Making the selection between a 32 bit and a 64 bit version of an op-

erating system is an important selection. In a 32 bit operating system the environment limits are how much memory the server can use. Limit is a 2^a 32 bytes. a 64 bit operating system does have a memory limit of 2^a 64 bytes which is a 16 Exabytes. The problem with a 64 bit operating system is that basic memory and hard drive consumption is higher because memory addressing and usage is using double amount of the addressing compared to a 32 bit operating systems.

Running a 64 bit operating system has several hardware and software limits. The server hardware must support a 64 bit operations before a 64 bit operating system can be installed and operated. A 64 bit operating systems requires a 64 bit drivers to operate correctly and if a 64 bit capable hardware and drivers are not available, a 32 bit operating system must be selected.

During a server deployment it is possible to deploying additional applications such as a basic server software and components like email web file and database server. Additional application components in today's environments can contain application files of several gigabytes.

2.6 Virtualization Properties and Virtual Server Deployment

Deploying a virtual server is a process of deploying a server operating system in a virtualization platform. In today's non mainframe environment the virtualization platform is provided by using an existing x86-architecture platform. A x86 architecture hardware is a common Intel compatible platform definition where other manufacturers can design and build compatible components. Virtualization is provided by software and hardware which use combining features of hardware emulation and direct hardware access to provide necessary hardware to support working server guest environment. The commissioner company mainly uses VMWare ESX products to virtualize servers.

Virtual servers known as a virtual machine guests are operating systems which are isolated from other guests and from host computer. The host computer provides a virtualized platform to guests. This platform is known as

hypervisor [3]. Hardware emulation is used to provide the virtualization layer between the virtualization host and guest.

The server infrastructure includes several standalone ESX servers and several clustered ESX servers. The standalone ESX server has same properties as a clustered server excluding all high availability (HA) features. ESX HA feature includes migration of the guest server from one cluster node to an other cluster node. In a failure situation when one node in the cluster fails an other node of the cluster restarts the guest operating system. ESX server HA features depend on the commands of the VMWare virtual center (VMWare vCenter Server). The ESX server can be accessed directly using a CLI (Command Line Interface) or the VMWare management server. A management server is a necessary service when using certain functions, such as moving guests between ESX servers. Virtual machines can be migrated when they are in an operational state. Direct management commands to cluster nodes should be avoided. Direct access can disturb automatic processes which a management server can perform to the server. Updating an ESX server is done by the management server. The system administrator can perform management tasks using vCenter Server.

A virtualization environment does not only have properties of deploying new virtual servers. The configuration definition of the cluster nodes which hosts virtual servers is important. In a MSP environment cluster nodes are under constant changes. New virtual networks need to be provisioned and old ones removed and new storage capacity is installed and configured to the all of the cluster nodes. All network and storage deployments, removes and all management tasks can be done using a virtual center or a provisioning manager software.

There are two different methods to deploy new guests in the ESX environment. The first method is to use a template. The second method is to deploy a completely new installation from installation files. Starting a new deployment process can be manual or automatic. In a manual deployment all necessary parameters such as guest type which is the operating system version virtual machine name number of the network interfaces disk space processor count and size of the RAM (Random Access Memory) must be typed manually. An automatic process needs to have same information as the

manual deployment but the requested information can be predefined in the configuration files.

A template is a server image from an existing virtual server which can be re-used multiple times. A template can have additional configuration and applications installed. In templates a predefined configuration can have a preset number of processors amount of memory networking configuration and storage capacity. A template image can have other predefined virtual machine configurations which define its behavior and location in virtualized environment.

A manual creation of the virtual server includes all necessary configurations such as network configuration number of processors amount of memory and number or hard disks and disk size. After all computer hardware parameters are set and configured the virtual server hardware is ready to continue the operating system installation. A basic operating system installation process is not different from an to installation process of a physical server operating system.

2.7 Bare Metal Server Provisioning Using the BladeLogic

A physical server is known as a bare metal machine. Physical installation of the server is required before provisioning process can begin. This includes all components such as power and network cables connected to the right places.

Provisioning a bare metal server can be done using two different methods. The first one is using preboot execution environment (PXE) and the second method is using installation through Dell Remote Access Card (DRAC). PXE provisioning allows installation of all operating systems which are supported by the BladeLogic and. DRAC installation process is limited to the Windows operating systems.

Before the provision process can start a server network interface card (NIC) needs to have proper settings configured. (Step 1 in Figure 7.) The process starts when the target machine contacts dynamic host control protocol (DHCP) server. (Step 2.) After successful contact the server receives an IP

address and other network parameters from the DHCP server. (Step 3.) The target server contacts the PXE server. (Step 4.) The PXE server contacts provisioning system database for server configuration information. (Step 5.) The PXE server deliver instructions to a bootstrap program how to boot the server. (Step 6.) Target machine boots and processes bootstrap parameters and contacts the application delivery server. (Step 7.) The provisioning application server checks the database for correct instructions for a target machine. (Step 8.) Instructions for provisioning are delivered to the target server. (Step 9.) The target machine contacts the file server where to get necessary files for OS deployment. (Step 10.) Optional steps 11 and 12 in Figure 7 represent a remote system call daemon (RSCD) agent installation to the provisioned server and post provisioning tasks.

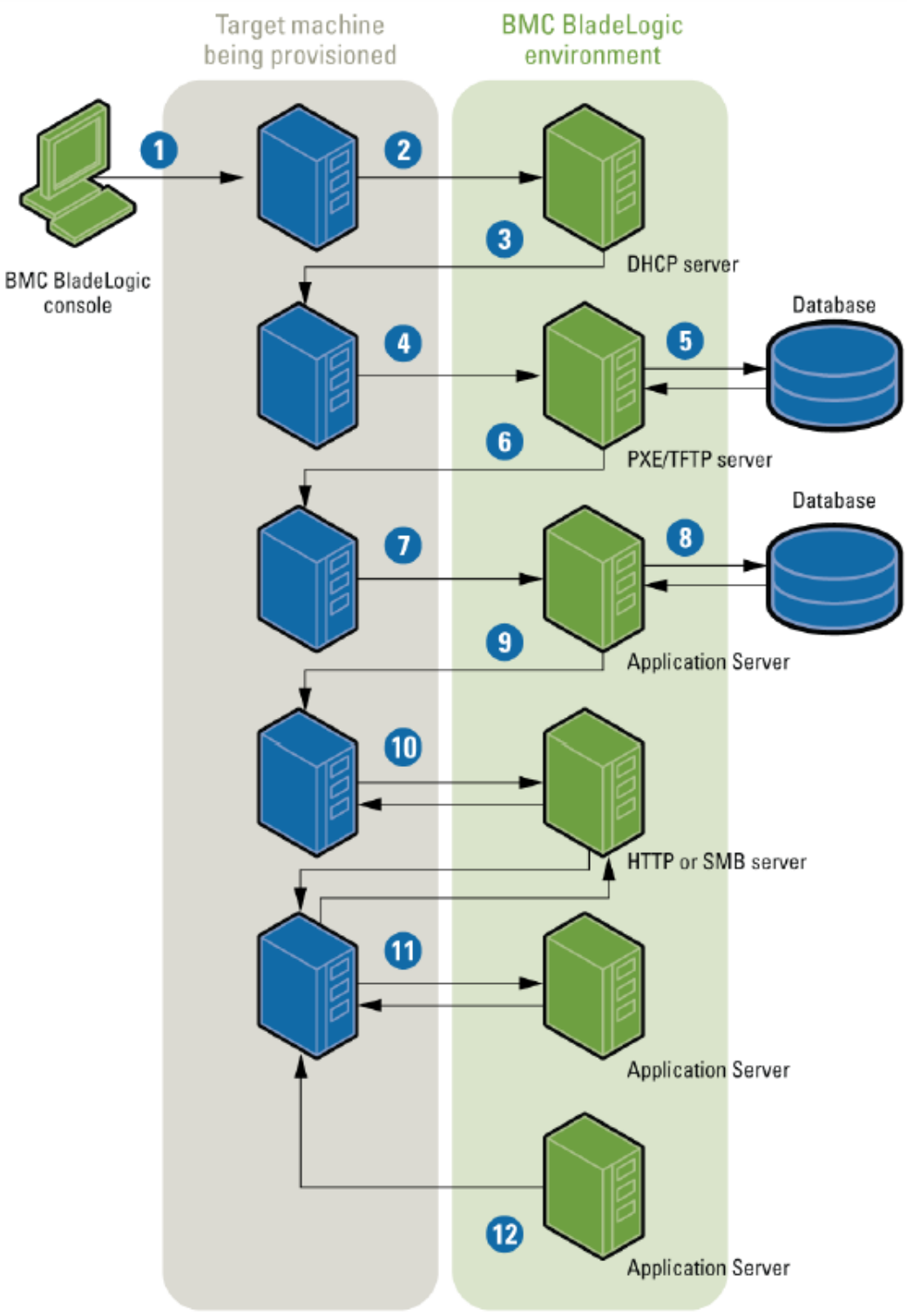


Figure 7.PXE provisioning steps. [12]

Some of the server installation steps are similar if the server is manually installed or a PXE provisioning is used. Before the installation can begin the operating system type and version must be known. IP addresses need to be

selected and a server hardware has to be installed to the proper location. In Figure 8 shows a process flow on how a new server deployment using manual installation method is done and it is compared to the PXE provisioning method. Figure 8 shows a case where the operating system installation, application installation and management software installation are separate processes and done by different persons.

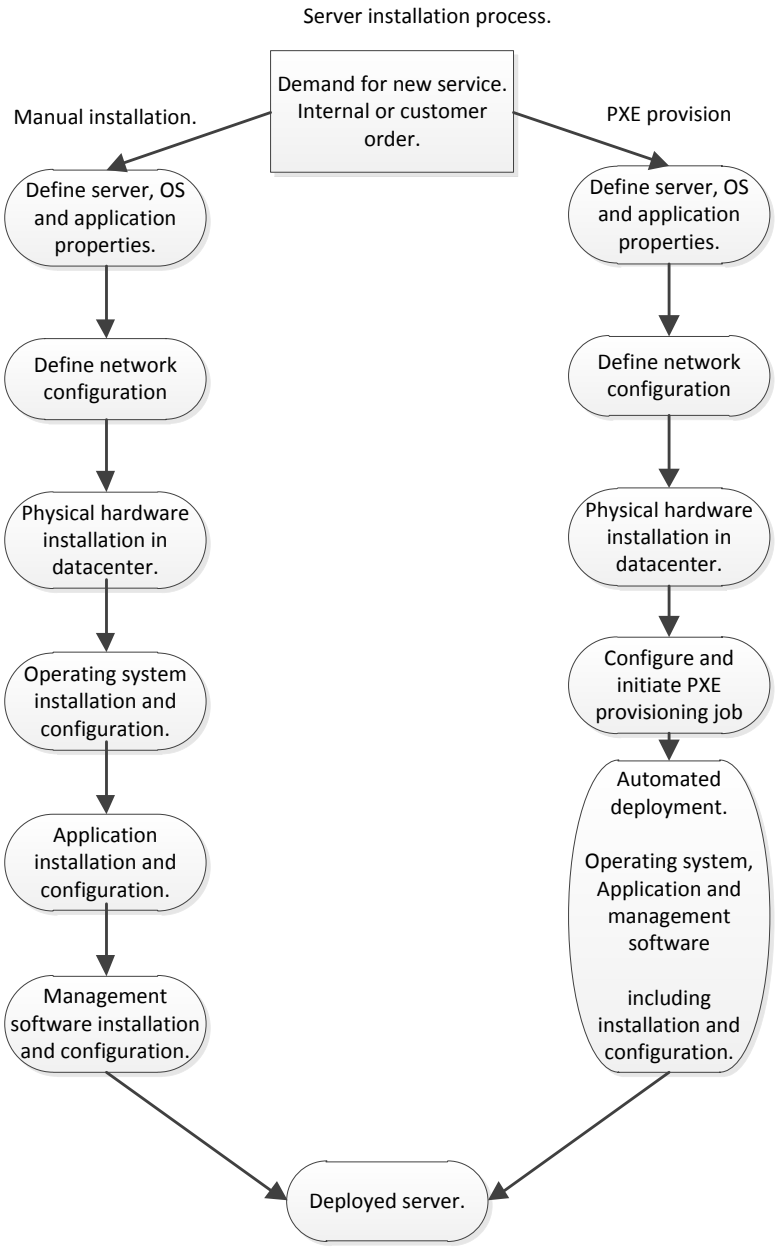


Figure 8. Process flow of the new server installation.

Figure 8 illustrates the steps which are necessary for a new server deployment. It describes what is different between manual installation process compares to PXE provisioning process which is done using the BladeLogic.

When new server is to be deployed every installation step takes certain amount of time. This time depends on what and how it was done. Table 1 shows examples of times which one single step can take.

Server Installation steps and times	Minutes
Network plan and IP addresses	30
Hardware installation	60
Operating system installation	35-60
Application installation	15-200
Management software installation	30
Total	170-380

Table 1. Installation times of the server components.

The manual server installation requires a certain amount of the time. Table 1 describes different steps and the average time which is required in each phase. Average time can change and this change depend speed of the server and the user behavior.

2.8 Server Configuration Parameters and Configuration Management

The provisioning software adds an additional possibility to manage and catalog servers and server properties. The managing server sees which server operating system version and updates have been installed. By comparing between updates one can define which are available and possible to install to the server. This helps to keep a server operating system updated. Change control is an important task in a server environment. Even if a server operating system version is the same all of the server life time applications and application configuration may change in time. Configuration and application changes without provisioning software are needed to do manually and make document changes to the server documentation card. Using provisioning

software all changes are updated automatically to the server database. This also gives a possibility to cancel changes made to the server. That is called a roll-back.

In a MSP server environment common username and password or common username database is required to allow server administrators to connect and manage servers. One common username and password is very a easy practice to deploy and use because all the servers have this combo in use. The problem is when one need to change the used password it is necessary to change the password for all the servers. In several situations this method is not acceptable and separate username and password are required. Provisioning software grants a possibility to change the password to all servers by making a password change where it is described which username password should be changed.

If there is a common database for usernames and passwords such as a lightweight directory access protocol (LDAP) or Microsoft AD (Active Directory) provisioning software can configure a server to use a pre-defined LDAP or AD server. If the LDAP or AD server IP address which is in use is changed for some reason the server configuration needs to be changed so that they can connect to a new LDAP or AD server IP address. Provisioning software can change LDAP or AD parameters to all of the servers instead of the administrators logging into each server and making all necessary configuration changes.

One of the common problems in the company is that they utilize a host file where the server IP addresses and domain names are configured instead of using the domain name servers (DNS). When the IP address of the server in a hosts file is changed or a new one is required hosts-file change is required to be done in all the servers. Provisioning software can be used to manage a hosts-file.

The previous chapters explained the basic functions and features of the BladeLogic. They also gave some background information of the environment where the BladeLogic is deployed. The next chapter goes more into depth as to what BladeLogic can do and how. It also describes more in details what is expected from BladeLogic.

3 PROVISIONING AND MANAGEMENT USING BLADELOGIC

One needs to make all the necessary configurations to the data center environment to support provisioning and configurations using BladeLogic. Also one should make a plan and make several test scenarios on how to test deployments and what modifications are needed and what are the modifications which need to be taken into consideration.

After completing this step one has to answer questions such as is the software tested suitable for the company? If it is then in what parts what are its limitations for its use and which deployment scenarios comply. This study tells how the provisioning software can be used. The provisioning software tests show to the company what are the savings in time and resources when using the provisioning software instead of the manual deployments and manual configuration.

Implementing a provisioned environment to the production environment needs a well thought test phase with detailed test scenarios and plans. The test environment can be installed and configured in the production environment. The current production systems should not be affected. Production environment settings are configured manually and they are not dependable on the provisioning software. Eventually when new servers and network configurations are configured using the provisioning software they do not require constant communication between the server and the provision software. Components in the production can be affected by changes using provision software and the changes need to be scheduled manually from the provisioning software.

3.1 Placement of BladeLogic Application in Network

The BladeLogic application location in a network is crucial. The application needs to have access to the servers which it manages. This point can be behind a firewall or even in another data center.

In Figure 9 are described the BladeLogic application components in the network with IP addresses of the company network. The application components are divided to the three physical servers. The firewall provides gate-

way to the IP packets to the Internet and company production networks. A firewall controls traffic and logs packets transmitted to the other networks. The BladeLogic application has a necessary access to the networks so that a RSCD agent can function properly. The RSCD agents have access to file server to access update

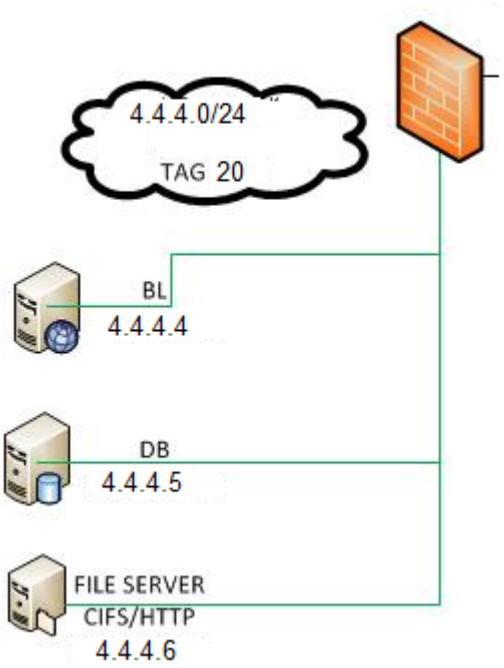


Figure 9. BladeLogic IP addresses.

If a direct connection between the BladeLogic application and a RSCD agent is not possible then the BladeLogic application component can communicate with a Network Shell (NSH) Proxy server which communicates directly to the RSCD agent (see Figure 10).

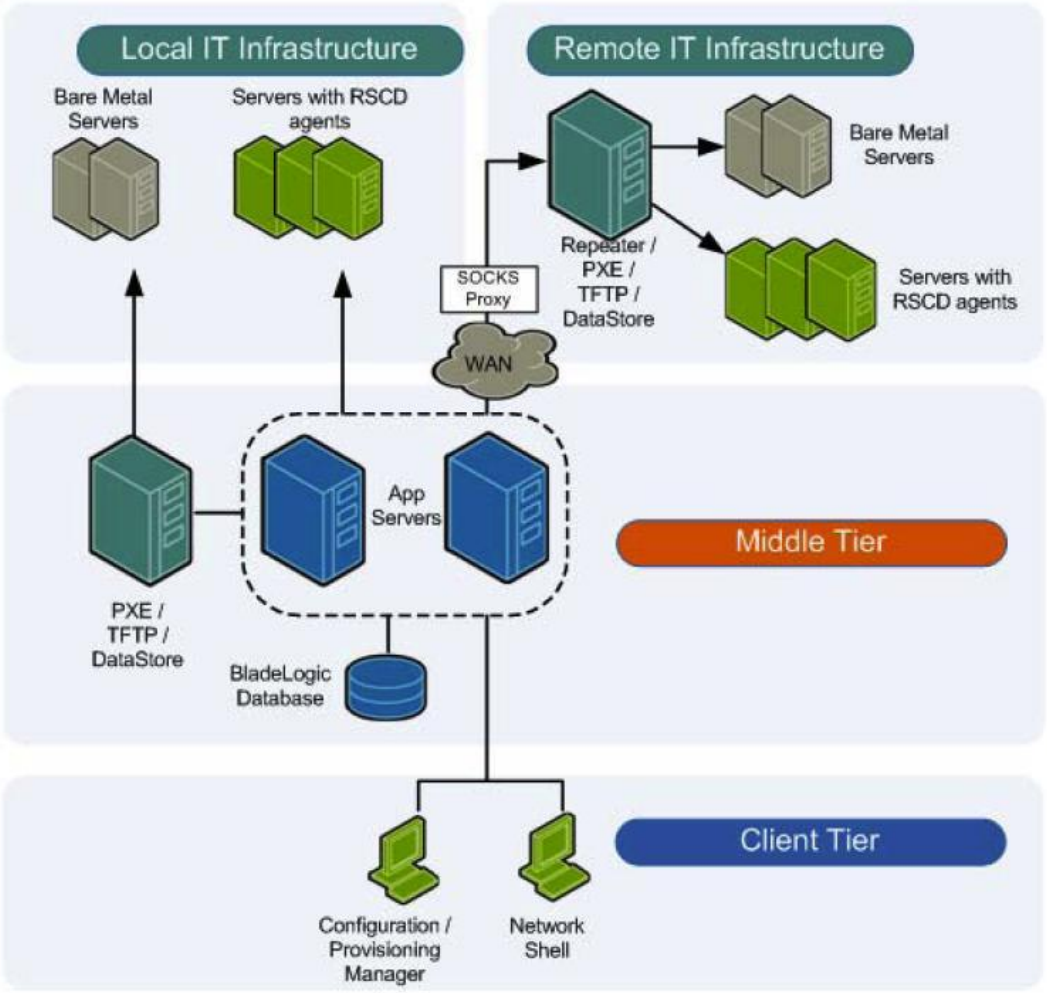


Figure 10. Network Shell Proxy Server Connectivity to Remote IT infrastructure [10]

Using a Network Shell (NSH) proxy server the BladeLogic application can manage servers that are located in places where a direct network connection between application server and a target server is not possible. It also manages authentication and traffic encryption between application servers and target servers. RSCD agent can connect to a file server using NSH proxy server.

3.2 Remote System Call Daemon Agent Deployment for Existing Servers

The first step to make servers to be managed using the BladeLogic managing software is to install the RSCD (Remote System Call Daemon) agent to

the server operating system. It includes a process which listens to TCP port 4750 where the BladeLogic application connects. [14]

The manual process requires users to log on to a every server and needs to transfer the RSCD agent installation packet to a server. Manual installation requires interaction during installation steps and removing the installation packet.

In order a RSCD agent to work properly in a target server, the user needs to provide sufficient privileges to the RSCD agent. In a Windows operating system the RSCD agent needs to have an administrator level privilege and in a Linux operating system it needs to have root level access.

The BladeLogic application provides automatic installation software for a RSCD agent. It is called BMC RSCD Agent Bulk Installer. This application provides method to distribute and install a RSCD agent simultaneously to multiple servers. It supports installing agents simultaneously to different type and a 32 and a 64 bit operating systems. During the selection of a server agent installation configuration parameters are needed to define the operating system. Different operating systems support only certain file transfer types and logon methods. Microsoft Windows supports natively CIFS (Common Internet File System) protocol. File transfers to the Linux operating system are done using SSH (Secure Shell) protocol.

The installation process of the RSCD agent to existing servers can be done manually or using automated installation. The manual process is a method for a few servers but when the number of the servers becomes very large, an automatic process lowers down the installation time per server (see Figure 11).

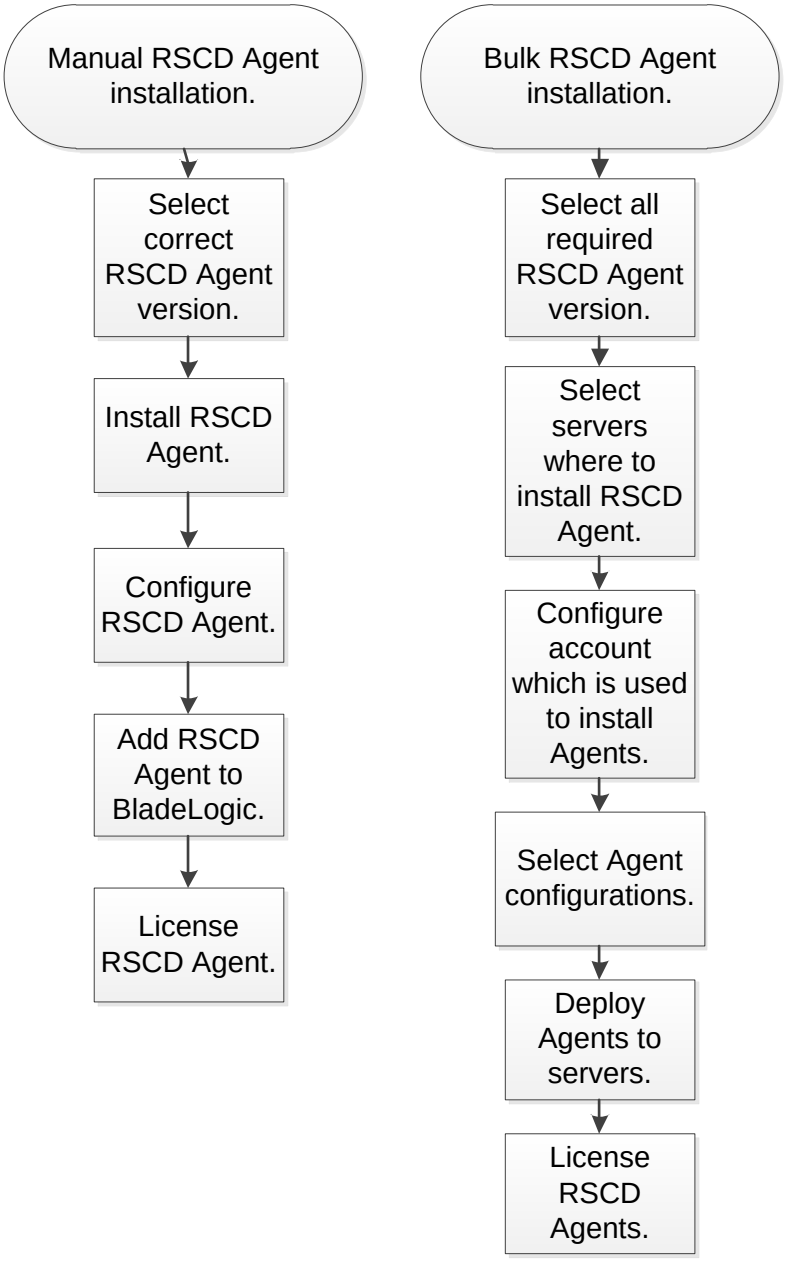


Figure 11. RSCD Agent installation flow.

Adding a server to installation process can be selected by using three different methods: Selecting a server manually using automated discovery setting or importing the list of the servers. A manual server selection requires the user to set all required parameters by hand and do this for all the servers where the agent is to be installed. The user needs to select a correct predefined installation script which the agent installer can use and to select a correct username and password combination which have enough privileges in the operating system to perform installation. Automatic discovery selection

requires the user to give an IP address range or IP subnet which the agent installer scans for the server where the agent is to be installed. The scan recognizes the operating system type and bit version.

The Bulk Installer provides functions that add a server after the agent installation to the BladeLogic inventory. When logging in to Bulk Installer it offers “Online” and “Offline” –method. Using “Online” it adds the agent to the inventory after the RSCD agent is successfully installed. Offline method requires that a target server is manually added to the BladeLogic inventory. The Bulk Installer allows automatic agent licensing. After the RSCD agent is installed the user can license target servers.

BMC offers agent installation packages to different operating systems. There is a separate installation package for a 32 bit Linux systems and a 64 bit installation package for a 64 bit Linux systems. For Windows servers there is a 32 bit installation package for a 32 bit Windows servers and a 64 bit installation package for a 64 bit Windows server installations.

The installation process is similar between a 32 and a 64 bit version of the operating system. For Windows agent installation the BMC offers and option to use a predefined configuration file. Using this file user does not need to provide any input during the installation process. Proper configuration parameters require settings where ACL (Access Control List) is defined. In this ACL the RSCD agent allows certain BladeLogic application to access RSCD agent and gives the required privileges to the BladeLogic application and its users.

3.3 BladeLogic Server Inventory Function

The BladeLogic offers a hierarchical system to manage servers. Before any management actions to a server can be done they must be added to the system. The added servers are included to a Servers folder or some other sub-sequential subfolder. The structural form of the servers can be modified to match the needs of the organization.

The BladeLogic offers two kinds of groups, where the servers can be located. The first one is a basic server group a where a server can be added

manually. If there are multiple basic server groups one single server can be added into all of the groups. Server objects and basic server groups can be copied or moved. The second server group type is a Smart Server Group. In a Smart Server Group servers are added automatically using different conditions (see Figure 12).

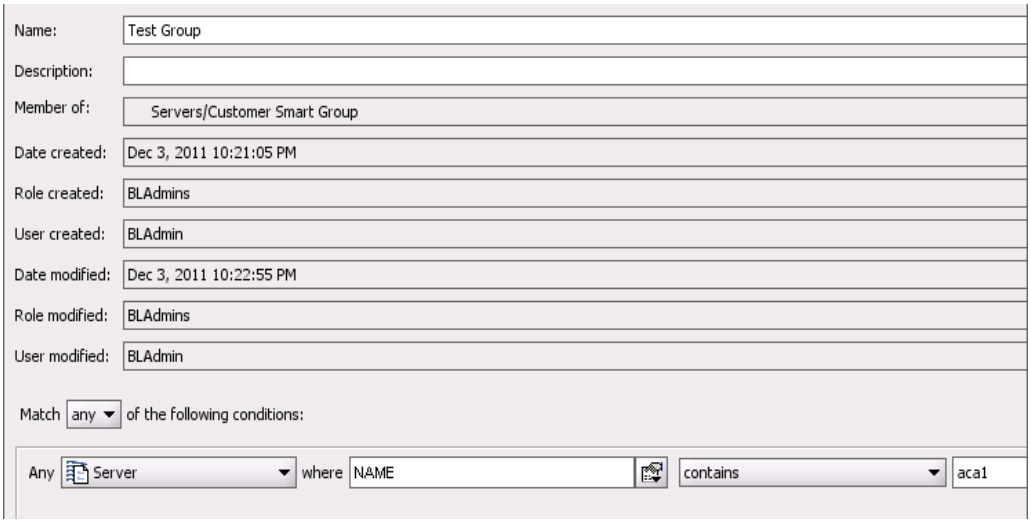


Figure 12. Server inventory configuration.

Moving a server to another group transfers the server object from the source group to a target group. Copying a server object to another group leaves the server object to a source group. Deleting the server group is allowed. Server objects cannot be deleted. If a server should be removed from the BladeLogic it is done using a decommissioning process. BladeLogic best practice recommends that if new server is commissioned using same name the old server object should be decommissioned not only renamed.

A server object from a Smart Server Group can only be copied. It is not possible to add manually new servers using the copy process to a Smart Server Group. Smart Server Group itself can be moved and copied. Group names can be renamed freely and it does not affect server objects inside group.

3.4 Managing Operating System and Application Updates with BladeLogic

Updating a managed server operating system and applications require the BladeLogic application to know what new operating system upgrades and application versions are available. The BladeLogic application can be used to download software updates from software manufacturers. The problem is that software manufacturers do not explicitly release new software update information what the BladeLogic application could use. The BMC BladeLogic application uses service provided by Shavlik Technologies who provide an XML (Extensible Markup Language) file where the update packages are described. The BladeLogic downloads this file periodically and processes its contents to get the information of the released software update packages. Using this information the BladeLogic can be scheduled to download software packages at a selected time (see Figure 13).

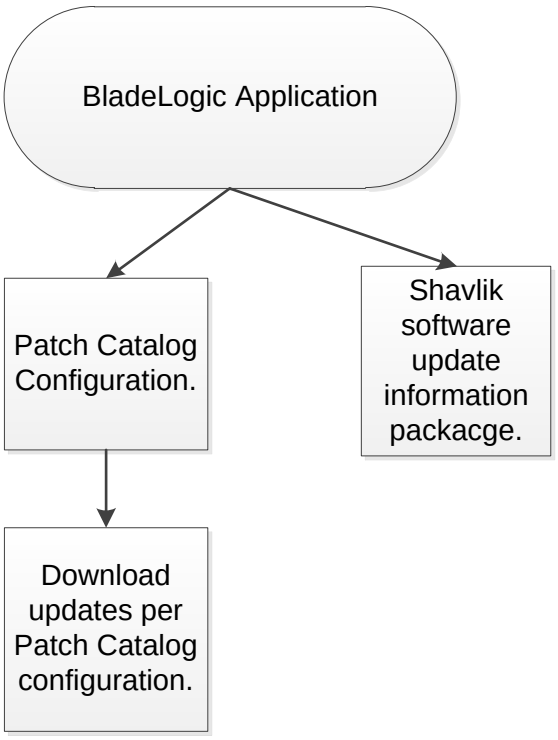


Figure 13. New software patches download schema.

The Shavlik not only publishes new update information updates are also tested and confirmed to work before the update file is updated. BladeLogic's best practice suggests scheduling periodic downloads of the XML-file from Shavlik.

Software manufacturers release packages to be downloaded using Internet connection. Some manufactures provide all software packages for free. Those packages BladeLogic can download using its configured Internet connection. Several software manufactures require a support contract to allow users to download software packages. Usually download privileges are provided to a username. For example Red Hat requires a valid support contract and username and password which are linked to the support contract that allows downloading of the patches. This username can be configured to the BladeLogic which allows downloading the Red Hat patches.

The BladeLogic application only downloads packages which are requested. Selecting packages which are requested to download, the user needs to configure a proper Patch Catalog. In a Patch Catalog it is configured how update packages are downloaded to the File server. Options are Direct Download from a Software manufacture also known as a Vendor. File Repository is an alternate method where the user downloads a file from a Software manufacturer.

If BladeLogic is requested to download update packages from a software manufacturer the BladeLogic requires that one selects which updates are downloaded. Single update packages are not selected. The BladeLogic offers a predefined software product list. These are applications and operating systems which are selected to the BladeLogic and which can be downloaded. To download updated components the user can manually start the software package download process from software manufacturers. An other option is to make a schedule which for example periodically downloads new and updated components.

When configuring a Patch Catalog for the Microsoft Windows operating system or its applications they must be selected in patch catalog configuration. This is when the software is selected that BladeLogic downloads those update packages (see Figure 14).

Figure 14. Selecting applications in Patch Catalog.

After a user has configured a Patch Catalog and selected which operating system versions and applications are supposed to be updated in next maintenance break, BladeLogic can be scheduled to download application and operating system updates. These downloaded files are put to the file server and information of the downloaded files is inserted in the BladeLogic database (see Figure 15).

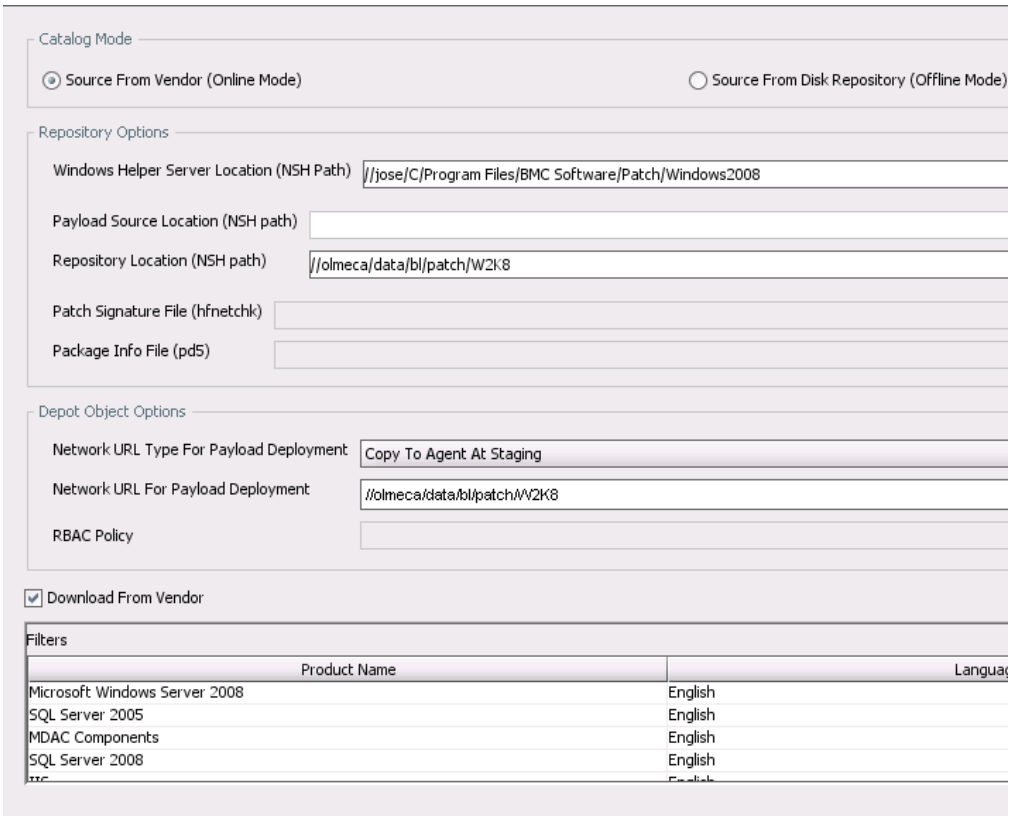


Figure 15. Patch catalog configuration.

In some cases a server requires an update as soon as the software manufacturer releases the update packet or update packet is custom made not available for public download. After an update packet is downloaded it must be imported to the BladeLogic application.

After importing an update package to the BladeLogic it can be installed to the managed servers. The procedure to install update package to a remote server requires that in BladeLogic the downloaded software update package needs to be made into a installable package form. In an import process several parameters such as installation parameters and update package version are required to be set. If the version number is not used by importer it is possible that importer can use some other parameter recommended by software manufacturer. In some cases if the package is to be removed uninstall parameters are recommended by the BMC BladeLogic best practices. [12]

Update packages are deployed using a normal software deployment process. In this deployment the server is scanned for the required patches. Deployment takes place by making a new deployment process and selecting a target server or servers. The last step is to schedule when the deployment process starts. A server is restarted or reconfigured in a way as required by the software update package.

3.5 Microsoft Windows Operating System Update Using BladeLogic

Updating Microsoft Windows servers is a process which requires several mandatory configurations and settings. First of all a suitable repository where the BladeLogic application can put update packages must be defined. Once this has been done the user does not need to set this again.

The first step is to create a new Windows update job (see Figure 16). Its first step is the analyze job. The analyze job scans a server and makes a catalog of the installed programs and the current versions. The analyze job calls a RSCD agent to perform the scan to select a server and to return results to the analyze job. This analyze job is done to the selected servers which the

user selects to perform the analyze job. The results from the analyze job can be different to all selected servers. The BladeLogic makes individual results from all scanned servers. During a new Windows patching job configuration and after making analysis, the user can select the type of the updates, which are included in the analysis. Those selections affect all of the servers where this patching job is pointed.

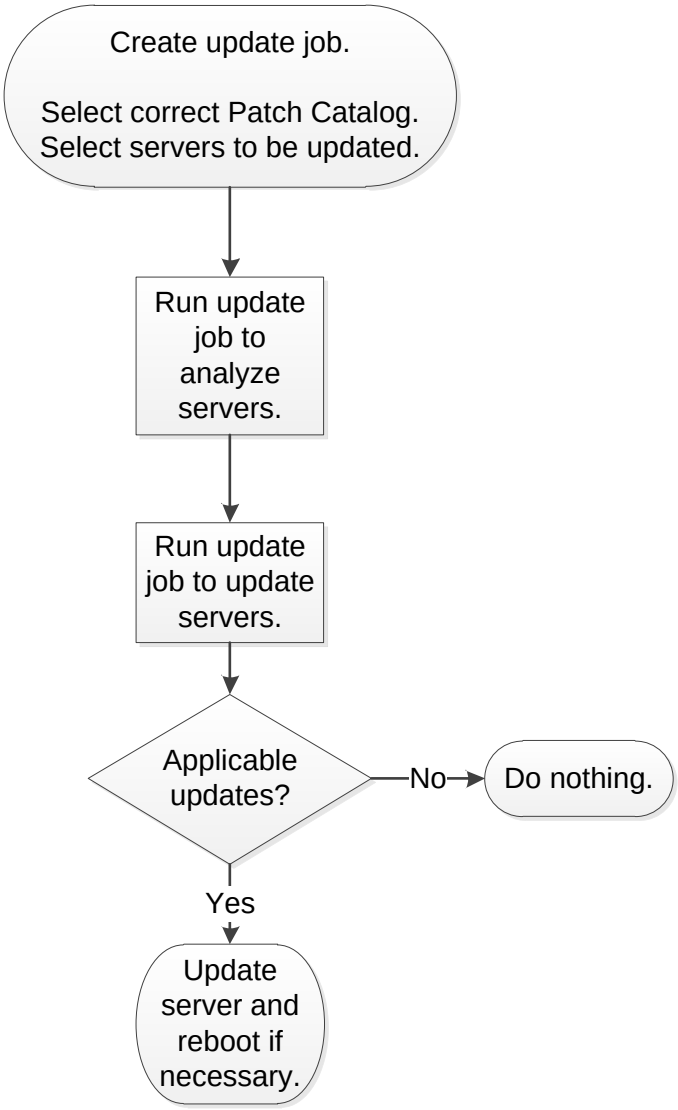


Figure 16. Update job flow.

When the analyze job is done, the server remediate job can be started. The patch deployment job to the servers is known as remediation. Before that the user can verify scan results and view details of the update packages which

can be installed to a server or servers. Using these results view updates can be deselected which are not to be installed. Every server selected in the analyze job has its own section in the results. The user can browse inside results and view if the analyze job was successful or if it failed and if it was successful BladeLogic produces a list of the updates which are available to install. The updates can be manipulated so that in the installation job the update is installed or ignored. Remediation job calls the RSCD agent of the server and controls it to do required tasks (see Figure 17).

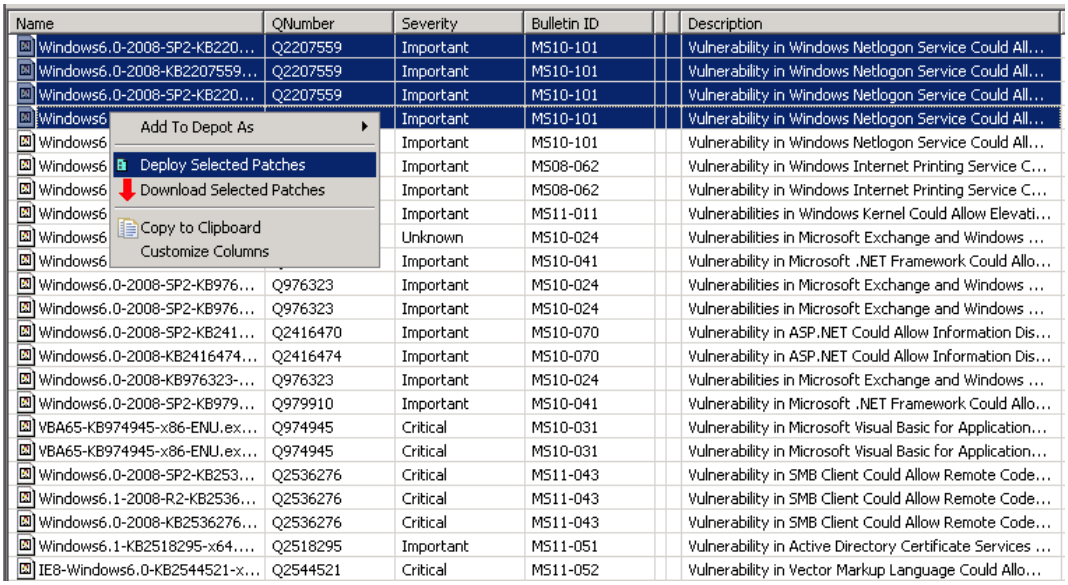


Figure 17. Selecting updates which are to be installed on a target server.

If the analyze job results are successful and there are no updates available for the server it can happen for two reasons. The first reason is that there are no updates available. This can happen for a few reasons. One of them is that Windows Update service is running in a server and it updates the operating system automatically or Server Administrator has manually updated the server the results in the BladeLogic finding no applicable updates. Another reason is that the Patch Catalog does not have information of the newer update packages.

The next step in a Windows patching job can be configured after the analyze job is finished and its results are correct and allows proceeding with patching. In remediation the user must configure such settings as time when the software updates are installed and how to react if a server restart request is made by patches during the update process. BladeLogic offers several op-

tions to the patching procedure. The first is a stage process. This is when the updates are transferred from the file server to the local disk of the server. This must be done prior to the actual patch installation. When the transfer is completed it is not required that the installation of patches starts immediately. Patches can be, for example, transferred in a time window when the network load is minimal and interrupts to the business traffic and impact to other processes are minimal. When the scheduled time is triggered the BladeLogic application calls the RSCD agent which then starts transferring selected update packages to the server.

The second phase is the simulation. The simulation in a patching job is optional. It determines if there is enough disk space on a target server. The patches can be very large and consume a lot of disk space. Usually patches are in a compressed form and when they are installed, the patches are uncompressed. The original compressed file and the uncompressed file both exist at the same time in a target server. This consumes even more disk space and there is a possibility that this can lead to disk full situation and this situation usually halts the operating system and the patch installation fails. The patches which are half installed can compromise operating system stability and prevent it from working properly even when the disk full situation is resolved.

The third process step of the patch installation is the commit phase. In that phase the patches are installed. Some of the patches require server restart after being installed. The best practice to server restart is to select the BladeLogic to ignore the restart request from the patch and to continue patching until all patches are installed.

When the commit process is done a server should be restarted if necessary. A server can be restarted after every patch install which requires restart. This can delay the commit process very much if for example the number of patches is very large. The final step in commit process is to remove the update packages from a server.

The BladeLogic supports the undo feature in patch deployments for installed packages. Even though it is supported BMC does not recommend using it. The reason is that the undo feature depends on the features of every operat-

ing system which are unique for each operating system. Using the undo feature can break a target server operating system. [12]

The patch update results can be viewed from the BladeLogic console. Examining the patch update process job results of the patch update is available. The job results are shown and they are divided into two classes successful and failed. In the classes the servers and results are viewed by selecting the desired servers. In a successful case the user can view how many and which update packages were installed. In a failed case the BladeLogic shows what went wrong in a patch update.

3.6 Updating Procedure of Red Hat Linux in BladeLogic

Using a patch update job to update Red Hat Linux operating system is almost identical to the Microsoft Windows patch update process. An exception is that Shavlik Technologies do not provide information of the newest update packages to the Red Hat Linux. Update packages can be downloaded directly from the Red Hat or they can be downloaded separately to a place where the BladeLogic application can transfer the update packages to the file server.

The update package method works when the Red Hat Linux patch catalog has been configured. BladeLogic then proceeds to get all the packages from the Red Hat Network or from a disk repository and places them to the file server. Red Hat Linux includes multiple software packages and their updates are provided in a Linux distribution. The BladeLogic application downloads all available files and when there are updates available it compares which it has in the file server and only downloads updated packages not already located in a file server (see Figure 18). The Red Hat Linux Patch Catalog can be configured to periodically check the newest update packages available and download them automatically.

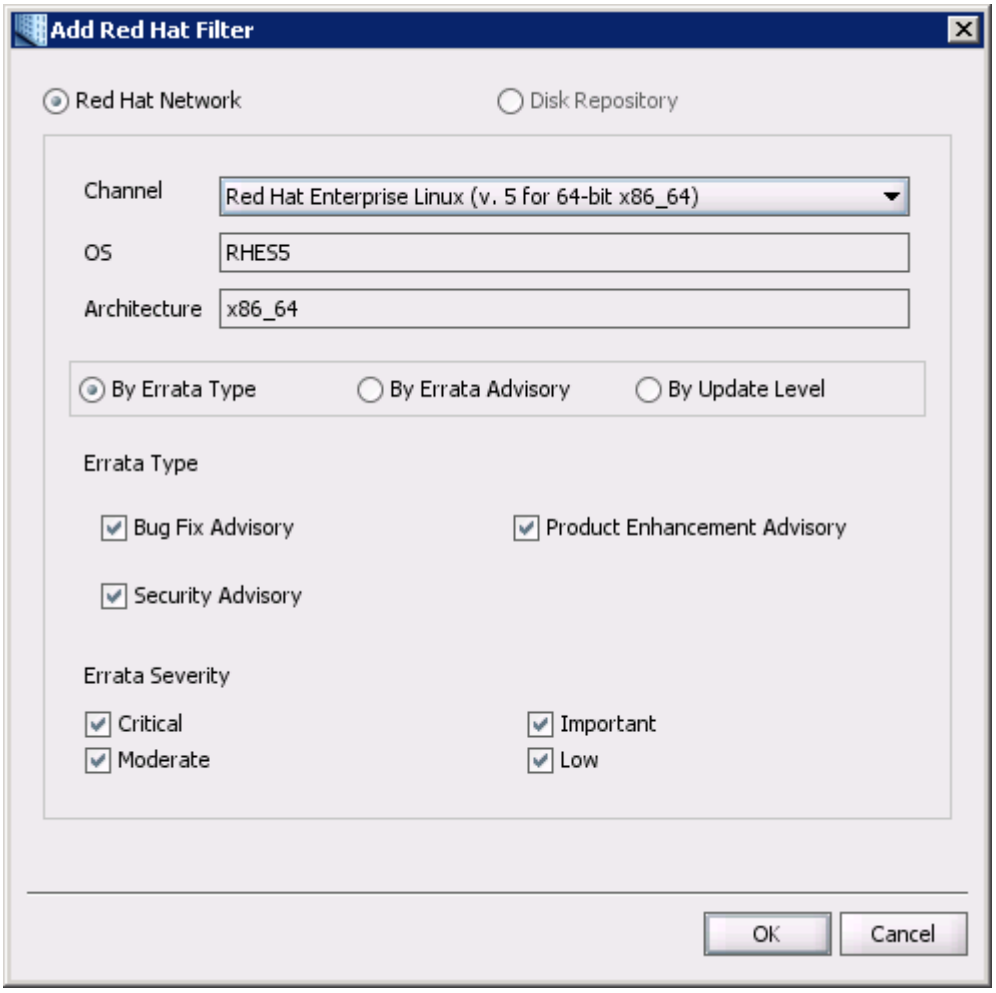


Figure 18. Linux update selection.

Updating Red Hat Linux server starts with creating analyze job in the BladeLogic. In the analyze process BladeLogic scans the servers for installed versions of operating system files and applications. When the scan is completed it compares the results to the update packages which are available through a patch catalog. The user can view the scan results and examine which updates are available to a server. Single and multiple updates can be selected to be installed from the analyze results.

Remediation job wizard is performed by selecting successfully scanned servers. In a remediation job wizard is configured how different phases are scheduled and what are the actions if patches which is installed request the server restart.

After the remediation job has been configured and the wizard is closed the user can examine tasks in progress windows in the BladeLogic console. If the remediation job is scheduled to run immediately user will see remediation job in progress in a tasks in progress window. By selecting and opening that job it is possible to view the progress of the job in real time. If the job is scheduled in multiple parts and scheduled to run in separate time window the user can view the job in a scheduled tasks windows when the scheduled job is triggered it moves to the tasks in the progress window.

When the remediation job is completed the user can view results of the remediation job. The results are shown in two classes: failed and successful. In a failed class are completely failed remediation tasks. The reason to the failure is shown under a server. In the successful class are the servers where the stage phase was able to transfer update packages and at least some of the packages were installed to the server by the RSCD agent.

Previously completed remediation jobs can be rerun. This could be beneficial in a situation where a patch update process has failed for some reason. Problems could be fixed and the servers are ready for update package installation. The user simply selects the remediation job in the BladeLogic console and selects “Execute Against”. The BladeLogic will then provide a list of the servers where the job was previously executed. Then one can select to execute a previously completed job against the servers or select new servers. Using this “Execute Against” method one can run multiple times to upgrade multiple servers if is not possible to upgrade servers simultaneously (see Figure 19).

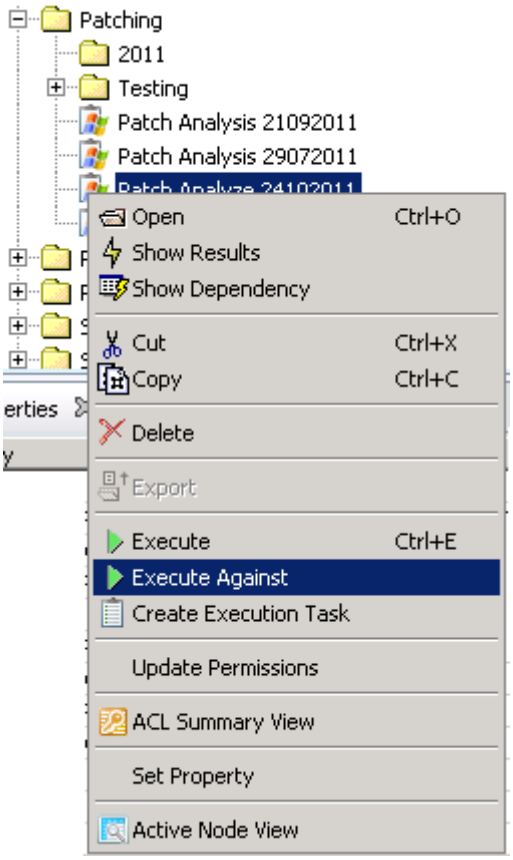


Figure 19. Patch execution after analysis job.

BladeLogic starts the job and the user can view its status. BladeLogic categorizes jobs in a categories listed by the date. If one job is run multiple times then in job results there are in many date entries and under the date entries the user can view the results of every job.

3.7 Server Provisioning Using BladeLogic PXE Installation Process

Pre-boot Execution Environment (PXE) provisioning is a method to provide installation of the operating system to a bare metal target machine. The target machine is a physical server. A server can be a new one without operating system or an existing server where the operating system is going to be reinstalled. The network interface card needs to have the PXE properties to use PXE provisioning.

BladeLogic supports Windows and Linux installations using the PXE. The PXE uses a TCP/IP protocol to establish a connection to services such as DHCP TFTP and file services such as CIFS and HTTP. The network interface card uses the PXE to receive installation instructions and files instead of using the floppy disks CD-ROM (Compact Disc – Read Only Media) and DVD (Digital Versatile Disk).

BladeLogic which is used to perform the bare metal provisioning needs to have proper configuration and the configuration includes boot descriptions to the PXE network cards. PXE provision requires the boot images deployed to PXE boot processes. A separate boot image is required for Linux systems. One Linux PXE boot image works with different Linux versions. Windows boot image needs to be a different one for a 32 bit and a 64 bit operating system.

A process where the operating system is provisioned to the bare metal server requires multiple independent steps. Many of the steps are done automatically by the BladeLogic but few configurations must be done manually. Manual interactions are the configurations of the BladeLogic server.

A target server MAC address is essential information and it must be acquired before provisioning job can be configured. It can be received from several places like printed sticker or from a server console (see Figure 20). If there are no PXE information in the start-up screen there is a possibility that the PXE is not enabled or the server does not support PXE booting.

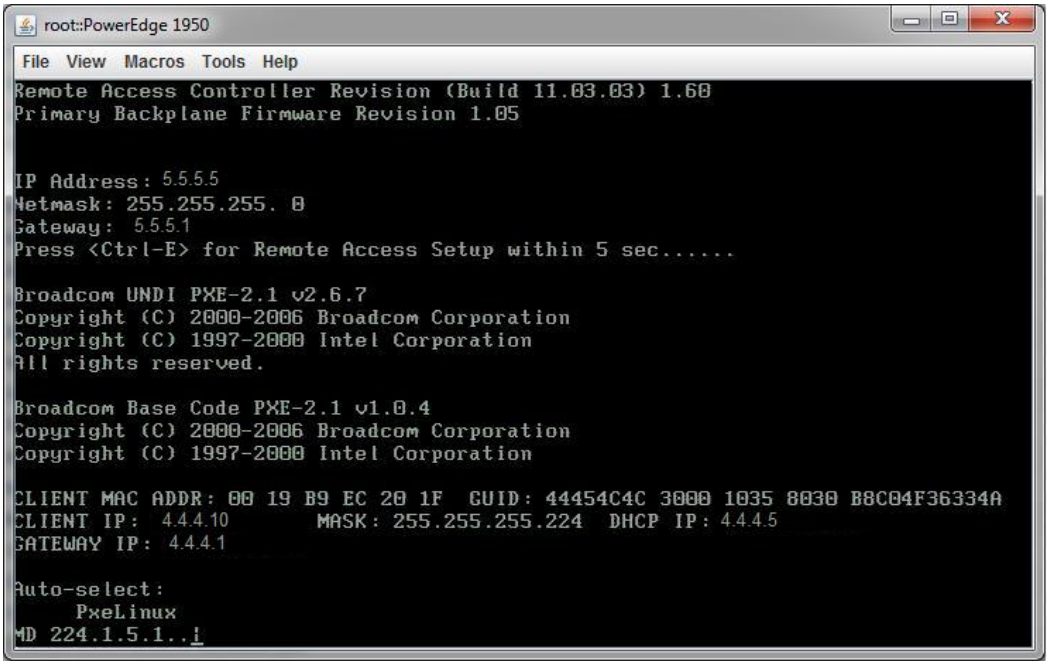


Figure 20. PXE boot example.

When a MAC address is resolved and necessary server parameters, such as operating system version and type is known a provision job wizard can be launched. In a provision job wizard the MAC address of the server is provided in xx-xx-xx-xx-xx-xx format where xx is the corresponding octet of the MAC address. Description is the name of the server. The name is how the BladeLogic application knows the server and connects to it. A server name in the operating system can be different.

In provisioning one must select a correct boot image based on what is the number of bits of the server operating system. By using the architecture setting BladeLogic knows which version of the operating system should be provisioned. If a user enters incorrect parameters to the provisioning wizard and finishes the wizard provisioning job it must be erased and a new provisioning job wizard was launched and correct parameters set (see Figure 21).

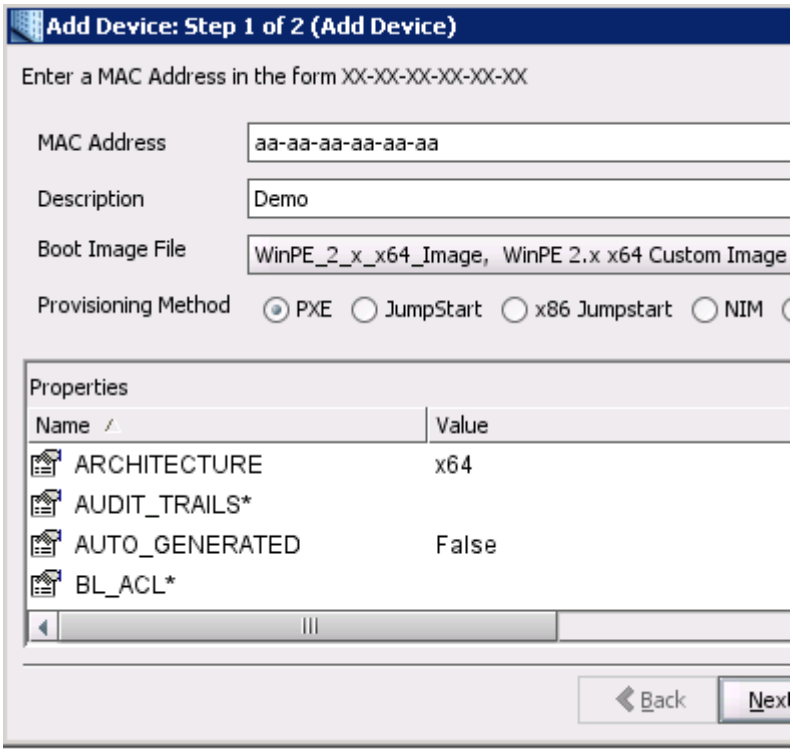


Figure 21. Creating PXE provisioning job.

When the provisioning job wizard is finished the provisioning job can be started. After the provisioning job has been started a target server can be booted using the PXE. All steps from hardware installation to the provisioning job wizard and restart start are included in step number 1 (see figure 22). During a server boot up process PXE is launched and it sends a broadcast message to request IP address using DHCP (Step 2). The DHCP server application is located in the server named DB and it responds with an IP address from the DHCP pool. A DHCP address is given from a predefined network range. The PXE server application is in the BladeLogic server and it also responds to a broadcast message send by the PXE client and in that respond the PXE server informs the PXE client that it is the PXE server. (Step 3.) A target server contacts the PXE server. (Step 4). The PXE server makes a query to the database using a target server MAC address. The database checks parameters such as boot image name and returns the parameters to the PXE server. A boot image name is predefined in the boot images of the BladeLogic and selected by the user who does the provisioning job (Step 5). The database server where the PXE server service is located delivers boot parameters to the target server bootstrap program. The

PXE server also delivers the IP address of the TFTP server (Step 6). Now with necessary information to a target server to boot it starts the booting process and when the booting is done it contacts the BladeLogic application server (Step 7). The application server checks the information from the database server. Information is requested using a target server MAC address (Step 8). With this information application server delivers that to a target server. Information contains all the data defined in a system package (Step 9). Now the target server has all the information to proceed with provisioning. A target server knows that the file server is an IP address and how to receive the operating system files. If a Windows platform is provisioned the target server receives correct operating system files using CIFS. Linux environment can receive files using a HTTP protocol. (Step 10). After the target server provision is completed the RSCD agent can be installed. If in the provisioning job it was selected that the RSCD agent should be automatically installed after operating system install BladeLogic transfer the RSCD agent files to a target server and performs non-interactive installation. A target server knows the location of the RSCD agent and requests that from the file server. With a RSCD agent installation package a target server gets the configuration parameters for a RSCD agent installation. Using the predefined configuration parameters the RSCD agent can control a target server and allow privileged users to perform management operations. Without a RSCD agent the BladeLogic application cannot access the provisioned server and has no information if the provisioning job was completed successfully. If the RSCD agent is not installed the BladeLogic application knows only that if the target server has requested operating system files from a file server but does not know the status of the further steps (Step 11). If the RSCD agent was installed to the server then the provisioning job can perform additional management tasks to a target server after operating system has been provisioned. The additional management tasks can include updating the operating system to a desired level or to install and configure all necessary applications (Step 12).

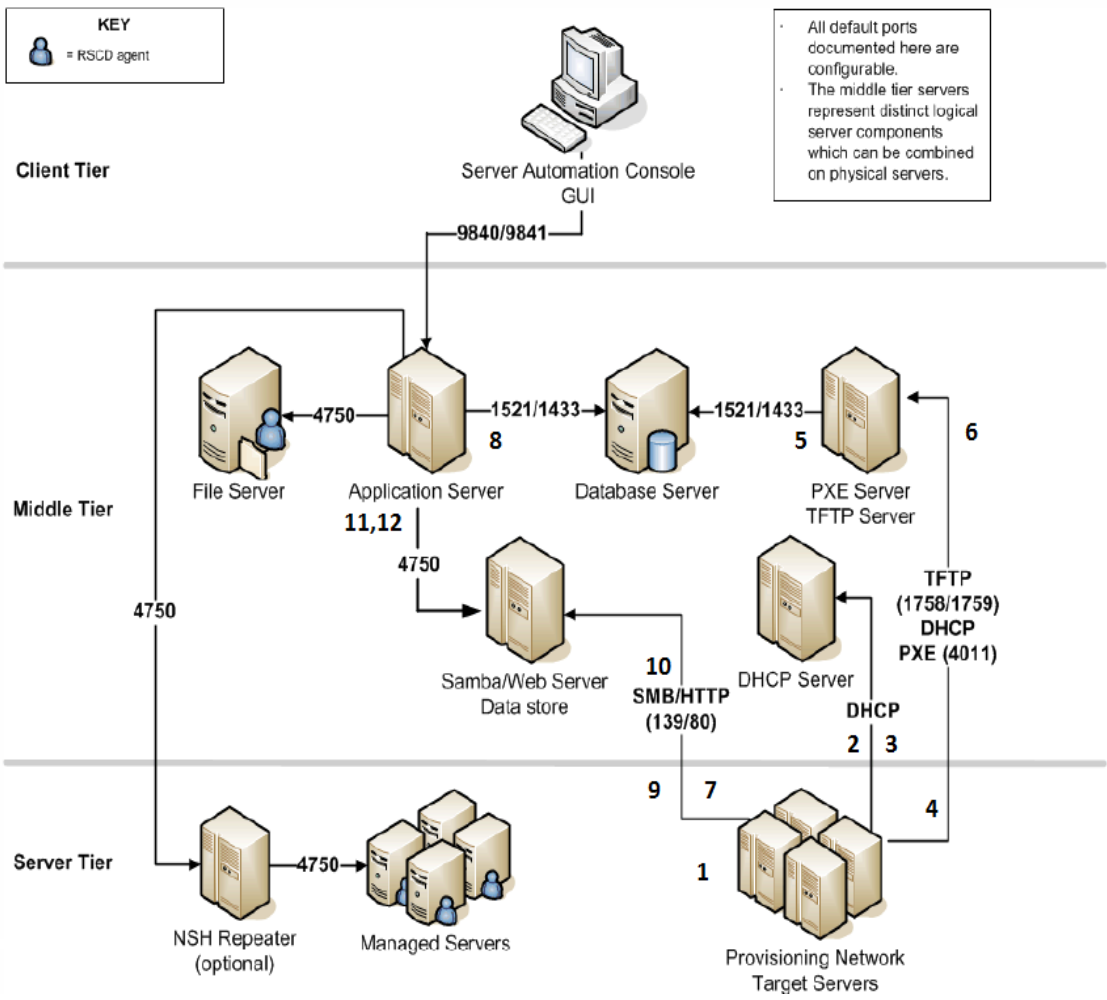


Figure 22. Detailed PXE provisioning job steps. [16]

Provisioning jobs using the PXE provisioning allows multiple simultaneous provisioning jobs with a combination of different type and versions of the operating systems. All provisioning jobs are independent jobs. Failed and successful provisioning jobs are saved and servers can be provisioned again by using previously made provisioning job configurations.

A failed provisioning job requires configuration changes to the provisioning job configuration if there were incorrect parameters. If the provisioning job fails before the BladeLogic application approves that it is complete the whole provisioning job needs to be removed and a server object to be removed from the provision job deploy folder. The reason for that is that BladeLogic does not allow a new provisioning job to restart with a same name unless the provision is completed successfully. This limitation also applies to failed provisions.

The provisioning job wizard requires a network interface which it uses to receive operating system files from a file server. The BladeLogic application and the provisioning job cannot control how the operating system boot image recognizes network interfaces or how the provisioned operating system recognizes network interfaces.

3.8 Provisioning New Server Using iDRAC Module

To provision a new server using the Dell Computers iDRAC the target server iDRAC must be known to the BladeLogic application. Only the Microsoft Windows server operating systems are supported by the iDRAC provisioning. iDRAC devices can be automatically discovered or manually added to BladeLogic (see Figure 23). The BladeLogic application needs to have a route to the device correct username password Windows ISO (International Organization for Standardization) image and iDRAC MAC address which is used to identify iDRAC in BladeLogic. If there is a firewall between the BladeLogic and iDRAC traffic through TCP port 443 must be allowed in a firewall.

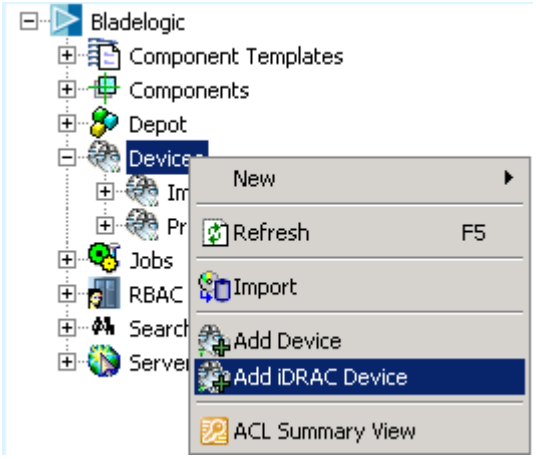


Figure 23. Adding iDRAC device to BladeLogic.

After the iDRAC device has been manually added to BladeLogic it needs to have files to proceed with provisioning. If device drivers are needed for the provisioning driver files can be send to a iDRAC. This happens by selecting the iDRAC device and selecting “Copy Drivers to Data Store”. This opens

the wizard which requires information where the correct drivers are located in the file server. After the wizard is finished BladeLogic sends drivers to the iDRAC. Before provisioning an iDRAC operating system ISO image can be transferred to the iDRAC. This is an optional phase if booting from a iDRAC was requested. Transferring the ISO image to an iDRAC is done by selecting a iDRAC device in the BladeLogic console and selecting the “Stage ISO to vFlash” option. This launches a wizard where the correct ISO image is located and after the wizard has been finished ISO image is sent to the iDRAC.

Automatically discovered iDRAC devices need to be known by BladeLogic before they are added to the BladeLogic inventory. This requires modifications to the idrac-config.xml file. In this file the iDRAC service tag username and password are set. iDRAC devices receive a correct IP address from the DHCP server. This IP address must have an allowed connection to the BladeLogic application.

The provisioning job is launched as a normal Windows based provisioning job. In the system package properties the “DATA_STORE” definition must be set so that it defines the property where the operating system installation files for the iDRAC device are located. Finally one must provide configuration information for the iDRAC panel so that booting is done using the ISO file from network or ISO file which is located in inside iDRAC vFlash. Now the provisioning job can be launched.

3.9 Deploying New Software to Target Servers Using BladeLogic

The BladeLogic application can be used to install software components remotely to the servers. Installation processes are unattended tasks which do not require any interaction from a user. If the application requires configuration files, they can be embedded to the installation packages or they can be deployed after installation using for example the BladeLogic’s BLPackage deployment process for configuration changes.

A different operating system type supports different application packages. BladeLogic supports several software package types for operating systems. The Red Hat Linux supports only the RPM (Repository Package Manager)

type of software package. The Microsoft Windows operating system supports MSI (Windows Installer) packages and InstallShield packages.

The deployed software needs to be added to the BladeLogic's depot. The depot section is a collection of the folders customizable by the user. The depot also supports a basic folder group type and a smart folder group type. To add a software package to a depot the user should select a folder where the package should be added. Then user should select a correct package type (see Figure 24).

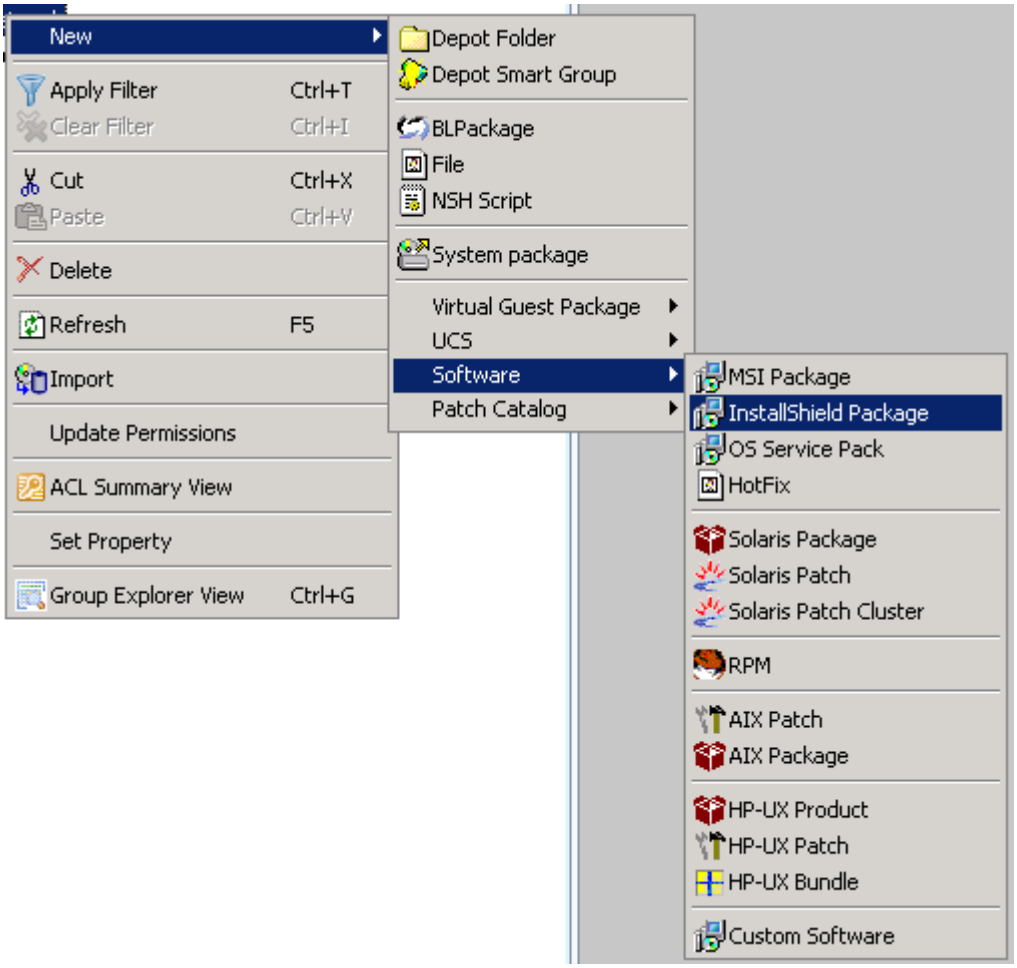


Figure 24. Creating deployable software package.

In the BladeLogic application the BMC provides the BLPackage which is an object including combined server objects, a software package and a XML file. These have all necessary information on how to process the contents of the BLPackage and install software. A BLPackage can be made using sev-

eral different methods. First a BLPackage requires file objects or a result of the server audit. For package placement in a target servers the BLPackage requires object information from live host depot snapshot or object which is located in server component.

A BLPackage has a restriction that it can only contain objects which are designed to Windows environment or Linux environment. Windows objects are: applications, COM+/MTS configuration files, event logs, files, directories, hotfixes, groups, users, metabase objects, registry values, security settings, services and external commands. Linux BLPackage can contain only configuration files directories RPMs daemons processes users groups and external commands. [14,414]

3.10 Using BladeLogic to Manage Server Configurations

The BladeLogic application can be used to make configuration changes to the servers. All changes made by BladeLogic are auditioned and logged. All changes are reversible with certain restrictions. BladeLogic can be used to make configuration changes to servers by using a server live view. A live view provides a view of the active configuration software and active state of the server. Servers can be managed individually by using this tool. Using live view BladeLogic refreshes the server status and state and displays the correct information. After the change is made to a server using live view the change can be made as a BLPackage and deployed to other servers (see Figure 25).

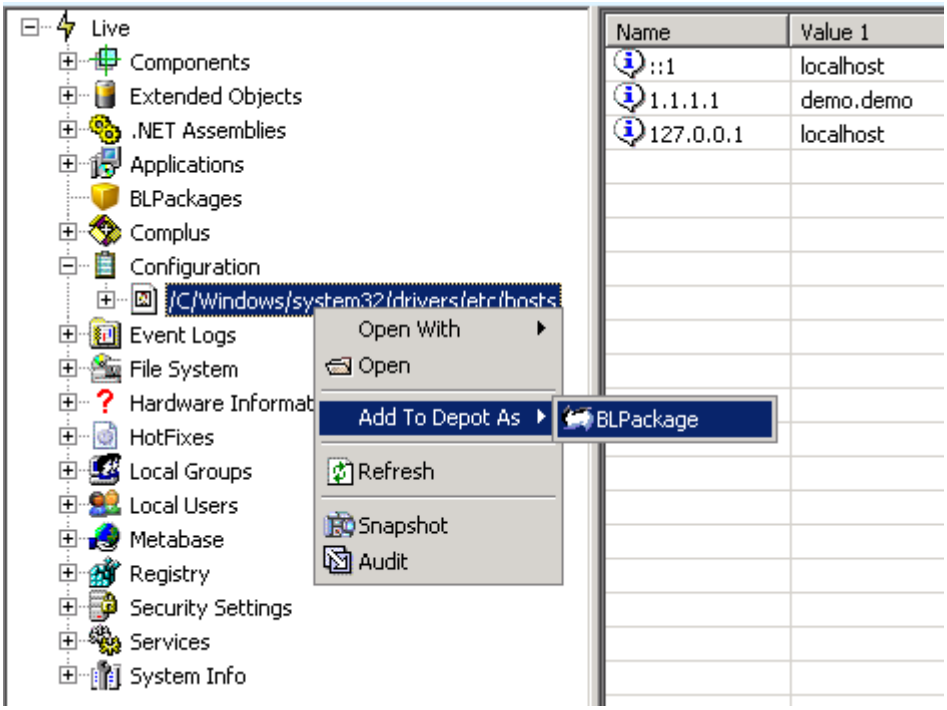


Figure 25. Creating configuration change package.

When a configuration is selected and it is made as a BLPackage it launches a wizard which requests a name of the package and several other parameters such as objects type it should use to collect the selected data. When the wizard is finished a BLPackage is placed on the selected folder. This BLPackage can then be used to make configuration changes to a selected group of servers. Server configuration objects deployed can be reversed.

The final step in a configuration change is that the changes are taken into use. Usually this requires a service or a daemon restart at the target server. BladeLogic provides a function that can stop and start services. If a software application needs to be restarted after configuration change it can be done under server view of the target server (see Figure 26). BladeLogic does not allow stopping services which are core services of the target server. Those services affect server functions and without them a target server usually becomes unusable.

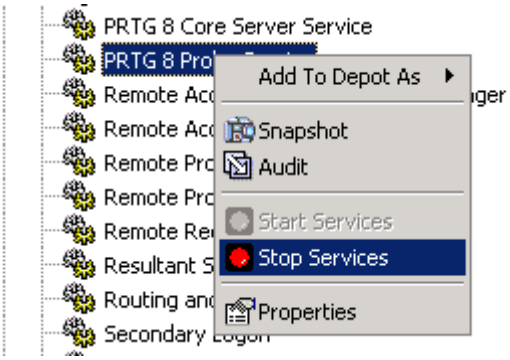


Figure 26. Stopping service using BladeLogic console.

For different configuration objects and object versions BladeLogic offers versioning. This method has a major and a minor version numbering scheme for objects. Versioning provides visualization for the user to use a correct object for deployment. Comparing version numbers to the deployed objects in servers which are available in BladeLogic a user can make decisions of the deployment. Version numbering is done by using positive integer numbers.

This chapter provided detailed information and some features of the BladeLogic application. It also shared information on how deployments, configurations and other required features are managed. In the next chapter, the BladeLogic environment and results of the tests which were done using the BladeLogic are described in detail.

4 RESULTS AND ANALYSIS OF THE PROVISIONING AND MANAGEMENT

The BMC BladeLogic environment was successfully installed and configured. The installed environment was proven to be working with the following items and conditions:

1) Three Dell PowerEdge 1950 rack servers with latest firmware packages installed.

2) IP network 4.4.4.0/24. IP address 4.4.4.1 which is the firewall and unrestricted connection to the Internet and to servers in the company network.

3) The BladeLogic is separated to three servers. First server has the Windows 2008 64 bit version with SP2 installed as the BladeLogic application PXE and TFTP server. Second server function as the database server with Windows 2008 64 bit version with SP2 installed and Microsoft SQL 2008 database engine configured. It also provides the DHCP service. Third server works as the file server with a CIFS server provided by SAMBA service and HTTP service provided by the HTTPD. The file server has a 64 bit Red Hat 6 Linux installed. All operating systems were updated to latest available patches.

4) Configurations to the BladeLogic environment were done using manuals provided by the BMC. PXE and TFTP services use multicast address which is provided by the configuration tool.

5) Update definitions are automatically downloaded from the Shavlik Technologies every 24 hours. Automatic download of the update packages are scheduled to be done once a week.

The crucial component of the tasks between the BladeLogic application and a target server is the RSCD agent. If RSCD agent configuration or privileges

are not properly set then management functions cannot be performed correctly. The BladeLogic provides tasks where the user can request RSCD agent information from a target server. If that task provides correct information such as RSCD agent license status and user mapping between RSCD agent and operating system then the BladeLogic application can manage a target server.

4.1 RSCD Agent Installation Results

Manual RSCD agent installation to a target server has proved to be working method in multiple cases. For unknown reasons configuration settings which were inputted to during RSCD agent installation was not correctly saved to the configuration file. The corrective action was to get configurations from a working RSCD agent installation. After restarting the RSCD agent in a server which now has correct privileges and after that the BladeLogic was allowed manage the server.

The Bulk Installer allowed automated RSCD agent installation to multiple target servers simultaneously. The Bulk Installer can handle different types of servers with different user accounts in one RSCD agent deployment job. The Bulk Installer was most of the time able to install the RSCD agent successfully to the target server. In several occasions remote installation failed for an unknown reason. Workaround was to install the RSCD agent manually to the target server.

The Bulk Installer proved to be a flexible tool deploying the RSCD agent to existing servers. It can be used to an upgrade the RSCD agent in the target server. The bulk Installer provides a group licensing feature. It is a feature providing a method to a register the installed RSCD agents to the BMC.

4.2 Windows Operating System Update Results

The updates were scheduled to be downloaded once a week. The first time BladeLogic downloaded all available updates selected in the Patch Catalog. Every 24 hours BladeLogic downloaded the XML file from the Shavlik Technologies. After the XML file was downloaded BladeLogic compared its con-

tents to the database for updates. If there were new updates available, BladeLogic downloaded files at next scheduled patch catalog update.

Windows updates to the servers were tested using several update scenarios. The scenarios were to only update security updates to the operating system update all updates including service packs to an operating system and update all updates to an operating system and its applications.

One test procedure was that after the analysis job was done and the update job was scheduled, the target server was updated manually to have all the latest updates. This test case was done to test how the BladeLogic reacted to unexpected changes in a server and how it behaves in those situations. The results were that no updates were installed to the target server.

If a server required several reboots during the update job, BladeLogic handled those situations and did not produce any errors in the update job events. In cases when all updates to an operating system selected except service packs updates which require a service pack to be installed failed. BladeLogic did try to install those updates but errors were logged in the update job events. Update packages which did not require a service pack to be installed were installed correctly. Even if only one update to the operating system was successfully installed BladeLogic was always able to command the server to restart if necessary. In every test case all the restarts were completed successfully.

Operating system update jobs were mostly successfully performed with limitations. The limitations were exposed by update packages, in example the update package was not able to be installed if the software which update package depends is not installed. That is not something what the BladeLogic update job can override.

Most of the errors were due to privilege conflicts between the RSCD agent and the Windows administrator user mapping. In some cases the RSCD agent configuration was missing a configuration parameter. If in the server properties of the RSCD_DIR –parameter is missing erratic behavior can happen between BladeLogic and the RSCD agent. The example of the correct configuration parameter can be seen in following example. (see Figure 27). This error condition was corrected by refreshing the RSCD agent configuration using the BladeLogic console view.

RSCD_DIR	/C/Program Files/BMC Software/BladeLogic/8.1/RSCD

Figure 27. RSCD_DIR configuration parameter.

The RSCD_DIR –parameter can be different in other deployments. In example the RSCD agent version is 8.1 and this version number is in the RSCD_DIR. Next version of the RSCD agent could be in different directory. In Figure 27 is RSCD agent is installed in the Microsoft Windows operating system and directory format is unique to that. The Red hat Linux uses different directory format and from that follows that the RSCD agent is installed in a different folder.

4.3 Results of Updating Red Hat Linux Using BladeLogic

The company's only Linux version is the Red Hat Linux distribution. The current versions to date are 5 and 6. Both are available to use as 32 bit and 64 bit versions. The company has made support contract with the Red Hat Corporation which allows direct downloads of the update packages from the Red Hat Network repository. Download privileges are given to the certain username which is configured to the BladeLogic Red Hat patch update package downloader. As long as the support contract is valid the BladeLogic application can download updated Linux packages.

Patch Catalog configuration were constructed and configured to contain updates for a certain Linux releases. Downloads from the Red Hat were scheduled to perform downloads periodically and it worked. This made Linux updates available from the file server. In the following scheduled downloads the BladeLogic only downloaded updates which were not available from the file server.

Update procedures were similar to updating the Microsoft Windows operating system and applications. The first step is to make the analysis job where the BladeLogic analyses current patch level of the server and its installed applications. If there were no problems with the RSCD agent then the ana-

lyze job was successful. After the analysis was completed a remediation job could be made and scheduled.

The Red Hat Linux operating system does not need to be restarted if only applications are updated. Only a kernel and a kernel module updates require server restart. Linux update tests were made updating all applications and operating system components except a kernel and kernel modules. After update was successful the BladeLogic restarted software components which required to be restarted.

Updating the Red Hat Linux using the BladeLogic tests were successful and there were no problems. Scheduled downloads from the Red Hat Network were proven to be a reliable and the BladeLogic only downloads files which are missing from the repository.

4.4 Results of PXE Installation Tests

Pre-boot Execution Environment installations provided to be a faster method of getting a new operating system installed in a bare metal server than using manual installation process. Before the PXE provisioning could be done the BladeLogic PXE environment was to be configured to support the PXE booting.

The PXE datastore is a central component which should be first component to be configured. The datastore has two instances. One datastore instance was configured for a Windows operating systems and the second datastore for a Linux provisioning (see Figure 28). In the Windows datastore username and password was configured which allows provisioned operating system to access datastore. Datastore path is configured to the BladeLogic where files are located in the file server. The VIRTUAL_DIR definition is the name of the CIFS share on the file server. In a Linux datastore only IP address of the file server path to the files and the VIRTUAL_DIR definition is configured.

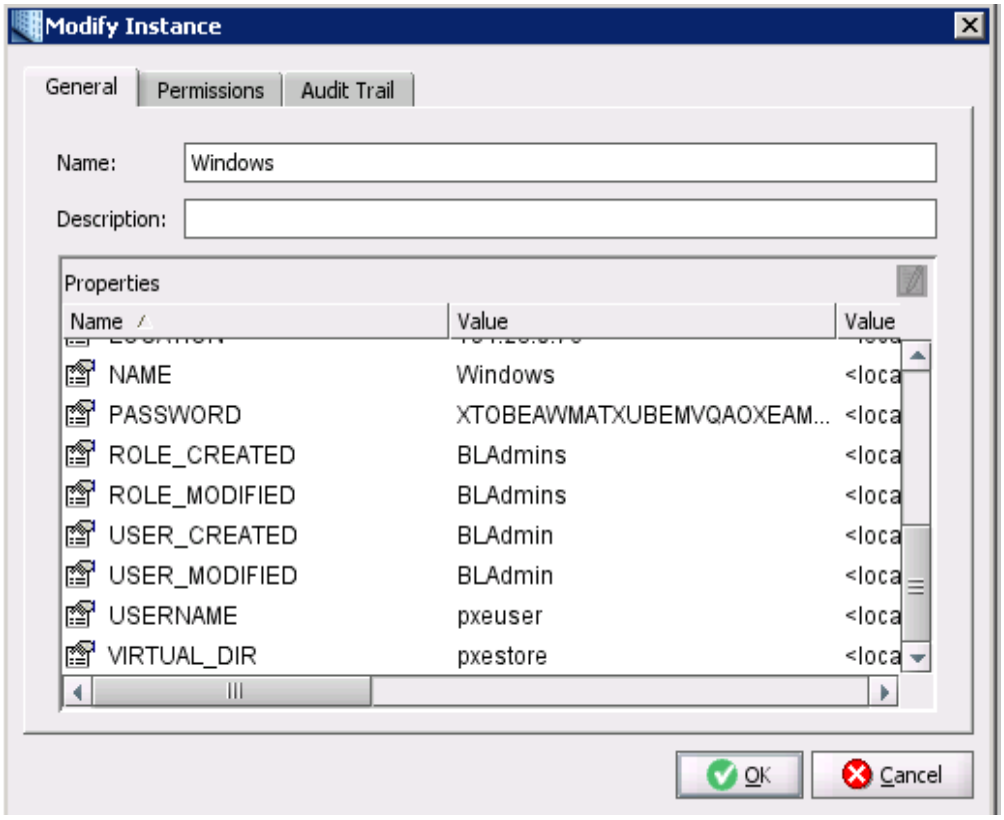


Figure 28. BladeLogic Windows PXE provisioning configuration example.

The PXE Provisioning supports multiple data stores for provisioning. In a provision job wizard the correct data store must be selected for a target server. In a test scenario the BladeLogic only had two data stores.

When PXE installation starts it needs an IP address which it can get from a DHCP server. The DHCP server was installed in the database server named CUERVO. The BladeLogic requires two special parameters configured to the DHCP server. First one is the bl-server and the second one is the bl-port (see Figure 29). Bl-server parameter is an IP address of the BladeLogic application server and the bl-port parameter is the BladeLogic application server TCP port where it listens for connections from PXE booted servers.

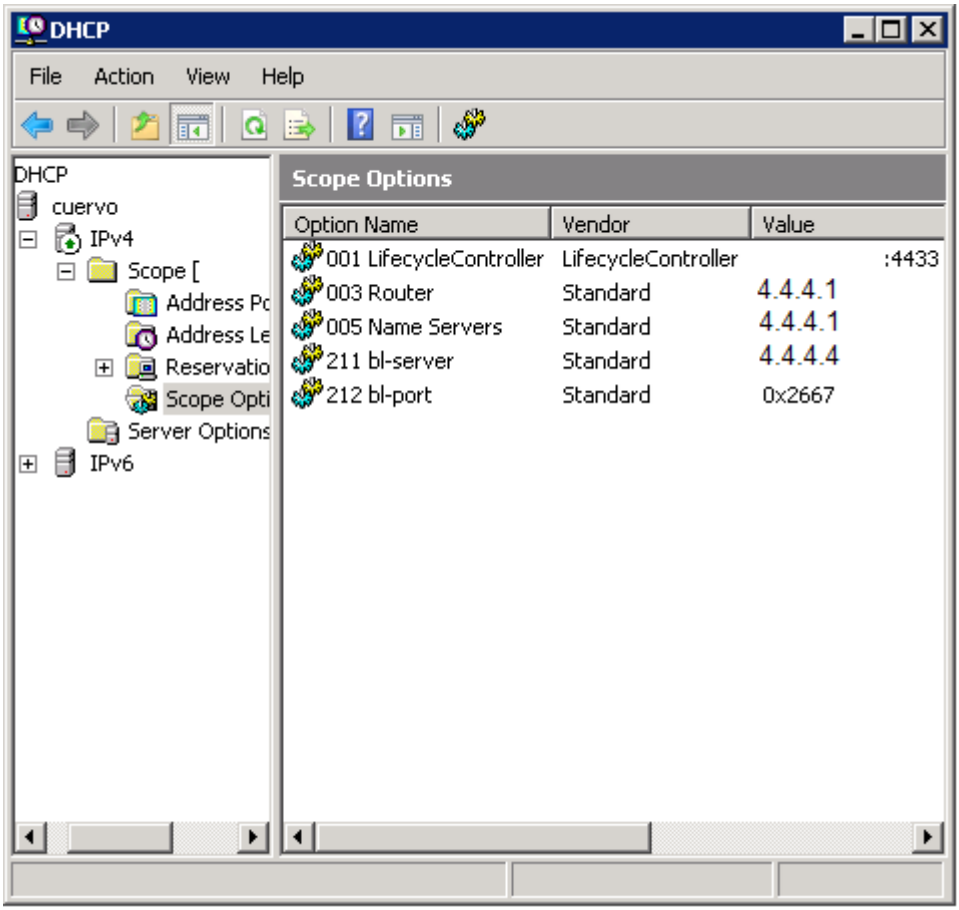


Figure 29. Parameters required by the PXE provisioning job configured to DHCP configuration.

PXE and TFTP are the software components provided by the BMC. PXE service was configured with the following parameters: Multicast IP address is bind to the IP address 224.1.5.1 and it listens in the TCP port 4011. The TFTP service was configured to use IP address 4.4.4.4 and multicast IP address 224.0.1.2. The TFTP listens in the following UDP ports 69, 1758 and 1759. TFTP services root was set to the C:\tftproot where it serves files to PXE devices.

PXE provisioning tests were made using the following operating systems: Windows 2008 and R2 server and Red Hat Linux 5 and 6. The BladeLogic provisioning configuration was updated with the information of the location where the BladeLogic can find the installation files. In the Provisioning Manager configuration are predefined operating system types which are useable.

In OS installer settings path of the operating system installation files were configured (see Figure 30).

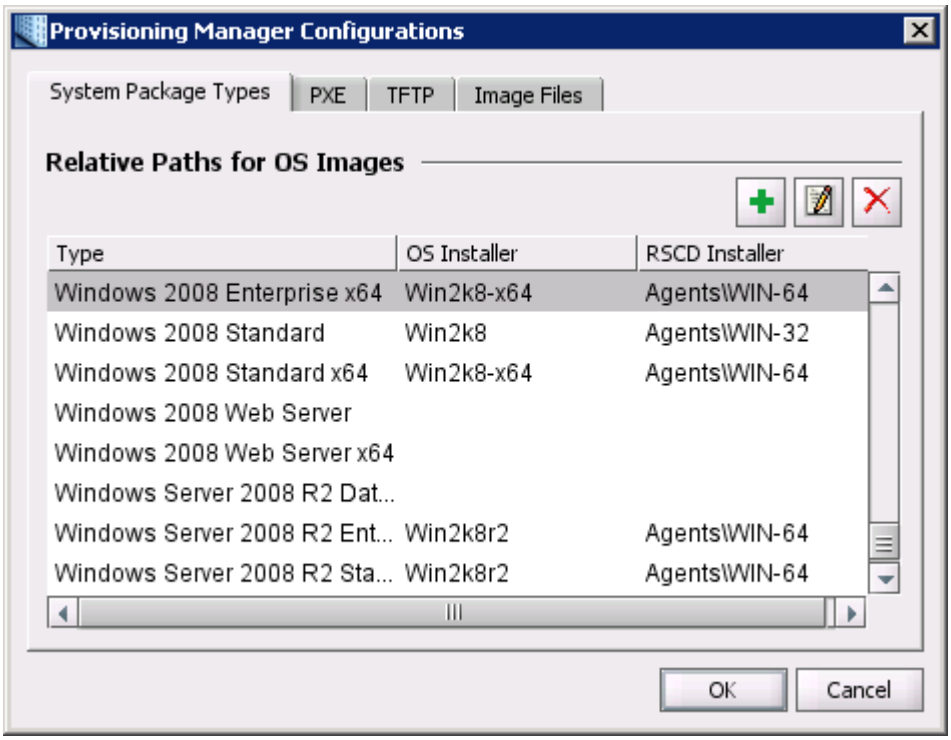


Figure 30. PXE provisioning installation files and RSCD agent installation package location configuration.

Suitable boot images for the Windows operating system were created using the Provisioning Image Creation. It uses external software named WAIK (Windows Automated Installation Kit). Version was used. It was downloaded from the Microsoft and installed to C:\WAIK directory in the JOSE BladeLogic Application server. Directory WAIK was selected because the BladeLogic does not allow spaces in the WAIK installation folder name.

The BladeLogic provides the PXE boot image for the Linux PXE installations. This PXE boot image was found suitable booting different versions of the Red Hat Linux. Windows operating system can require separately installed drivers to support the server hardware. In the image creation required drivers can be embedded to the PXE boot image. All different drivers for a different server types which company supports are embedded in a single

boot image. For testing boot image to Dell PowerEdge 1950 servers was created and in this image were drivers for a different raid controllers. If a new driver is required in a PXE deploying new image must be created. Drivers in Red Hat Linux operating system are embedded in the kernel if a new driver is needed then newer Red Hat Linux version must be selected.

After the Windows PXE boot images are configured and image processing is done they can be viewed modified and deleted using a Provisioning Manager Configurations Image Files tab. In Provisioning Manager Configurations can be selected which images are set for default for certain types in the PXE provisioning and configure if the image is for a 64 bit systems or a 32 bit systems. Two Windows images were made to be used in the PXE boot (see Figure 31).

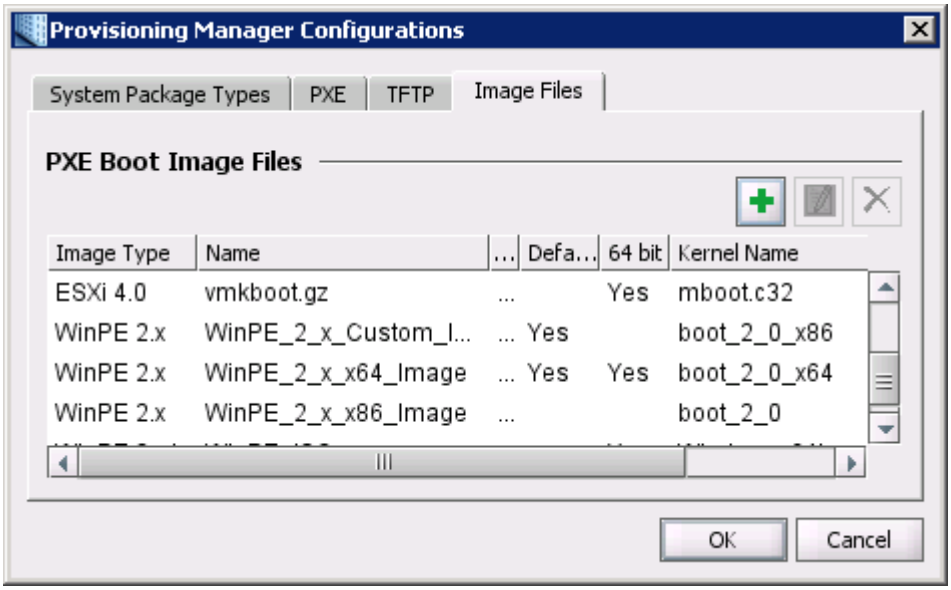


Figure 31. PXE provisioning boot images for different operating systems.

Before the provisioning job could be started a target server PXE network card MAC address was added to the BladeLogic. In the Provision Device wizard computer name was selected and folder where the provision job is saved (see Figure 32). During the provision wizard a correct system package configuration was selected along with a boot image.

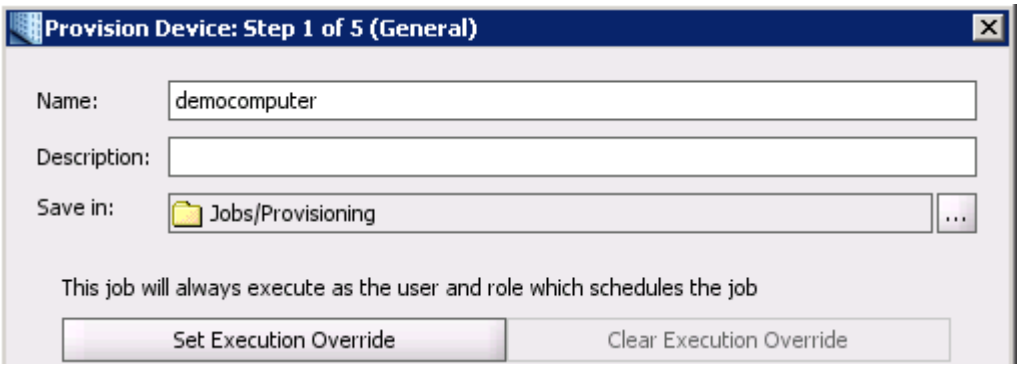


Figure 32. PXE provisioning jobs first step.

The provision job wizard asks dedicated information of the server such as what is the computer name, password for administrator or root user and IP address of the configuration. IP address can be set manually or the server can obtain IP address from a DHCP server. During a testing both settings were used. Using static IP address and IP address provided by DHCP was successfully deployed.

In the testing phase the target server PXE network card was configured to VLAN 20. In that VLAN the BladeLogic provisioning services such as a PXE TFTP and DHCP services were located. This configuration scenario does not require any firewall and routing configuration. If the PXE configuration was correct then the target server did receive an IP address. Boot process continued getting the boot image from TFTP server (see Figure 33).

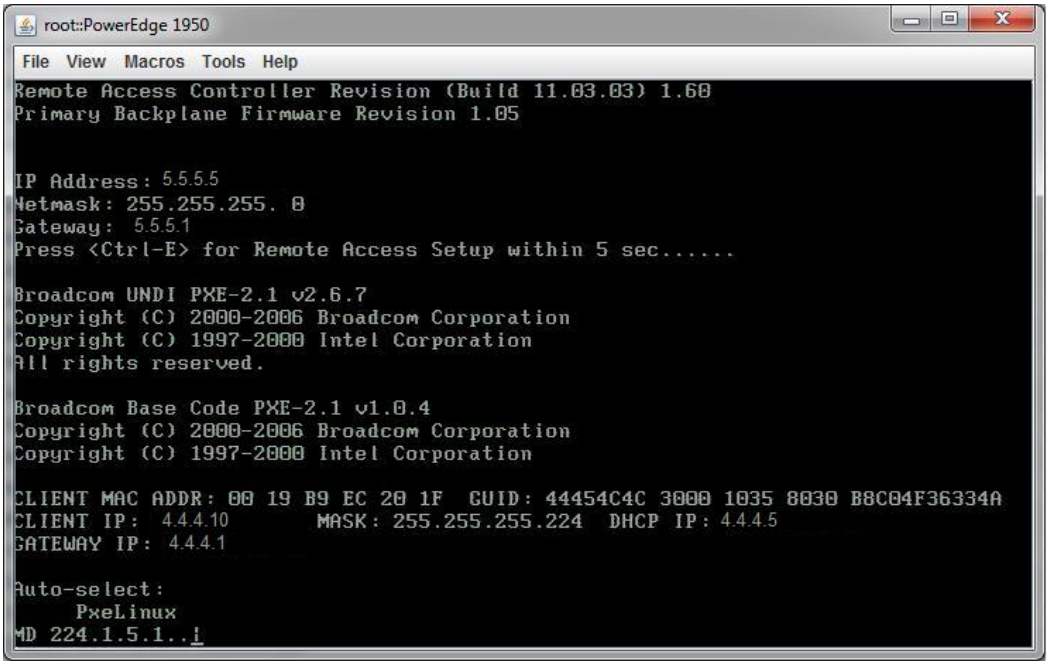


Figure 33. Successful PXE booting start example.

In the BladeLogic provisioning there are settings and parameters which must be take into consideration before PXE installations are possible. Different operating systems can behave differently when using the PXE provisioning. Provisioning the Windows operating system some problems was discovered. During provisioning the 32 bit version of the Windows 2008 server in the beginning when the hard drive partitioning was complete it didn't work at first. The partitioning manager removes existing partitions but cannot create a new one. The provisioning fails and the target server reboots. During this reboot phase PXE booting should be selected again. The target server boots using the PXE and starts installation from the beginning. The second time hard drive partitioning was successful and operating system installation could continue.

Windows 2008 32 bit and 64 bit version operating system files have multiple system versions bundled in the single installation image such as a standard enterprise data center and web versions. The BladeLogic does not select which versions should be installed even if it is configured in a provisioning job wizard. User must select the correct version of the operating system before installation can continue (see Figure 34).

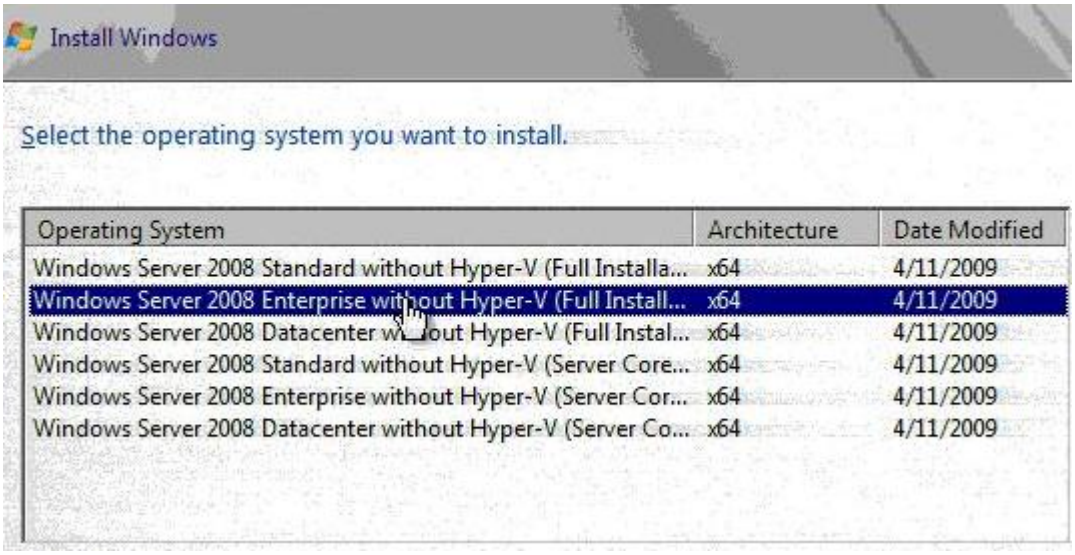


Figure 34.Additional step in Windows 2008 PXE provisioning job.

When provisioning the Windows 2008 R2 version network interface numbers are switched over after provisioning is completed. In the Dell PowerEdge 1950 server network interface number zero is the network interface card which has PXE features. During the provisioning IP configuration is set to network interface zero but after Windows 2008 R2 installation is completed physical network interface one is recognized as a network interface zero.

In some rare cases during the provisioning operating system boot up phase the installer process cannot configure the network interface card. This prevents the installation process to contact the application server and the PXE provisioning fails and this situation can be corrected by rebooting the server.

During provisioning of the Red Hat Linux 6 in the provisioning job wizard ethernet interface one should be selected because if the PXE features are in a network interface zero. This is for a reason that Red Hat Linux version 6 recognizes network interface zero as one. Selecting a correct interface and then the PXE provisioning boot image can bind IP address to the correct network interface.

If post provisioning jobs are required then the RSCD agent installation must be selected. After provisioning the operating system the RSCD agent can be installed. To manage the target server after PXE provisioning server needs

to be added to the BladeLogic management. Servers are added to the BladeLogic using its domain name or IP address.

Installed RSCD agents have a trial license by default which allows then to run for a two weeks from installation date. Registration of the license was done using a network shell. Registration process makes new license and this license is transferred to RSCD agent (see Figure 35).

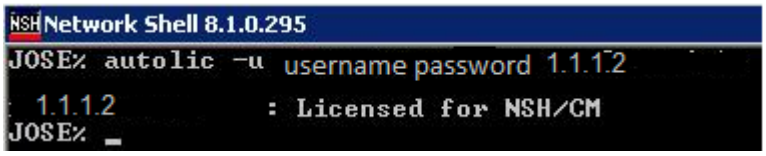


Figure 35. Licensing the RSCD agent using a Network Shell.

All of the tests installing the RSCD agent in a post provisioning jobs were successfully. ACL setting were not automatically deployed to the RSCD agent installations in a Linux environment. Refreshing ACL settings to RSCD agent after installation was the work around for this problem.

The BladeLogic remembers provisioned servers and keeps configuration of the provisioned server. This configuration can be used to re-provision server again or it can be modified to fit future needs.

4.5 BladeLogic iDRAC Provisioning Results

Only the Windows server operating systems installation is supported in the iDRAC provisioning. Prior to adding iDRAC devices to the BladeLogic routing and firewall configurations changes were made. iDRAC card received static IP address from network management and iDRAC is placed on dedicated network block. This IP network block can be accessed through firewall. In firewall TCP port 443 was opened from the BladeLogic application to an IP network where iDRAC cards are located.

iDRAC devices were added to the BladeLogic when a iDRAC IP address username and password were given. iDRAC provisioning wizard requested correct MAC address which is used to recognize iDRAC in the BladeLogic.

After the iDRAC device was added to the BladeLogic operating systems provision could be started. Added device can be managed by selecting it and opening tool bar (see Figure 36). As this iDRAC feature is a new and introduced in BladeLogic Server Automation Suite 8.1. There were problems using iDRAC features in this version. Only feature which were working was password change for root user. The provision job wizard was launched but nothing happened and the provisioning job ended without results. Copying drivers from datastore to iDRAC crashed and the BladeLogic produced an error. Copying ISO image to iDRAC vFlash could not be performed because the BladeLogic console did not allow selection any ISO images.

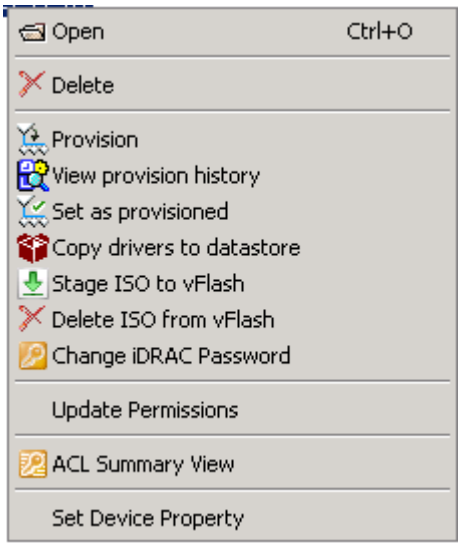


Figure 36. iDRAC management options in BladeLogic console.

In the future versions the evaluation of the iDRAC provision should reevaluated. iDRAC provisioning and management could be a very affordable option to use.

4.6 Software Deployment Results

Installation of the software to a managed server using the BladeLogic application server allows managed software deployments. The BladeLogic can be used to make the BLpackage which can be deployed to a server.

With preconfigured software packages which can be deployed to the server is a fast and convenient method. Multiple installations can be done simultaneously. The BladeLogic provides uninstallation for a deploying software and removing the software.

First software packages must be build which the BladeLogic can deploy to the server can take long time. After the software package is done it can be installed to multiple servers simultaneous which can reduce installation time dramatically compared to manually installing software to selected servers.

4.7 BladeLogic Server Inventory Results

Making inventory of the managed servers using the BladeLogic did require a plan because the server groups can be used for different purposes. The different groups have different meaning. In the simplified mode the server groups shows all server. The server object was distributed to a several static groups to make an example of the patching job targets and how it makes selecting multiple servers simpler. The server smart group was used to show only target servers which are only visible per filter rules (see Figure 37).

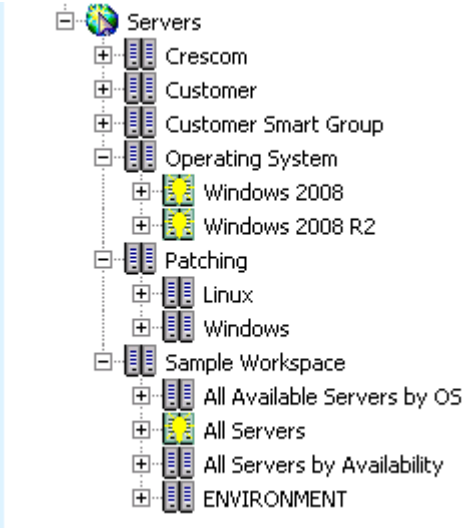


Figure 37. Server inventory example using static and dynamic groups.

The smart group filters provided to be a powerful tool to define groups for certain servers. At least one static group was used that where the new server were added for first time. The same static group is used to when a server is decommissioned. Using decommission to the server object was removed from the smart groups.

4.8 Server Configuration Changes Summary

The BladeLogic is a tool which can manage target server configurations. It keeps list of the configuration changes in a database that those changes can be analyzed or reverted if necessary. From audit log can be viewed that who and when and what configuration changes were performed.

Using the BladeLogic to make a configuration change to multiple servers gives the server operators fast and a convenient opportunity reduce time which was before required to make changes to servers. If there is a new configuration change what must be deployed to multiple servers or the configuration parameter which must be removed, the BladeLogic can process those changes in efficient way compared to manual configuration change. Now changes can be applied to multiple servers at the same time. Manual changes which are repeated multiple times can produce errors during repeats. Making configuration change only once and deploying that change to servers reduces chances of the configuration errors.

The server processes or daemons can be started and stopped using the BladeLogic application console. The BladeLogic can manage all processes and daemons with certain exceptions. The exceptions are stopping the RSCD agent process which disconnects management connection to the server and the server core services which can affect the server operational status negatively.

5 CONCLUSIONS OF BLADELOGIC PROVISIONING AND MANAGEMENT

The BladeLogic provided to be a powerful tool to manage servers. It also provides additional methods to install operating systems to new bare metal servers. Install software packages to the managed servers. Making configuration changes using the BladeLogic provided to be a flexible to server managers who manage multiple servers which requires equal configuration changes.

Documentation provided by the BMC allows server managers to develop best practices which can help in daily management and maintenance tasks. To work with the BladeLogic efficiently the network infrastructure it need to have connections between different application components. Communication between BladeLogic application and RSCD agents requires network connection between them. The BladeLogic do not require continuous active connection to the RSCD agent only when information is exchanged between RSCD agents and the BladeLogic application. Network interrupts can make server tasks to fail if it happens during management tasks. Most common problem when BladeLogic application cannot manage a target server is that RSCD agent privileges are not correct or broken network connection. If RSCD agent privileges are not correct it can view only the target server status only with read-only privileges but is unable to perform any changes.

5.1 Microsoft Windows Operating System Update

The Windows server update process using the BladeLogic application provided to be successful task. The BladeLogic provided customizable update procedures and it can work with the different software and the version combinations which are installed to the server. It can handle situations when the Windows is updated manually or automatically by the Windows update process. The BladeLogic understands those situations and does not precede installing updates which exists in the target server.

Even that update process can update multiple servers simultaneously it is not a perfect. The user interaction is needed to monitor analyze and update results. If there are problems in results the user needs to make correspond-

ing actions and the action must be based on problem results and the target server configuration.

Before making analyze and update jobs against the Windows server user must check that the BladeLogic has the new software update information. If this information is missing then the BladeLogic has no information to download updates from a software manufacturer and deploy then to the target server. After verifying that the BladeLogic have required information it can download updates and make analyze job.

Using the BladeLogic application to update Windows operating systems and its software components is a method which is useful. It has small flaws which are manageable if the user checks update processes results. If there are no major problems with the server then the BladeLogic manages to updates successful.

5.2 Red Hat Linux Operating System Update

The BladeLogic application can be used to update Linux operating systems. Only limit is that the BladeLogic can only update supported Linux operating systems. Same rules considering about the update procedure and the BladeLogic application configuration applies to the Linux update job as to Windows update job.

Analyze and update jobs usually goes through successfully but the job administrator must monitor both jobs for errors: Most common errors are when the BladeLogic application server cannot communicate with the RSCD agent and the RSCD agent configuration problems when it cannot manage the target server. The BladeLogic application can perform Linux updates successfully. No errors were received from update jobs in any phase of the testing.

5.3 PXE Provisioning

Using the PXE installation to deploy the operating system to the target server is a complex process which requires all the necessary application components to work together. Setting the BladeLogic to support the PXE installa-

tions requires software configurations of the BladeLogic to match network configuration where target servers are connected and PXE configuration in network interface card enabled and operating system boot files configured. The BladeLogic PXE installation process does not need pre-existing pre-defined operating system images for different types of the server hardware. Different hardware types are handled by a separate driver packs which set correct driver for the installation job.

The target server preparation for PXE installation job requires only the MAC address of the network interface card which is used to identify the target server to the BladeLogic. The BladeLogic PXE installation jobs have predefined certain settings which are required to operating system to be installed. Such settings are how to partition hard disk which software components are to be installed and network configuration.

Installation time between operating systems and deployment type was calculated using timer. Time was calculated using minutes and rounded to the nearest minute. Disk partitioning and network configuration was made during the installation process. The time calculation did begin when the bare metal server booted to the installation program and the clock stopped when operating system booted to the installed operating system. In figure 38 is a comparison chart between operating system types and installation method. In the PXE installation method operating system installation times were much faster than non PXE installation. Non PXE installation was a manual user interactive installation process (see Figure 38).

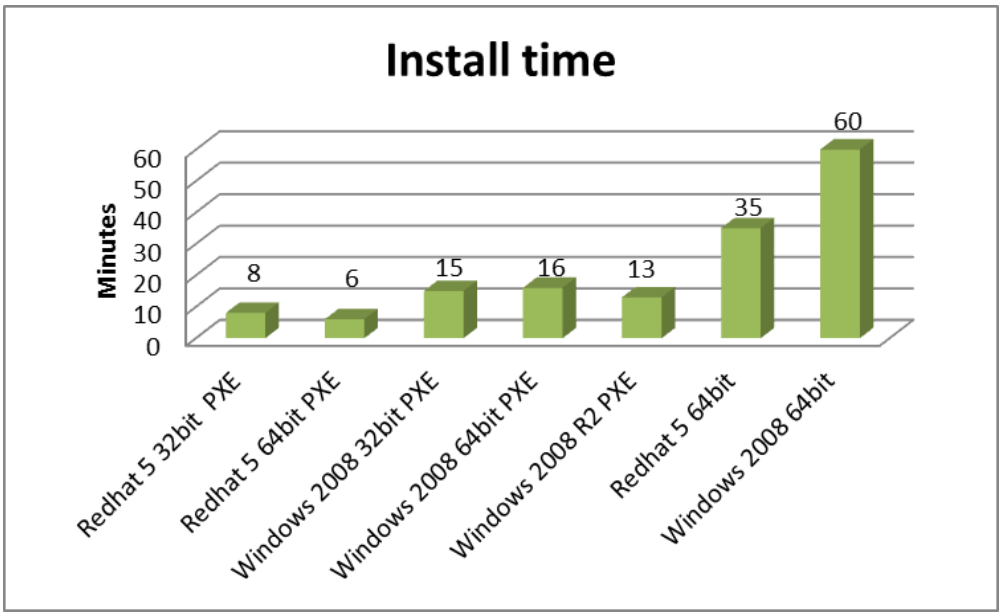


Figure 38. The time difference between installations using PXE and manual installation process.

The BladeLogic PXE deployment job allows multiple operating system deployments to bare metal target servers. The PXE deployment job is not restricted to deploy only one type of the operating system at one time. For example there are five bare metal servers that need to have new operating systems. The user can deploy Linux and Windows operating systems simultaneously. The PXE deployment job can deploy different versions of Windows operating systems to target servers.

The PXE installation method provided to be fast method to deploy a new operating system to the bare metal server. The PXE installation can be used to reinstall operating system to the server regards if there is the operating system installed in the server. It replaces the existing operating system with a new freshly installed operating system. The PXE installation is a working method to deploy different types of the operating systems to a different type of the server hardware.

5.4 iDRAC Provisioning

Using the iDRAC provisioning with current version of the BladeLogic is not working. Only usable feature was the iDRAC password management. The provisioning using the iDRAC could be practical feature in the future when the BMC fixes the BladeLogic software.

The iDRAC management using the BladeLogic is an idea that should be discarded when software features and functions of the BladeLogic supports more iDRAC functions. The BladeLogic could be very powerful tool to manage and provision servers using the iDRAC.

Only servers from the Dell Computers are equipped with the iDRAC. The other hardware manufacturers have similar remote access cards such as the iLO (Integrated Lights-Out) made by Hewlett-Packard. The iLO is not compatible with the BladeLogics iDRAC functions. If company has BladeLogic software and does not use Dell Computer servers then iDRAC provision has no use for them. The PXE installation can be used to provision operating systems to the bare metal servers.

5.5 Software Deployment to Servers

A new software deployment to the target server using the BladeLogic software deployment job deploys and removes software from managed target servers and it also allows software upgrades. When software package has been made deployed to at least one target server should be done. After this deployment software deployment should be tested. After testing deployment jobs to the target servers can be performed.

The software deployment time depends of the software and speed of the target server. The transfer time from the file server to the target server depends of the speed of the network. Today’s gigabit speed networks provide fast connection to the servers. Multiple simultaneous deployments require mode bandwidth from the file server and from the network. If the file server and network bandwidth is limited then deployments can take more time.

5.6 Server Inventory

The BladeLogic can be used to make list of the server types based on an operating system version, the server owner if there are servers for a multiple customers and many other detailed server information. This information can help in different situations such as problem situations which can rise for different reasons. Identify servers that the maintenance can be targeted to correct servers.

The server inventory provides a fast view to a managed server and gives brief status of the servers. It provides functions to sort servers to a different category. One customer can have a multiple server types which are managed by a different server administrator.

5.7 Server Configuration Management and Change

Using the BladeLogic to manage and make configuration changes to the target servers can bring in a few features which can help daily maintenance jobs. All changes are audited, reversible and repeatable. Auditing logs keep track of the all changes which are made and who made the change and when. The audition feature also brings in a tracking feature and allows server administrator to see all the changes which are made to the server. Reverse option for the configuration allows the server administrator to reverse incorrect or out dated configuration parameters. All changes which are made can be repeated to the other target servers which have same type of the operating system. Windows configuration changes can be made only to the Windows systems and Linux configuration changes only to the Linux systems.

The BladeLogic provides versioning for changes which helps system administrator to keep track of the change path. Under configuration parameters the BladeLogic can be used to manage the target server processes. Usually processes are needed to be restarted if the configuration changes. The services can be stopped and started for various reasons such as if the service is crashed. The Server configuration function allows flexible way to manage target servers

6 SUMMARY

The BladeLogic provisioning software from the BMC gives enhanced deployment capabilities to do new server deployments more efficiently than the company's current deployment method allows. Removing multiple selections and steps from the deployment process and making the process steps standardized helps making more error free installations.

Managing several thousand servers in a heterogenic environment can be a very complicated task. Using BladeLogic to support the servers' management processes has turned out to be more simplified and many times more efficient compared to manual support. Automation processes such as updating server software deploying new applications and making configuration changes have become more flexible.

Using the BMC BladeLogic provisioning software with certain limits is a very good solution to MSPs that have multiple servers containing different configurations. It provides a flexible approach to concrete managing processes.

BladeLogic provides a simplified management process to multiple operating systems and servers. Using only a one centralized software to provide necessary and requested functions helps in daily and seasonal operational tasks instead of using multiple software applications to provide only one management function per application.

Using only one application means there is single software needed to be taught for server administrators to use. If changes take place in processes or in software it is easier to provide them to only BladeLogic rather than to multiple management software.

The BladeLogic application was investigated for provisioning software updates and audit properties. Provisioning using the PXE provisioning method was successful. Using BladeLogic to manage and perform operating system and software updates to a target server was also a successful method. The BladeLogic audit property of the target server provided information of the server status and its components.

Provisioning using an iDRAC module was not successful. The problem is in the BladeLogic software which prevents provisioning jobs to from function-

ing. The iDRAC provisioning feature may have software fixes in time and then it should be reevaluated.

The recommendation based on the study is for Crescom to use the BladeLogic application to manage servers and to deploy servers in its data centers. This is based on the benefits of using the centralized management application which provides all the required features. In the testing environment evaluated features such as a new server deployment server operating system and application updates and configuration changes were successful.

There were some problems with the BladeLogic application software which were resolved with BMCs support services. New versions of the BladeLogic application may be released in the future. New versions could introduce new features and bug fixes. The new software version can introduce new bugs that could affect the functionality of the software. The recommendation is that the application is kept up to date but keeping in mind that there could be problems in future releases. There will be new operating system versions and new applications which can be managed and updated using BladeLogic.

BladeLogic is flexible software and there are multiple ways to use it. It is recommended that the company produces a process documentation on how the BladeLogic application and its processes should be managed. Working with the BladeLogic application demands continuous development to processes used. New practices should be developed, tested and deployed to production.

Installing and deploying the BMC BladeLogic application to production use is not a simple and fast process. First it requires careful planning how to deploy the BladeLogic application itself and users managing servers require training.

Benefits BladeLogic brings to multi server environments cannot be denied. It provides all the required functions and features which Crescom requires for daily management tasks. The BladeLogic provisioning helps deploying multiple servers simultaneously to save time in installation. The server management function helps managing server configurations. Configuration changes can be made to multiple target servers simultaneously instead of using the manual management process to access servers one by one and making changes manually.

REFERENCES

[1] BMC BladeLogic Server Automation components. **http://www.bmc.com/products/product-listing/BMC-BladeLogic-Server-Automation-Suite.html** (Accessed Jun 2011)

[2] VMWare virtualization products. **http://www.vmware.com/products/vsphere/** (Accessed Jun 2011)

[3] Citrix virtualization products. **http://www.citrix.com/** (Accessed May 2011)

[4] Addess allocation for Private Internets. http://www.faqs.org/rfcs/rfc1918.html (Accessed Jan 2011)

[5] IP Network Address Translator (NAT) Terminology http://www.faqs.org/rfcs/rfc2663.html (Accessed Jan 2011)

[6] VLAN Aggregation for Efficient IP Address Allocation. http://www.faqs.org/rfcs/rfc3069.html (Accessed Jan 2011)

[7] Microsoft Corporation Windows 2008 server information. http://www.microsoft.com/en-us/server-cloud/windows-server/default.aspx (Accessed Jan 2011)

[8] OSPF as the Provider/Customer Edge Protocol for BGP/M. http://www.faqs.org/rfcs/rfc4577.html (Accessed Feb 2011)

[9] Cisco Systems. Example http://www.cisco.com/ex/US/docs/solutions/Enterprise/Network_Virtualization/PathIsol.html (Accessed Jun 2011)

[10] BMC Network Shell Proxy Server http://discovery.bmc.com/confluence/display/Configipedia/BMC+Bladelogic+Server+Automation+Suite (Accessed July 2011)

[11] BMC Software, 2011, *BMC BladeLogic Server Automation Installation Guide*. 12.

[12] BMC Software, 2011, *BMC BladeLogic Server Automation User Guide*. 414 1011, 1015.

[13] BMC Software, 2011, *BMC BladeLogic Server Automation Administration Guide*. 14

[14] BMC Software, 2009, *BMC BladeLogic Bulk RSCD Agent Installer User Guide*. 11, 414

[15] BMC Software, 2011, *Using BMC BladeLogic Server Automation for Microsoft Windows Patching.* 3

[16] BMC Software, 2011, *Using BMC BladeLogic Server Automation for PXE-Based Provisioning*. 11

Detailed components of the BladeLogic Server Automation deployment:

Servers are Dell PowerEdge servers. Servers connect to the network using the switch which is a Dell PowerConnect 6248 switch with the latest firmware. All servers are connected to each other through one gigabit network connection. Switch has configuration where all server are in a same VLAN. The ports are configured in a switch as untagged mode with Spanning Tree Protocol disabled.

Four Dell PowerEdge 1950 servers. Four servers have equal components:

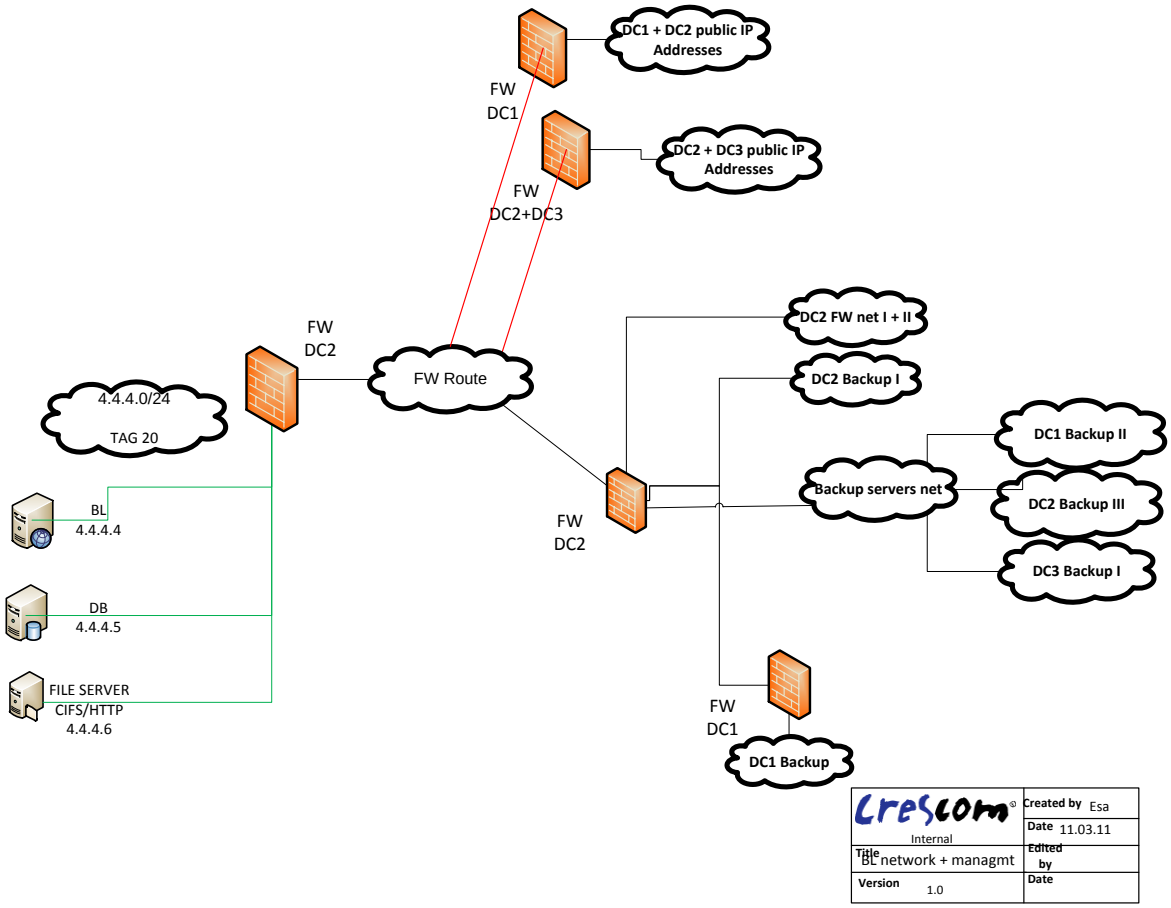
2.66Ghz Intel Xeon Quad CPU Processors
4GB of memory
Two 3.5” 146GB 10krpm SAS hard disks in RAID 1 configuration.
Two one gigabit network interface cards.

Fifth server is Dell PowerEdge 6850. It has equal components as other servers except it has six hard disks in RAID 5 formation.

Three of the servers are BladeLogic Server Automation components and two of the servers are built for testing purposes.

Application server and database server have Windows 2008 R2 operating system installed. The fifth server which has six hard disks has Red Hat Linux 5.5 installed and it operates as a file server.

All servers have latest firmware updated from Dell. Operating systems are updated to the newest updates level of June 2011.



This network picture describes the logical view of the company network diagram which describes network locations and access points to other networks. It shows how the BladeLogic application can connect to managed target servers.