# Consumerization of IT – Test Lab Guide: Hyper-V Windows 8 corporate virtual machine on personal computer

Published: September 2012

Version: 1.0

Author: Jérémy Julia

Co-authors/reviewers: Philippe Beraud, Jean-Yves Grasset



## Abstract

Thinking about Consumerization of IT (CoIT) necessarily leads to some security and management challenges.

Microsoft has enabled CoIT through many technologies for many years and now helps IT managers face security, compliance and compatibility issues they might deal with and give users access to corporate intellectual property from ubiquitous devices, both managed and unmanaged.

More specifically, this document deals with the situation where a company would like to put in place a “Bring You Own Device” (BYOD) environment. For that purpose, the document demonstrates how Microsoft technologies such as Windows Server 2012 and Windows 8 can allow to work anywhere with an employee's Windows 8 computer hosting a corporate virtual machine (VM) protected by BitLocker, while enjoying connectivity to his workplace. In such a context, the Windows 8 Client Hyper-V technology and DirectAccess technologies are used to implement this CoIT scenario.

This document is part of a series of documents on Consumerization of IT, and more especially aims at demonstrating the Hyper-V Windows 8 Enterprise Virtual Machine on personal computer scenario in a logical progression.

# Content

# 1 Introduction

## 1.1 Objectives of this guide

### *1.1.1 Consumerization of IT and Test Lab Guides*

Consumerization of IT is now a reality and users expect to be able to use their own devices, such as smartphones, tablets or laptops, for their work. In enterprises, IT departments can prevent problems by enabling these typical scenarios and being aware and ready to meet both users' needs and security policies.

This document is part of a series of Test Lab Guides (TLGs) that allow you to get hands-on experience using a pre-defined and tested methodology that results in a working configuration for the most frequent and relevant CoIT scenarios.

Indeed, when you use a TLG to create a CoIT test lab, instructions tell you what servers to create, how to configure the operating systems and platform services, and how to install and configure any additional products, technologies or devices. A TLG experience enables you to see all of the components and the configuration steps on both the front-end and back-end that go into a single or multi-product or technology solution.

More specifically, this TLG deals with the situation where a fictitious company would like to put in place a "Bring You Own Device" (BYOD) environment. For that purpose, the TLG demonstrates how Microsoft technologies such as Windows Server 2012 and Windows 8 can allow to work anywhere with an employee's Windows 8 computer hosting a corporate virtual machine (VM) protected by BitLocker, while enjoying connectivity to his workplace. In such a context, the Windows 8 Client Hyper-V technology and DirectAccess technologies are used to implement this CoIT scenario.

It is important to notice that this guide is independent in the sense that it **allows to build a full functional lab** on its own and does NOT require to follow other guides to implement the expected scenario. As a result, it comes as an addition to a series of TLGs already available on the Microsoft Download Center entitled CONSUMERIZATION OF IT TEST LAB GUIDES – 2ND SERIES[1] and that illustrates key CoIT scenarios.

Please **check carefully the hardware and software prerequisites** that are described in section § 1.6.2 HARDWARE AND SOFTWARE REQUIREMENTS before deciding to begin the construction of this lab.

In this regard, promoting a BYOD environment implies to develop and/or revise (technology) policies and quality controls that mitigate risks. These new policies must be developed jointly by IT and business units along with HR, finance and the legal department to ensure that all enterprise HR, legal, compliance and financial requirements are met.

Beyond the minimum specifications for hardware and operating system, the major areas the policies have to cover include:

- The employee's responsibility to have a suitable machine available for company use at all times;
- Who will pay — and how much — for hardware, software and third-party support ;
- What is and isn't supported by IT organization;
- Remote-access policies;

[1] CONSUMERIZATION OF IT TEST LAB GUIDES: http://www.microsoft.com/en-us/download/details.aspx?id=30177

- Security policies;
- Levels of permissible data access;
- Safe storage of company data;
- What to do if the system is lost or stolen;
- What to do at termination of employment;
    - Financial liabilities of enterprise and user;
    - Data cleansing from notebook hard drive.

The above areas and related considerations aren't further explored in the rest of this TLG and are outside the scope of this guide. This TLG rather concentrates to the technical implementation aspects of the covered scenario (see next section).

### *1.1.2 What is the scenario covered by this guide?*

The scenario of this TLG is based on the virtualization feature called **Client Hyper-V**, available on the Windows 8 Pro and Enterprise editions, and directly inherited from the feature found in Windows Server 2012. **The personal computer of the employee is used to host a corporate VM based on an image of a corporate computer**. This corporate VM is built with a Windows 8 Enterprise version, integrated in the enterprise Active Directory infrastructure and controlled by the internal management tools.

When inside the company, the user starts his personal computer, connects to the corporate network and launches the Windows 8 corporate VM. From within the corporate virtual machine, he can therefore access both the (Line-Of-Business (LOB)) applications and resources of the organization in accordance to his entitlements and (security) policies in place.

Furthermore, when the user is in a mobility scenario, i.e. connected from the outside with a typical Internet connection, **the Windows 8 corporate VM uses the DirectAccess technology to connect seamlessly and safely to the corporate network**. The user experience is identical in the sense that he is able to access the (LOB) applications and internal resources of the company in the same way as if he was connected to the internal corporate network.

From a security perspective, the Windows 8 corporate VM is domain-joined, controlled by the Active Directory domain and can be operated by the management infrastructure. Even when connected from the outside, the VM remains visible from the management infrastructure thanks to DirectAccess and will automatically receive security updates.

In addition, the corporate VM is protected by the BitLocker encryption technology. During the VM start-up, the user is prompted to enter the BitLocker password in order to allow the VM to boot and later connect to the corporate network with DirectAccess.

The guide also provides a mean to **automatically build the Windows 8 corporate image and deploy the VM onto the employee personal computer** based on the Microsoft Deployment Toolkit 2012 Update 1 (MDT)[2]. This toolkit is a Solution Accelerator for operating system and application deployment and is freely available on the Microsoft web site.

The guide illustrates how the user connects his personal computer on the corporate network and has at his disposal a seamless deployment process to deliver the Windows 8 corporate VM with minimum interaction. He only has to specify his corporate credentials at the beginning of the build process, and define the BitLocker password when the VM boots for the first time.

[2] Microsoft Deployment Toolkit (MDT) 2012 Update 1: http://www.microsoft.com/en-us/download/details.aspx?id=25175

The MDT also allows the administrator to easily create an image of the corporate VM that will be made available for deployment in this scenario.

Eventually, the last two optional steps provide the **opportunity to leverage the infrastructure that has been built over the lab, to implement the same kind of scenario using the Windows To Go feature of Windows 8 Enterprise**. The employee's personal computer can then be used to boot the Windows 8 corporate image from the USB drive or key. It also allows the secure connection on the corporate network based on the DirectAccess technology.

It completes a formerly published TLG entitled CONSUMERIZATION OF IT TEST LAB GUIDE: WINDOWS TO GO WITH DIRECTACCESS[3].

## 1.2 About this guide

### *1.2.1 What this guide provides*

As described previously, the purpose of this TLG aims at creating a CoIT test lab, based on the Windows Server 2012 Hyper-V virtualization technology. This CoIT can serve as a basis to build your own customized test lab that can include Microsoft or non-Microsoft products, and technologies, as well as relevant devices in the context of the Consumerization of IT.

This document contains instructions for setting up the "Hyper-V Windows 8 corporate virtual machine on personal computer" test lab by:

- Deploying three server computers running Windows Server 2012 as Hyper-V virtual machines (VMs), one physical client computer running Windows 8 Pro and one Windows 8 Enterprise virtual machine.
- Setting up the virtual networks, the Active Directory infrastructure, and the DirectAccess server.

The resulting configuration simulates both a private corporate intranet and the Internet.

Please note that the objective of this document consists in guiding you throughout the steps to implement a working scenario in the context of a test lab. In order to limit the number of physical resources needed to construct this lab, the virtual machines can host multiple services. This configuration is neither designed to reflect best practices nor does it reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a dedicated test lab network.

> **Note:**
>
> *Any modifications that you make to the configuration details in this TLG may affect or limit your chances of setting it up successfully on first try. Microsoft has tested this TLG successfully with the Windows Server 2012 Hyper-V virtualization technology, Windows Server 2012 virtual machines, and Windows 8 Enterprise for the client systems.*

[3] CONSUMERIZATION OF IT TEST LAB GUIDE: WINDOWS TO GO WITH DIRECTACCESS: http://www.microsoft.com/en-us/download/details.aspx?id=29990

> **Important Note:**
>
> *Before you try and build the configuration described in this guide, please make sure you have access to the* **Windows 8 Enterprise** *product.*

### *1.2.2 What this guide does not provide*

This guide does not provide guidance for advanced settings.

## 1.3 About Client Hyper-V technology

The Windows 8 Client Hyper-V enables to run more than one 32-bit or 64-bit x86 operating systems at the same time on the same host computer. But instead of working directly with the computer's hardware, the operating systems run inside a virtual machine (VM).

Client Hyper-V is the same computer virtualization technology that was previously available in Windows Server. In Windows 8, the technology is now built into the non-server version of Windows, often called the "desktop" version because it does not run on server-class hardware.

Client Hyper-V provides the same virtualization capabilities as Hyper-V in Windows Server 2012.

> **Note:**
>
> *For additional information on Client Hyper-V, please refer to the article* CLIENT HYPER-V[4]*.*

## 1.4 About DirectAccess technology

DirectAccess is a feature that gives users the experience of being seamlessly connected to their corporate network any time they have Internet access. With DirectAccess, mobile users are able to access corporate resources such as e-mail servers, shared folders, or intranet Web sites, with the same user experience and without having to open a VPN connection.

DirectAccess also improves the manageability of remote users and computers, greatly contributes to a secure and flexible network infrastructure, and consequently to IT simplification and cost reduction.

## 1.5 About BitLocker technology

BitLocker Drive Encryption (BitLocker for short) helps keep everything from documents to passwords safer by encrypting the entire drive that Windows and your data reside on. Once BitLocker is turned on, any file you save on that drive is automatically encrypted.

BitLocker helps prevent a thief who boots another operating system or runs a software hacking tool from breaking Windows 8 file and system protections or performing offline viewing of the files stored on the safeguarded drive

[4] CLIENT HYPER-V: http://technet.microsoft.com/en-us/library/hh857623.aspx

Data on a lost or stolen computer is vulnerable to unauthorized access, either by running a software attack tool against it or by transferring the computer's hard disk to a different computer. BitLocker helps mitigate unauthorized data access by enhancing Windows 8 file and system protections.

> **Note:**
>
> *For additional information on this technology, please see the article BITLOCKER DRIVE ENCRYPTION TECHNICAL OVERVIEW[5].*

## 1.6 About the "Hyper-V Windows 8 corporate virtual machine on personal computer" Test Lab

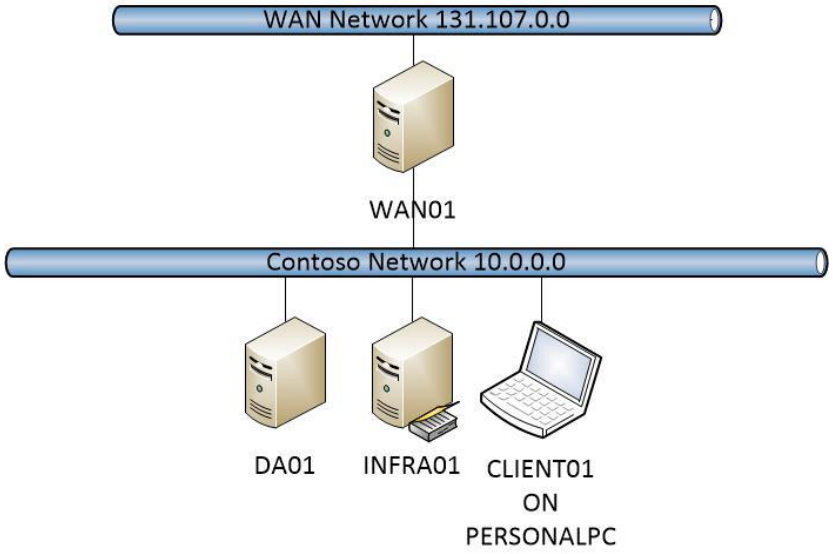
### *1.6.1 "Hyper-V Windows 8 corporate virtual machine on personal computer" Test Lab Overview*

During the construction of the "Hyper-V Windows 8 corporate virtual machine on personal computer" test lab, you will install and configure the following components:

1. Three virtual machines hosted by a physical server (named HYPERV01) as follows;
   - A virtual machine running Windows Server 2012 named INFRA01 that is configured as an intranet domain controller, a Domain Name System (DNS) server, a Dynamic Host Configuration Protocol (DHCP) server and a Windows Deployment Server (WDS) with Microsoft Deployment Toolkit (MDT);
   - An intranet member server running Windows Server 2012 named DA01 that is configured as a remote access server and will offer the DirectAccess functionality;
   - An external standalone server running Windows Server 2012 named WAN01 that is configured as Dynamic Host Configuration Protocol (DHCP) server, NAT Server, DNS server and Web Server (IIS).
2. A physical client computer running Windows 8 Pro named PERSONALPC with Hyper-V role installed that is the host of the following corporate VM:
   - One virtual machine running Windows 8 Enterprise named CLIENT01.
3. Two networks:
   - An intranet for the corporate network, referred to as the ContosoLAN network (10.0.0.0).
   - The external network simulating the Internet for the remote connection scenario, referred to as the ContosoWAN network (131.107.0.0).

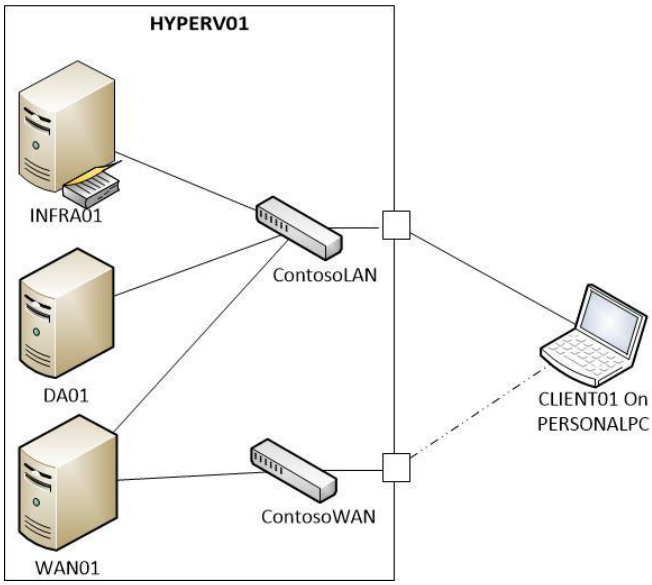
[5] BitLocker Drive Encryption Technical Overview: http://technet.microsoft.com/en-us/library/cc732774(v=WS.10).aspx

The following diagram shows a logical view of the test lab. ContosoLAN is the intranet network and ContosoWAN is the “Internet” network. The client systems can be connected to either one of them.




The second diagram below represents the Hyper-V Host (HYPERV01) and the laptop computer. The Hyper-V host runs three virtual machines that are connected to the virtual network ContosoLAN. The virtual machine WAN01 has a second attachment to the ContosoWAN virtual network.

The host has two physical network adapters with the ContosoLAN virtual network connected to the first adapter and ContosoWAN to the second one. Using an Ethernet cable, the laptop PERSONALPC can be connected to the first network adapter to simulate a connection to the internal corporate network, or on the second one to simulate a remote connection through the WAN01 gateway.



### *1.6.2 Hardware and Software Requirements*

As far as the hardware requirements are concerned, you will need:

- One physical server that supports both the Hyper-V technology and with the minimum amount of RAM required for running this lab in a virtualized environment. As previously outlined, this machine will host the three Windows Server 2012 VMs (INFRA01, DA01, and WAN01) plus the Windows 8 corporate VM.

  The following table lists the several minimum requirements for this machine.

| Requirement | Description |
|---|---|
| Processor | 64-bit dual core with 2.0 gigahertz (GHz) or higher CPU speed |
| Operating system | Windows Server 2012 Standard or Datacenter |
| Memory | 8 gigabytes (GB) of RAM recommended with a minimum of 4 GB |
| Disk drive | 60 GB or more free available space |
| Network | 2 Ethernet network adapters[6] |
| Additional software | The following server role must be added: Hyper-V |

- A physical computer, for instance a laptop, equipped with a processor supporting virtualization technology and the **Second Level Address Translation** (SLAT) capability to allow the Client Hyper-V technology.

> **Important note:**
>
> *Please ensure that Virtualization Technology is enabled in the computer BIOS.*

The following software components are required for installing the test lab:

- The ISO distribution file for Windows Server 2012 (64-bit);
- The ISO distribution file for Windows 8 Pro (64-bit);
- The ISO distribution file for Windows 8 Enterprise (32-bit or 64-bit);
- MDT 2012 Update 1 (available for download on the Microsoft Download Center[7]).
- Windows Assessment and Deployment Kit (available for download on the Microsoft Download Center[8]):
  - Download the file *adksetup.exe* and execute it. Please ensure that the option **Download the Assessment and Deployment Kit for installation on a separate computer** is checked in order to get the whole package. Notice that, due to the size of the package, this step can take a few moments.

[6] It is possible to construct the lab with only one network card but it will require changing the virtual network bindings in order to make the final test. This procedure is not described in the current lab.

[7] Microsoft Deployment Toolkit 2012 Update 1: http://www.microsoft.com/en-us/download/details.aspx?id=25175

[8] Windows Assessment and Deployment Kit: http://www.microsoft.com/en-us/download/details.aspx?id=30652

> **Important note:**
>
> *Run Windows Update on all VMs either during the installation or immediately after installing the operating systems. After running Windows Update, you can isolate your virtual test lab from your production network.*

### *1.6.3 Steps for building the "Hyper-V Windows 8 corporate virtual machine on personal computer" test lab*

This document describes how to build the CoIT Hyper-V Windows 8 corporate virtual machine onto personal computer test lab in seven sections, each of which representing a specific step to establish a working test lab environment.

Please note that each step must be covered in order for a successful completion.

1. HYPER-V SERVER INSTALLATION;
2. WINDOWS SYSTEMS PROVISIONING;
3. NETWORK CONFIGURATION;
4. ACTIVE DIRECTORY DOMAIN CREATION;
5. WDS AND MDT INSTALLATION AND CONFIGURATION;
6. PERSONAL COMPUTER INSTALLATION AND CONFIGURATION;
7. DIRECTACCESS INSTALLATION AND CONFIGURATION;
8. CONFIGURATION OF THE INFRASTRUCTURE SIMULATING THE INTERNET CONNECTIVITY;
9. TEST OF THE CORPORATE VM CONNECTION.

### *1.6.4 Administrative credentials used for the Hyper-V Windows 8 corporate virtual machine on personal computer test lab*

To perform all the tasks in this guide, use the Contoso domain Administrator account for each VM, unless instructed otherwise.

To simplify the steps in this guide, the same password "*Pa$$w0rd*" is used throughout this guide. **This is however NOT mandatory for a real collaboration scenario.**

# 2 Hyper-V Server installation

In this first step, the physical computer, acting as the server hosting the three infrastructure VMs, will be installed with the Windows Server 2012 operating system. Then, the Hyper-V role will be added to allow the creation and configuration of the virtual machines INFRA01, DA01 and WAN01.

To build the Hyper-V Server, proceed as follows:

1. Install Windows Server 2012 Standard or Datacenter with GUI on a physical machine that satisfies the minimal required configuration as previously expressed (see section § 1.6.2 HARDWARE AND SOFTWARE REQUIREMENTS).
2. Enter "*Pa$$w0rd*" when the password is asked.
3. Press the ⊞ key to bring up the start menu and select **Server Manager**.
4. Select **Local Server** then click the computer name**.**
5. In the **System Properties** window, click **Change**.
6. Type **HYPERV01** as the computer name and click **OK** twice, then click **Close** and **Restart Now**.
7. Once the server has restarted, in **Server Manager**, click **Manage**, select **Add Roles and Features**, and then click **Next** three times.
8. On the **Select server roles** screen, check **Hyper-V**, and then click **Add Features**.
9. Click **Next** three times, then select the network adapter who is connected to your internet network and click **Next** three times. Then click **Install**. (Be sure that the cable corresponding to the network card is connected, otherwise the network adapter will not appear in the selection).
10. At the end of the installation click **Close** and restart the computer.

Windows Server 2012 and the Hyper-V role are now correctly installed.

# 3 Windows Systems provisioning

This step describes how to create the three “infrastructure” VMs required for the CoIT “Hyper-V Windows 8 corporate virtual machine on personal computer” test lab environment as previously depicted.

The following table summarizes the VMs along with their role(s) and memory requirement.

| VM Name | Roles | Minimum Required Memory[9] | Recommended Memory |
|---|---|---|---|
| INFRA01 | Domain controller, DNS, DHCP, WDS, MDT | 1.5 GB | 4 GB |
| DA01 | Remote Access | 1 GB | 2 GB |
| WAN01 | DNS, DHCP, IIS | 1 GB | 2 GB |

## 3.1 Create and install the VMs

To create the VMs, proceed as follows, for each VM in the table above:

1. On the start screen, select **Hyper-V Manager**.
2. On the left pane, click **HYPERV01**.
3. On the right pane **Actions** menu, point to **New**, and then click **Virtual Machine**.
4. When the **New Virtual Machine Wizard** appears, click **Next**.
5. On the **Specify Name and Location** page, do the following, and then click **Next**.
   a. In **Name**, type the name of the VM that you are creating as the name of the VM. “*INFRA01*” for example for the INFRA01 VM.
   b. In **Location**, use the default location.
6. On the **Assign Memory** page, in **Memory**, enter the amount of RAM provided in the previous VM description and check **Use Dynamic Memory for this virtual machine**, and then click **Next**.
7. On the **Configure Networking** page, in **Connection**, select the default virtual network switch, and then click **Next**.
8. On the **Connect Virtual Hard Disk** page, click **Next**.
9. On the **Installation Options** page, check **Install an operating system from a boot CD/DVD-ROM**, select the correct DVD Drive or ISO Image of Windows Server 2012, and then click **Finish**.
10. Inside **Hyper-V Manager**, start the virtual machine by selecting the desired virtual machine in the **Virtual Machines** list, click **Start** in the right pane, and then click **Connect**.
11. Install Windows Server 2012 Standard or Datacenter with GUI.
12. Repeat steps 1 through 11 to create all VMs (INFRA01, DA01, and WAN01) before moving to the next step of the process.

[9] With the Hyper-V dynamic memory feature, a server with 4GB of memory can be used to run the Windows Server 2012 host system and the 3 VMs with the minimum memory requirements.

# 4 Network configuration

This section describes the steps that are necessary to create the network components and configure network settings for the VMs.

First, two virtual networks need to be created:

- The ContosoLAN virtual network simulating the Contoso internal network;
- The ContosoWAN virtual network which will be used for simulating a connection from the Internet.

Next, the network connections, IP and DNS settings will be configured for each of the three VMs to allow them to communicate together and offer services to the client computers.

After completion of the previous steps, it is no longer necessary to keep the VMs configured for Internet access through the host server network adapters.

## 4.1 Create the virtual networks

> **Important note:**
>
> *Before creating the two virtual networks, you have to identify the two physical network adapters on the Hyper-V host, and know which one will be connected to the ContosoWAN virtual switch and which will be connected to the ContosoLAN virtual switch.*

All of the VM images must be reconfigured to use an external network interface. The following procedures describe how to create these networks and reconfigure the VMs to use them.

In the steps below, the default virtual network will be renamed ContosoLAN, and a new ContosoWAN virtual network will be created.

To create the **ContosoLAN** virtual network, proceed as follows:

1. Log on to the Hyper-V host server.
2. On the start screen click **Hyper-V Manager**.
3. In **Hyper-V Manager**, on the **Action menu**, click **Virtual Switch Manager**.
4. In the **Virtual Switch Manager** window, on the left side, under **Virtual Switches**, select the existing virtual switch (Note that the name of the switch will reflect the name of the physical NIC).
5. On the right pane change the actual **Name** by **ContosoLAN**.
6. Ensure that **External Network** is checked and that the virtual switch is bound to the correct network adapter: it must be the one you chose to be connected to the Contoso internal network.
7. Click **Apply** (don't close the Virtual Network Manager window now).

To create the **ContosoWAN** virtual network, proceed as follows:

1. In the **Virtual Switch Manager** window, on the left side, click **New Virtual Network**.
2. On the right pane, select **External** for the type of virtual network that you want to create.
3. Click **Create Virtual Switch.**
4. In New Virtual Network, next to **Name**, type "*ContosoWAN*".

5. Under **External**, choose the physical network adapter to bind the new virtual network. It must be the network adapter you chose to be the one connected to the “Internet” network.
6. Click **Apply**, and then **OK**.

> **Note:**
>
> *The virtual network names are case sensitive and should be entered exactly as indicated above.*

At this stage, all three VMs are connected to the ContosoLAN virtual network. However, as previously depicted, the WAN01 VM is a multi-homed server and requires a second network adapter that needs to be connected to the **ContosoWAN** network.

To add a second virtual network adapter to WAN01, follow the next steps:

1. Shutdown the WAN01 virtual machine.
2. From HYPERV01, on the start screen click **Hyper-V Manager**, and then select the WAN01 VM in the **Virtual Machines** list.
3. On the **Action** menu, click **Settings**.
4. Click **Add Hardware**.
5. In the right pane, select **Network Adapter** and then click **Add**.
6. Select the **ContosoWAN** network in the **Virtual Switch** list.
7. Click **OK**.
8. Restart the WAN01 virtual machine.

## 4.2 Configure static IP and DNS settings for each VM

At this stage, all the VMs must be reconfigured to use static IPv4 addresses and Domain Name System (DNS) client settings.

To configure static IP and DNS settings, for each VM proceed as follow:

1. Log on with local admin account.
2. Right click the **Network** icon in the notification toolbar, and then click **Open Network and Sharing Center**.
3. In the **Network and Sharing Center** window, click **Change adapter settings**.
4. In the **Network Connections** window, right-click the connection that you want to manage, and then click **Properties**.
5. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
6. Click **Use the following IP address**, and then type the connection’s IP address, the subnet mask and the Default gateway.
7. In **Preferred DNS server**, type the IP addresses of the DNS server.
8. Click **OK** and then **Close**.

The IP addresses table below provides you the settings for each VM.

| Host/VM | IP Address | Default gateway | DNS |
|---|---|---|---|
| INFRA01 | 10.0.0.1 /24 | 10.0.0.3 | 127.0.0.1 |
| DA01 | 10.0.0.2 /24 | 10.0.0.3 | 10.0.0.1 |
| WAN | 10.0.0.3 /24 (Ethernet)<br>131.107.0.1 /24 (Ethernet 2) | 131.107.0.254 | 127.0.0.1 |

## 4.3 Change the name of computers

The name of each VM computer has to be changed according to the following table.

| VM | Computer Name |
|---|---|
| INFRA01 | INFRA01 |
| DA01 | DA01 |
| WAN01 | WAN01 |

To change computer name, for each VM proceed as follow:

1. Log on with local admin account.
2. On the start screen, type **PowerShell**, then right click **Windows PowerShell** and click the **Run as administrator** circle that appears at the bottom of the screen, if a **User Account Control** prompt appears, click **Yes**.
3. Enter the following command where *<ComputerName>* is listed in the aforementioned table, and press ENTER:

```
Rename-Computer –NewName <ComputerName>
```

4. Enter the following command and then press ENTER:

```
Restart-Computer
```

# 5 Active Directory Domain creation

This step describes how to setup the organization single-domain forest environment based on Active Directory Domain Services (AD DS).

Active Directory Domain Services (AD DS), formerly known as Active Directory, is the central location for configuration information, authentication requests, and information about all objects that are stored within the forest.

Using AD DS, the fictitious company Contoso can efficiently manage users, computers, groups, printers, applications, and other directory-enabled objects from one secure, centralized location.

In this step, you will more specifically create the contoso.com single-domain forest for the Contoso company.

## 5.1 Create the contoso.com single-domain forest

You can use the Add Roles Wizard to create a new Active Directory forest for Contoso. In the wizard pages, use "*Contoso*" as the company name and *"contoso.com*" as the AD DS domain name.

To install AD DS on the INFRA01 VM, proceed as follow:

1. Launch **Server Manager**.
2. On the **Dashboard** screen, under **Configure this local server**, click **Add roles and features**.
3. Click **Next** three times to get to the server role selection screen.
4. In the **Select server roles** dialog, select **Active Directory Domain Services**. Click **Add Features** when prompted, and then click **Next**.
5. In the **Select features** dialog, click **Next**.
6. In the **Active Directory Domain Services** dialog, click **Next**.
7. In the **Confirm installation selections** dialog, click **Install.** Wait for the installation to complete. (Do **NOT** click **Close** button at the end of the installation process).
8. In the **Results** window under the progress bar, click **Promote this server to a Domain Controller**.

> **Note:**
>
> *If you close the **Installation Progress** dialog before it presents the promotion link, click the gray **Tasks** flag in the upper right section of **Server Manager**. When the installation is complete you will see the **Promote this server to a Domain Controller** link.*

9. In the **Deployment Configuration** dialog, select **Add a new forest**. In the **Root domain name** field, type *"contoso.com*". Click **Next.**
10. In the **Domain Controller Options** dialog, leave the default values, specify "*Pa$$w0rd*" as the password twice, and then click **Next** four times to accept default settings for DNS, NetBIOS domain name, and directory paths.
11. In the **Review Options** dialog, review your selections and then click **Next**.

12. In the **Prerequisites Check** dialog, allow the validation to complete and verify that no errors are reported. Since this is the first DNS server deployment in the forest, you can safely ignore all warnings regarding DNS delegation. Click **Install** to start the domain controller promotion. Allow the installation to complete.
13. Allow the domain controller to restart. After the server restarts, logon using the *CONTOSO\Administrator* credentials.

> **Note:**
>
> *The creation of the new single-domain forest will automatically install and configure a DNS Server on the INFRA01 computer.*
>
> *Ensure that the IP addresses are configured as specified in the table in the section § 4.2* CONFIGURE STATIC IP AND DNS SETTINGS FOR EACH VM *of this guide before you attempt to install AD DS. This helps ensure that DNS records are configured appropriately.*

## 5.2 Install and configure the DHCP server

To provide automatic IP configuration on any client devices, you need to deploy a DHCP infrastructure on the intranet. For the purpose of this test lab, we simply install and configure a DHCP server on the INFRA01 computer.

The IP address plan is described in the table below.

| Item | Values |
|---|---|
| Network address | 10.0.0.0 |
| Net mask | 255.255.255.0 |
| Domain name server | 10.0.0.1 |
| DHCP IP address range | 10.0.0.100 to 10.0.0.200 |

To install the DHCP server on the INFRA01 computer, proceed as follows:

1. In the **Dashboard** console of **Server Manager**, under **Configure this local server**, click **Add roles and features**.
2. Click **Next** three times to get to the server role selection screen.
3. In the **Select server roles** dialog, select **DHCP Server**, click **Add Features** when prompted, and then click **Next**.
4. In the **Select features** dialog, click **Next**.
5. Click **Next** on the **DHCP Server** screen, and then click **Install**.
6. Allow the installation to complete, and then in the **Results** window, click the link for **Complete DHCP configuration**.
7. In the **DHCP Post-Install configuration wizard**, click **Next**, and then click **Commit**.
8. On the **Summary** page, click **Close**.
9. In the **Add Roles and Features** Wizard, click **Close**.
10. Press the ⊞ key to bring up the start menu and select **DHCP**.
11. In the DHCP console tree, expand **infra01.contoso.com**. Right-click **IPv4**, and click **New Scope**.

12. Click **Next** in the **New Scope** Wizard.
13. Type **Corpnet** for scope name, and then click **Next**.
14. Next to **Start IP Address**, type "*10.0.0.100*", next to **End IP Address**, type "*10.0.0.200*", and next to **Subnet Mask**, type "*255.255.255.0*".
15. Click **Next** eight times to accept all scope option default settings, and then click **Finish**.
16. Close the **DHCP Manager** console.

## 5.3 Join DA01 to the contoso.com domain

To join DA01 to the *contoso.com* domain, proceed as follows:

1. Log on with local admin account.
2. From the start screen, type **PowerShell**, then right-click **Windows PowerShell** and click **Run as administrator**. If a **User Account Control** prompt appears, click **Yes**.
3. Type the following command and then press ENTER:

```
Add-Computer –DomainName contoso.com –Restart
```

4. Enter "*Administrator*" as username and "*Pa$$w0rd"* as password, and then press **OK**.

## 5.4 Create a test account in the contoso.com domain

After you set up the contoso.com forest, log on as the domain Administrator on the INFRA01 VM and start the **Active Directory Administrative Center** console to create a user account, named **user1** which you will use to test the different scenarios.

| First name | Last name | Full name | User logon name | User logon name (pre-Windows 2000) | Password |
|---|---|---|---|---|---|
| | | User1 | User1 | User1 | Pa$$w0rd |

To create a test account, proceed as follow:

1. Log on the INFRA01 computer with the *CONTOSO\Administrator* credentials.
2. On the start screen, click **Active Directory Administrative Center**.
3. In the console tree, click the arrow to expand **contoso (local)**, and then double-click **Users**.
4. In the **Tasks** pane, click **New**, and then click **User**.
5. In the **Create User** dialog, type "*User1*" next to **Full name** and type "*User1*" next to **User SamAccountName logon: contoso\.**
6. In **Password**, type "*Pa$$w0rd*" for the password, and in **Confirm password**, type the password again.
7. Under Password options, choose **Other password options**, and select **Password never expires**.
8. Click **OK** to close the **Create User** dialog.
9. Exit from the **Active Directory Administrative Center**.

## 5.5 Allow BitLocker without TPM

Since virtual machines do not have access to the Trusted Platform Module (TPM) chip on the physical computer, it was not possible, before Windows 8, to protect virtual machines at rest using BitLocker.

Coming with Windows 8, BitLocker allows using a startup password instead of the TPM chip. This capability will be used to protect the corporate virtual machine hosted by the personal laptop. However, this setting must be enabled on the targeted computers and a GPO will be used to authorize this feature.

- To allow BitLocker without TPM for domain computers, on the INFRA01 VM proceed as follow:

1. On the start screen click **Group Policy Management**.
2. On the left pane, expand **Forest:contoso.com/domains/contoso.com**, right click the **Default Domain Policy** and click **Edit**.
3. On the left pane, navigate to **Computer Configuration / Policies / Administrative Templates / Windows Components / BitLocker Drive Encryption / Operating System Drivers**.
4. Double-click **Require Additional authentication at startup**, then check **Enabled** and check **Allow BitLocker without a compatible TPM** and click **OK**.
5. Close the **Group Policy Management** windows.

> **Note:**
>
> *For simplification purpose, the setting is positioned in the Default Domain Policy and will therefore be applied to all computer accounts in the domain. In a production scenario, a GPO would be created and targeted only to corporate virtual machines.*

# 6 WDS and MDT installation and configuration

In order to reflect as much as possible a real CoIT scenario in the enterprise, we provide as part of this TLG, a mean to automate the deployment of corporate virtual machines to be hosted on the end-user's personal computers.

The objective aims at allowing users to connect to the corporate network with their personal computer and to have at their disposal an automated process for installing the corporate virtual machine.

To implement such a process, we will leverage the Windows Deployment Services included as a role of Windows Server 2012 and the Microsoft Deployment Toolkit (MDT) 2012 Update 1 freely available on the Microsoft Download Center[10].

The Windows Deployment Services role enables to efficiently deploy Windows operating systems. It can be used to set up new computers through a network-based installation without IT Professionals having to be physically present at each computer and without having to install directly from CD or DVD media.

Interestingly enough, Microsoft Deployment Toolkit provides a common console with comprehensive tools and guidance for every organizational role making it the recommended process and toolset to automate large-scale desktop and server deployments.

For deploying Windows 8 or Windows Server 2012 it is necessary to download and install the Windows Assessment and Deployment Kit (ADK), instead of Windows Automated and Installation Kit (AIK), which is proposed by default in the MDT console.

This step describes how to install and configure Windows Deployment Service and the Microsoft Deployment Toolkit.

## 6.1 Install Windows Deployment Service and ADK

- To install Windows Deployment Service on the INFRA01 VM, proceed as follow:
  1. Launch **Server Manager**.
  2. On the **Dashboard** screen, under **Configure this local server**, click **Add roles and features**.
  3. Click **Next** three times to get to the server role selection screen.
  4. In the **Select Server Roles** dialog, select **Windows Deployment Services**. Click **Add Features** when prompted, and then click **Next** four times.
  5. In the **Confirm installation selections** dialog, click **Install**. Wait for the installation to complete and click **Close**.
- Before installing MDT and ADK:
  1. Copy the corresponding packages on the host server (if the download has been made from another machine)
  2. Change the settings of the host network adapter connected to the ContosoLAN switch with an IP address 10.0.0.4 and 255.255.255.0subnet mask.
  3. On the host, share the directory containing the two packages.

[10] Microsoft Deployment Toolkit 2012 Update 1: http://www.microsoft.com/en-us/download/details.aspx?id=25175

4. On the INFRA01 VM, connect to the share in order to access to these installation packages.

To install MDT on the INFRA01 VM, proceed as follow:

1. Launch *MicrosoftDeploymentToolkit2012_x64.msi*.
2. On the welcome screen, click **Next**.
3. Accept the end-user License Agreement, and then click **Next**.
4. On a **Custom Setup** screen, click **Next**.
5. On a **Customer Experience Improvement Program** screen, choose the approriate option and click **Next**, then click **Install** and, at the end of the installation, click **Finish**.

To install ADK on the INFRA01 VM, proceed as follow:

1. Run *adksetup.exe* from the shared directory.
2. On the **Specify Location** screen click **Next**.
3. On the **Join the Customer Experience Improvement Program** screen, choose the appropriate option and click **Next**.
4. Accept the Lience Agreement.
5. Select only **Deployment Tools** and **Windows Preinstallation Environment** and then click **Install**.
6. Once the installation is completed, click **Close**.

## 6.2 Configure Windows Deployment Services and MDT

In this step, a share will be created on the deployment server and a Windows 8 image will be imported on the share. Then, a task sequence will be created that will be used to control the OS installation.

The task sequence will be customized to add the BitLocker script that need to be executed at the end of the OS installation. The default installation settings will be modified to be adapted to the Contoso environment.

Finally, the WDS service is configured to propose the Windows 8 image as an available boot image that can be selected for constructing the corporate virtual machine.

On the INFRA01 VM, to create a deployment share and populate it with the Windows 8 Enterprise image, proceed as follow:

1. On the start screen, launch **Deployment Workbench**.
2. On the left pane, right-click **Deployment Share**, and then select **New Deployment Share**.
3. On the **Path** screen, click **Next**.
4. On the **Share** screen, click **Next**.
5. On the **Descriptive Name**, click **Next**.
6. On the **Options** screen, uncheck all checkbox, and click **Next**.
7. On the **Summary** screen click **Next**.
8. Once the installation is completed, click **Finish** in the **Confirmation** window.
9. Expand **Deployment Share/MDT Deployment Share**, and then right-click **Operating Systems**.

10. Select **Import Operating System**.
11. On **OS Type** screen, check **Full Set of source files**, and then click **Next**.
12. On **Source** screen, click **Browse,** select the Windows 8 source file directory, and then click **Next** three times.
13. Once the installation is completed, click **Finish**.

To create the task sequence, and generate the catalog corresponding to the Windows 8 image:

1. On the **Deployment Workbench console,** expand **Deployment Share/MDT Deployment Share**, right-click **Task Sequences**, and then select **New Task Sequence**
2. In the **Task sequence ID** box, enter "*1*", and, in the field corresponding to **Task sequence name**, enter "*Windows 8*", and then click **Next**.
3. On **Select Template** screen, choose **Standard Client Task Sequence**, and then click **Next**.
4. On the **Select OS** screen, choose **Windows 8 Enterprise**, and then, click **Next**.
5. On the **Specify Product Key**, choose **Do not specify a product key at this time** or, if you have a MAK product key, choose instead **Specify a multiple activation key** and specify the key, and then click **Next**.
6. On the **OS Settings** screen, enter "*Contoso*" as **Organization name**, and then click **Next**.
7. On the **Admin Password** screen, select **Use the specified local Administrator password**, enter "*Pa$$w0rd*" as password twice, and then click **Next** two times.
8. Once the installation is completed, click **Finish** in the **Confirmation** window.
9. Open **Windows Explorer** and navigate to *C:\DeploymentShare\Scripts*.
10. Paste the *bitlocker.bat* script who is delivered with this TLG.
11. Return in the **Deployment Workbench** console, navigate to **Deployment Share/MDT Deployment Share/Task Sequences** and on the middle pane double-click the Windows 8 task.
12. On the **Windows 8 Properties** screen, select **Task Sequence**.
13. In the left pane, select **State Capture** and click **Remove** at the top of this window.
14. Expand **Preinstall** and remove **Offline User State Capture** and **Refresh Only**.
15. Expand **State Restore** and remove **Imaging**, **Restore User State** and **Restore Groups**.
16. Go to **OS Info** tab and click **Edit Unattend.xml**.
17. Wait until the end of the generation of the catalog for the OS image.

To customize the task sequence, follow the next steps:

1. On the Windows System Image Manager, click **Insert/Synchronous Command/Pass 7 oobeSystem.**
2. Enter "*INFRA01\DeploymentShare$\Scripts\bitlocker.bat*", and then click **OK**.
3. Click again **Insert/Synchronous Command/Pass 7 oobeSystem**.
4. Enter "*shutdown –r –t 0*", and click **OK**.
5. Close the **Windows System Image Manager** and click **Yes** to save the changes.
6. On **Windows 8 Properties** screen, click **OK**.
7. On the **Deployment Workbench** console, expand **Deployment Shares,** right-click **MDT Deployment Share**, and then click **Properties**.

8. Click on **Rules** tab and replace the **Default** category by the following list of parameters:

```
[Default]
OSInstall=Y
SkipCapture=YES
SkipAdminPassword=YES
SkipProductKey=YES
SkipDomainMembership=YES
JoinDomain=contoso.com
SkipUserData=YES
SkipComputerBackup=YES
SkipPackageDisplay=YES
SkipBitLocker=YES
HIDESHELL=YES
DISABLETASKMGR=YES
```

The following table summarizes the parameters used in the task sequence and their description:

| Parameter | Description |
|---|---|
| SkipCapture | Skip the screen which allows to capture an already installed OS |
| SkipAdminPassword | Skip the screen which asks for an admin password |
| SkipProductKey | Skip the screen which asks for a product key |
| SkipDomainMembership | Skip the screen which allows to join manually a domain |
| JoinDomain=contoso.com | Allows to automatically join the contoso.com domain |
| SkipUserData | Skip the screen which allows users to save and restore data previously available on the disk. |
| SkipComputerBackup | Skip the screen which allows users to back up the previous Windows installation. |
| SkipPackageDisplay | Skip the screen which allows users to install additional packages. |
| SkipBitLocker | Skip the screen which allows standard activation of BitLocker (with TPM or USB Drive) |
| HIDESHELL | Hide Explorer Shell during Windows installation. Prevent users from interfering with the installation. |
| DISABLETASKMGR | Disable Task manager to prevent users from starting it. |

9. Click **OK**.
10. On the **Deployment Workbench** console, on the left pane, expand **Deployment Shares,** right-click **MDT Deployment Share**, and then click **Update Deployment Share**.
11. On the **Update Deployment Share** Wizard, click **Next** twice, then wait during the files generation, and then click **Finish**.

To configure WDS to use MDT deployment, proceed as follow:

1. On the start screen, click **Windows Deployment Service**.
2. On the left pane expand **Servers,** right-click **INFRA01.contoso.com**, and then select **Configure Server**.
3. On **Windows Deployment Services** Configuration Wizard ,click **Next** three times, answer **Yes** to the warning message, and click **Next**.
4. On the **PXE Server Initial Settings** screen, select **Respond to all client computers,** click **Next** and then **Finish**.
5. Right click again on **INFRA01.contoso.com** and select **All Tasks/Start**, then click **OK**.
6. Expand **INFRA01.contoso.com,** right-click **Boot Images**, then select **Add Boot Image**.

7. On the **Image File** screen, click **Browse** and select the file *C:\DeploymentShare\Boot\LiteTouchPE_x64.wim*, click **Next** three times, and then click **Finish**.

# 7 Personal computer installation and configuration

## 7.1 Install the Windows 8 personal laptop

As already outlined, a Windows 8 physical computer is required to simulate the personal equipment of the user; this computer will NOT be joined to the enterprise domain but will host the Windows 8 corporate VM.

Consequently, on this laptop, the Windows 8 Pro version needs to be installed in order to benefit from the Client Hyper-V feature.

Please use the information hereafter when asked for input:

1. Boot from Windows 8 Pro Setup and launch the install wizard.
2. When the computer reboots, enter the computer name "*PERSONALPC*", and then click **Next**.
3. On the **Wireless** screen, select **Connect to a wireless network later**.
4. On a **Settings** screen, click **Use express settings**.
5. On a **Sign in to your PC** page, click the **Sign in without a Microsoft account**, and then click **Local account**. (This option is not proposed if the computer is not connected to a network).
6. Enter "*localadmin*" as the username and "*Pa$$w0rd*" as the password, and then click **Finish**.

> **Note:**
>
> *You can use the free tool Windows 7 USB-DVD Download Tool[11] to create a bootable USB drive (4GB minimum size) with the Windows 8 Pro image that will allow you to easily proceed to the personal laptop installation.*

## 7.2 Install and configure the Client Hyper-V role

Once Windows 8 Pro is installed on the user's personal laptop, the Client Hyper-V role has to be installed in order to host the corporate virtual machine. Then, the virtual machine needs to be created.

To install Client Hyper-V role on the personal computer, proceed as follow:

1. Open a session on the personal computer.
2. Right click the *InstallHyperV.cmd* script, which is included in this TLG package. You can alternatively paste the following lines in a command-line file that will be named *InstallHyperV.cmd*:

```
powershell Set-ExecutionPolicy RemoteSigned
powershell Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All -NoRestart

@echo Press enter to restart your computer
PAUSE
powershell Restart-Computer
```

[11] Windows 7 USB-DVD Download Tool: http://www.microsoftstore.com/store/msstore/html/pbPage.Help_Win7_usbdvd_dwnTool

3. Click **Run as Administrator**, and then click **Yes** at the prompt.
4. Wait for the script execution to finish, and press ENTER to restart the computer.

The computer will restart two times.

To create the corporate virtual machine on personal computer, proceed as follow:

1. Open a session on the personal computer.
2. Right click the *CreateVM – MDT.cmd* script, which is included in this TLG package. You can alternatively paste the following lines in a command-line file that will be named *CreateVM – MDT.cmd*:

```
@echo Welcome to this workspace creator
@echo off
powershell (New-VMSwitch -Name Network -NetAdapterName Ethernet)

powershell (New-VM -Name CorporateWorkspace -MemoryStartupBytes 1073741824 -BootDevice
LegacyNetworkAdapter -SwitchName Network -NewVHDPath c:\Users\Public\Documents\Hyper-
V\CorporateWorkspace.vhdx -NewVHDSizeBytes 53687091200)

powershell (Set-VMMemory CorporateWorkspace -DynamicMemoryEnabled:$true)

powershell (Disable-VMIntegrationService -VMName CorporateWorkspace  -Name "Time
Synchronization")
@echo Your Workspace is ready to use.
Pause
```

3. Click **Run as Administrator**, and then click **Yes** at the prompt.
4. Wait for the script execution to finish, and press **enter** to close the command prompt.

## 7.3 Install the Windows 8 Enterprise virtual machine

The corporate VM is now created and the last part of the process is the installation of the Windows 8 corporate image. This image is available for deployment through the WDS service that you've previously installed and configured.

To install Windows 8 Enterprise on the virtual machine, proceed as follow:

1. Connect the laptop computer to the network adapter of the Hyper-V server and ensure that you receive an IP address from the DHCP server. (You can also verify that you ping correctly the INFRA01 server).
2. On the personal computer, open a session.
3. On the **Start** screen, type "*Hyper-V*", and then click **Hyper-V manager**.
4. On the **Hyper-V Manager** console, select and double-click the corporate virtual machine created during the previous step.
5. Click **Action**, and then click **Start**.
6. When you are invited, press F12 on the keyboard.
7. Wait during the copy of the installation files (wim image).
8. On the **Welcome screen**, choose your keyboard language, and then click **Run the Deployment Wizard to install a new Operating System**.
9. On the **credentials** screen, enter the domain credentials for User1 :
    - User Name: *User1*
    - Password: *Pa$$w0rd*
    - Domain: *contoso.com*

10. Select the **Windows 8** task and then click **Next**.
11. Enter CLIENT01 as computer name and click **Next**.
12. Choose your regional settings and click **Next**.

> **Important Note:**
>
> *If the keyboard layout you are using is not US (for example French), you have to select the same format for Time and currency otherwise the default keyboard will be US (even if the French keyboard layout is installed).*

13. Click **Begin** to launch the installation.
14. Wait during the installation process and, on the confirmation screen, click **Finish**.
15. When the command prompt appears corresponding to the execution of the *BitLocker.cmd* script, enter the BitLocker password of your choice twice to activate BitLocker. (The password must be at least 8 characters). The computer will restart.

Please note that the BitLocker password that you will have to enter at each boot of the virtual machine **uses a QWERTY keyboard**.

> **Note:**
>
> *If the VM clock is synchronized with the personal laptop clock and that there is a delay between the INFRA01 VM and the laptop, the BitLocker GPO will not apply on the VM, the BitLocker.bat script will throw an error and BitLocker protection will not be installed.*

## 7.4 Start the corporate virtual machine

This step explains how to start the corporate virtual machine on the personal computer.

To start the corporate virtual machine on the personal laptop, proceed as follows:

1. Open a session under the local account localadmin.
2. On the **Start** screen, type "*Hyper-V*", and then click **Hyper-V manager**.
3. Inside the **Hyper-V Manager** console, select and double-click the corporate virtual machine.
4. Click **Action**, then click **Start.**
5. Enter the BitLocker password when prompted.
6. Log on with the User1 account in the CONTOSO domain.

For a more convenient usage, you can adjust the screen resolution of the VM to match the one used for the host.

# 8 DirectAccess installation and configuration

## 8.1 Install the Remote Access role

The Remote Access server role in Windows Server 2012 combines the DirectAccess feature and the former Routing and Remote Access Services (RRAS) server role into a new unified server role.

This new Remote Access server role allows centralized administration, configuration, and monitoring of both DirectAccess and VPN-based remote access services.

Use the following procedure to install the Remote Access role on DA01.

To install the Remote Access role on the DA01 computer, proceed as follows:

1. Log on the DA01 computer using the *CONTOSO\Administrator* account.
2. Launch **Server Manager**.
3. On the **Dashboard** screen, under **Configure this local server**, click **Add roles and features**.
4. Click **Next** three times to get to the server role selection screen.
5. In the **Select Server Roles** dialog, select **Remote Access**. Click **Add Features** when prompted, and then click **Next**.
6. In the **Select features** dialog, click **Next**.
7. In the **Remote Access** dialog, click **Next**.
8. In the **Select role services** dialog, verify that the option **DirectAccess and VPN (RAS)** is checked and click **Next** three times, then click **Install**.
9. Allow the installation to complete, and then in the **Results** window click **Close**.

## 8.2 Create a security group for DirectAccess computers

When DirectAccess is configured, a Group Policy Object (GPO) containing DirectAccess settings is created automatically. Please note that these settings are applied to DirectAccess clients and servers.

By default, the Getting Started Wizard applies the client GPO to computers belonging to the Domain Computers security group and detected as mobile computers through a WMI filter.

With this default setting the Hyper-V Windows 8 Corporate VM would not be detected as mobile computer and the DirectAccess GPO would not be applied. Consequently, the procedure in this lab will not use the default setting, but instead create an alternate security group for DirectAccess clients.

To create a DirectAccess Client security group, proceed as follows:

1. Log on INFRA01 computer with the *CONTOSO\Administrator* credentials.
2. On the start screen, click **Active Directory Administrative Center**.
3. In the console tree, click the arrow to expand **contoso (local)**, and then click **Users**.
4. In the **Tasks** pane, click **New**, and then click **Group**.
5. In the **Create Group** dialog, type "*DA_Group*" as the group name.
6. Scroll down to access the **Members** section of the **Create Group** dialog, and click **Add**.
7. Click **Object Types**, select **Computers**, and click **OK**.

8. Type "*CLIENT01*" and then click **OK**.
9. Click **OK** to close the **Create Group** dialog.
10. Exit the **Active Directory Administrative Center**.

## 8.3 Configure Remote Access role

You now need to configure DirectAccess in a single server deployment using the **Remote Access Setup** Wizard.

To configure the Remote Access role on the DA01 computer, proceed as follows:

1. Log on the DA01 computer using the *CONTOSO\Administrator* account.
2. On the start screen, click **Remote Access Management Console**.
3. In the **Remote Access Management Console**, click **Run the Getting Started Wizard**.
4. In the **Configure Remote Access** screen, click **Deploy DirectAccess only**.
5. Select **Behind an edge device (with a single network adapter)**, type "*remote.contoso.com*" in the textbox as the public name address, and then click **Next**.
6. Click the **here** link to edit default settings.
7. In the **Remote Access Review** screen, next to **Remote Clients** click **Change…**
8. Click **Domain computers** and then **Remove**.
9. Click **Add…**, type "*DA_Group*", and then click **OK**.
10. Uncheck **Enable DirectAccess for mobile computers only**, click **Next** and then **Finish**.
11. In the **Remote Access Review** screen, click **OK**, and then, in the **Configure Remote Access** screen, click **Finish**.

> **Note:**
>
> *At the end of the configuration a warning message appears: this is an expected behavior and you can click Close.*

## 8.4 Create a shared folder on INFRA01

A shared folder is now created on INFRA01 to demonstrate the ability to connect to a SMB share over the DirectAccess connection.

To create a shared folder on INFRA01, proceed as follows:

1. Log on INFRA01 computer with the *CONTOSO\Administrator* credentials.
2. On the start screen click **Computer**.
3. Double-click **Local Disk (C:)**.
4. Create a new Folder and name it **Share**.
5. Right-click the **Share** folder and select **Properties**.
6. On the **Share Properties** dialog box, on the **Sharing** tab, click **Advanced Sharing**.

7. Check **Share this folder**. Accept the default share name, which is Share, and click **OK** then **Close**.
8. Double-click the **Share** folder.
9. Create a **New Text Document**.
10. Double-click the **New Text Document.txt** file.
11. In the **New Text Document.txt – Notepad** window, type "*This is a text document on INFRA01*".
12. Close Notepad. On the Notepad dialog box, click **Save** to save the changes.
13. Close Windows Explorer.

# 9 Configure the infrastructure simulating the Internet connectivity

The WAN01 VM will be used to:

- Simulate Internet connectivity;
- And allow to implementation of the full scenario where the personal computer hosting the corporate VM is connected from outside the corporate network through an Internet connection (for example at home or at the hotel).

The WAN01 VM will consequently provide the following services on the network card connected to the ContosoWAN network:

1. The **NAT gateway** is the only service directly exposed to the internet and is used to provide access to the internal network as well as protecting the DirectAccess server.

> **Note:**
>
> *This feature, available in the DirectAccess version of Windows Server 2012, is an enhancement compared to Windows Server 2008 R2 and that implementing DirectAccess no longer requires two consecutive IPv4 public addresses. The NAT gateway role will be provided in this lab by the Remote Access role of Windows Server 2012 but could be implemented by an external non-Windows NAT solution.*

2. The **DHCP service** is used to assign automatically an IPv4 address to the personal computer simulating the IP address given in a real case by the Internet provider.
3. The **DNS service** offers name resolution for the client connected to the ContosoWan network in order to resolve the name of the remote access and NCSI services (see below).
4. The **Network Connectivity Status Indicator (NCSI) service** is used by the Windows 8 computer to allow DirectAccess to determine if the computer is connected to the internet.

   NCSI examines the connectivity of a network in a variety of ways but more specifically by trying to connect to http://www.msftncsi.com, a simple Web site that exists only to support the functionality of NCSI, and to request for page called ncsi.txt, which contains the following line of text with no terminating new line or other non-printing characters: "*Microsoft NCSI*".

> **Important note:**
>
> *For additional information, see for instance APPENDIX H: NETWORK CONNECTIVITY STATUS INDICATOR AND RESULTING INTERNET COMMUNICATION IN WINDOWS 7 AND WINDOWS SERVER 2008 R2[12] on the Microsoft TechNet.*

[12] APPENDIX H: NETWORK CONNECTIVITY STATUS INDICATOR AND RESULTING INTERNET COMMUNICATION IN WINDOWS 7 AND WINDOWS SERVER 2008 R2: http://technet.microsoft.com/en-us/library/ee126135(v=WS.10).aspx

## 9.1 Install and configure the NAT Server

To provide the NAT router feature on the external ContosoWAN network, the Remote Access role of Windows Server 2012 need to be installed and configured.

To install the remote access role on WAN01 computer, proceed as follows:

1. Log on the WAN01 computer using the *Administrator* account.
2. Launch **Server Manager**.
3. On the **Dashboard** screen, under **Configure this local server**, click **Add roles and features**.
4. Click **Next** three times to get to the server role selection screen.
5. In the **Select Server Roles** dialog, select **Remote Access**. Click **Add Features** when prompted, and then click **Next**.
6. In the **Select features** dialog, click **Next**.
7. In the **Remote Access** dialog, click **Next**.
8. In the **Select role services** dialog, select **DirectAccess and VPN (RAS)** and **Routing** and click **Next** three times, then click **Install**.
9. Allow the installation to complete, and then in the **Results** window click **Close**.

> **Note:**
>
> *Even if only the Routing feature is necessary, the DirectAccess and VPN feature will be installed.*

To configure the NAT translation on WAN01 computer, proceed as follows:

1. Log on the WAN01 computer using the *Administrator* account.
2. On the start screen, click **Routing and Remote Access**.
3. On the **Routing and Remote Access** screen, on the left pane, right-click **WAN01 (local)**, and then choose **Configure and Enable Routing and Remote Access**.
4. On the welcome screen, click **Next**.
5. On the configuration screen, check **Network address translation (NAT)**, and then click **Next**.
6. On the **NAT Internet Connection** screen, ensure that **Use this public interface to connect to the Internet** is checked and select **Ethernet2** network interface with the **131.107.0.1** IP Address. Click **Next**.
7. On the **Name and Address Translation Services** screen, select **I will setup name and address services later,** click **Next**, and then **Finish**.

To allow IP/HTTPS traffic to the Direct Access server, on the WAN01 computer proceed as follows:

1. Still on the **Routing and Remote Access** console, expand **WAN01 (local) / IPv4** and click **NAT**.
2. Right-click the **Ethernet2** network interface and select **Properties**.
3. Go to **Services and Ports** tab and check **Secure Web Server (HTTPS)**.
4. In **Private address** field, type "*10.0.0.2*", and then click **OK** twice.
5. Close the **Routing and Remote Access** console.

> **Note:**
>
> *If the NAT feature does not appear under WAN01 (local) / IPv4, you will need to set it up manually. Please refer to the procedure description in Annex A.*

## 9.2 Install and configure the DHCP Server

The DHCP service needs to be deployed on the ContosoWAN network to provide an automatic IP configuration for client devices.

For the purpose of this test lab, the DHCP role has to be installed and configured on the WAN01 computer.

The IP address plan is described in the table below.

| Item | Values |
|---|---|
| Network address | 131.107.0.0 |
| Subnet mask | 255.255.255.0 |
| Default gateway | 131.107.0.1 |
| Domain name server | 131.107.0.1 |
| DHCP IP address range | 131.107.0.100 to 131.107.0.200 |

To install the DHCP server on the WAN01 computer, proceed as follows:

1. In the **Dashboard** console of Server Manager, under **Configure this local server**, click **Add roles and features**.
2. Click **Next** three times to navigate to the server role selection screen.
3. In the **Select server roles** dialog, select **DHCP Server**, click **Add Features** when prompted, and then click **Next**.
4. In the **Select features** dialog, click **Next**.
5. Click **Next** on the DHCP Server screen, and then **Install**.
6. Once the installation is completed, in the **Results** window, click the link for **Complete DHCP configuration**.
7. In the **DHCP Post-Install configuration wizard**, click **Commit**.
8. On the **Summary** page, click **Close**.
9. In the **Add Roles and Features Wizard**, click **Close**.

> **Important note:**
>
> *In this demonstration lab, WAN01 is a multi-homed server connected to both the ContosoLAN and ContosoWAN networks. During the installation process, the DHCP Server role checks if another DHCP Server is executed on all accessible networks. If this is the case, the DHCP Server activation is forbidden.*
>
> *As the INFRA01 server already offers the DHCP service on the ContosoLAN network, this detection must be disabled to allow the DHCP installation on the ContosoWAN network.*
>
> *Note that this setting is applicable in a demonstration context but must not be reproduced in a production environment.*

10. On the **Start** screen, type "*regedit*" and press ENTER.
11. Create and set the following registry key (the key does not exist by default):

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DHCPServer\Parameters

Value name: DisableRogueDetection
Data type: REG_DWORD
Value data: 1
```

12. Close **Registry Editor** and restart the computer.
13. On the start screen, click **DHCP**.
14. In the DHCP console tree, expand **wan01**. Right-click **IPv4**, and then click **New Scope**.
15. Click **Next** in the New Scope Wizard.
16. Type **Internet** for scope name, and then click **Next**.
17. Next to **Start IP Address**, type "*131.107.0.100*", next to **End IP Address**, type "*131.107.0.200*", and next to **Subnet Mask**, type "*255.255.255.0*".
18. Click **Next** four times. Specify "*131.107.0.1*" as the Default Gateway. Click **Add**, and then click **Next** four times to accept all scope option default settings.
19. Click **Finish** and close the DHCP Manager console.

## 9.3 Install the DNS Server role

To install the DNS role on WAN01 computer, proceed as follows:

1. On the Server Manager **Dashboard** screen, under **Configure this local server**, click **Add roles and features**.
2. Click **Next** three times to move forward to the server role selection screen.
3. On the **Select Server Roles** page, select **DNS Server** and click **Add Features** when prompted, and then click **Next** three times to accept the default DNS server settings. Finally, click **Install.**
4. Verify that the installation is successful, and then click **Close**.

## 9.4 Configure the NCSI site

As previously described, to determine Internet connectivity, a Windows client attempts to request the http://www.msftncsi.com/ncsi.txt URL and should resolve the FQDN name *www.msftncsi.com*.

In the following procedure, the ncsi.txt file is created in the IIS wwwroot directory of WAN01.

To configure the NCSI web site on WAN01, proceed as follows:

1. On the WAN01 computer, launch **Windows Explorer**, and then navigate to *C:\inetpub\wwwroot*.
2. In the details pane, right-click an empty area, point to **New**, and then click **Text Document**.
3. Rename the document to *ncsi*.
4. Double-click **ncsi**.
5. In the **Notepad** window, type "*Microsoft NCSI"* but do not press ENTER to add a new line.
6. Click **File**, and then click **Exit**. In the **Notepad** dialog box, click **Save**.
7. Close the Windows Explorer window.

## 9.5 Configure DNS Server

Next, the DNS server has to be configured to provide the name resolution for the FQDN names *www.msftncsi.com* and *remote.contoso.com*.

To configure the DNS Server on WAN01, proceed as follows:

1. On the start screen, click **DNS**.
2. In the console tree of DNS Manager, expand **WAN01**.
3. Right-click **Forward Lookup Zones**, click **New Zone**, and then click **Next**.
4. On the **Zone Type** page, click **Next**.
5. On the **Zone Name** page, type **contoso.com**, and then click **Next**.
6. Click **Next** twice to accept defaults for zone file and dynamic update, and then click **Finish**.
7. In the console tree, select and right-click **contoso.com**, then click **New Host (A or AAAA).**
8. In **Name**, type **remote** in the **IP address** field, type "*131.107.0.1*". Click **Add Host** then **OK** and **Done**.
9. Right-click **Forward Lookup Zones**, click **New Zone**, and then click **Next**.
10. On the **Zone Type** page, click **Next**.
11. On the **Zone Name** page, type **msftncsi.com**, then click **Next**.
12. Click **Next** twice to accept defaults for zone file and dynamic update, and then click **Finish**.
13. In the console tree, select and right-click **msftncsi.com**, and then click **New Host (A or AAAA).**
14. In **Name**, type **www** in the **IP address** field, type "*131.107.0.1*". Click **Add Host** then **OK** and **Done**.
15. In the console tree, right-click **msftncsi.com**, and then click **New Host (A or AAAA).**
16. In Name, type **dns** in the **IP address** field, type "*131.107.255.255*". Click **Add Host** then **OK** and **Done**.
17. Close the **DNS Manager** console.

# 10 Test the Corporate VM remote connection

If all previous steps have been completed successfully, the DirectAccess connection between the corporate virtual machine and the Contoso corporate network can be tested.

Before testing the connection, you must apply the GPO created during the DirectAccess setup process to the client corporate VM.

1. Using an Ethernet cable, connect the personal computer to the **ContosoLAN** network card.
2. Open a session under the local account **localadmin**.
3. On the **Start** screen, type "*Hyper-V*", and then click **Hyper-V manager**.
4. On the **Hyper-V Manager** console, double-click the corporate virtual machine CLIENT01.
5. Click the **Action** menu, and then click **Start.**
6. Enter the BitLocker password when prompted. (The keyboard is in QWERTY).
7. Log on with the *User1* account in the CONTOSO domain.
8. On the **Start** screen, type "*cmd*" and press ENTER.
9. On the command prompt, type the following command and press ENTER.

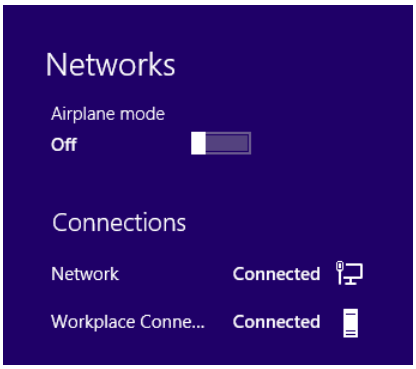
```
gpupdate /force
```

10. Wait for the command to complete.

> **Important note:**
>
> *Please check that there is **no error message** when applying the GPO. In case of problem, verify that you can ping the 10.0.0.1 address then INFRA01. Some network cards could not function correctly with Hyper-V and DirectAccess; in this case, just try to swap the bindings between ContosoLAN and ContosoWAN before retesting. It could be necessary to reboot the three server VMs to take in account the network change.*

We will finally test the scenario where the personal computer and the corporate VM are connected to the internet

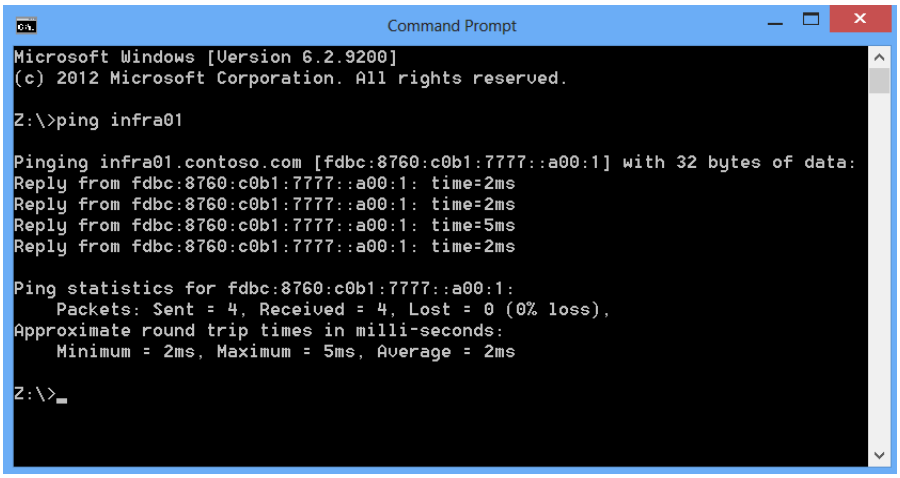
1. Disconnect the Ethernet cable from the **ContosoLAN** network card and connect it to the **ContosoWAN** network card to simulate a connection of the personal computer to the internet.
2. Restart the virtual machine computer (not the personal host computer).
3. After reboot, click the **Networks icon** on the **notification area** and verify that the **Workplace Connection** status is Connected (see below).




4. Verify you can ping the domain controller: switch to the **Start** screen, then type "*cmd*" and press ENTER.
5. On the command prompt, type the following command and press ENTER.

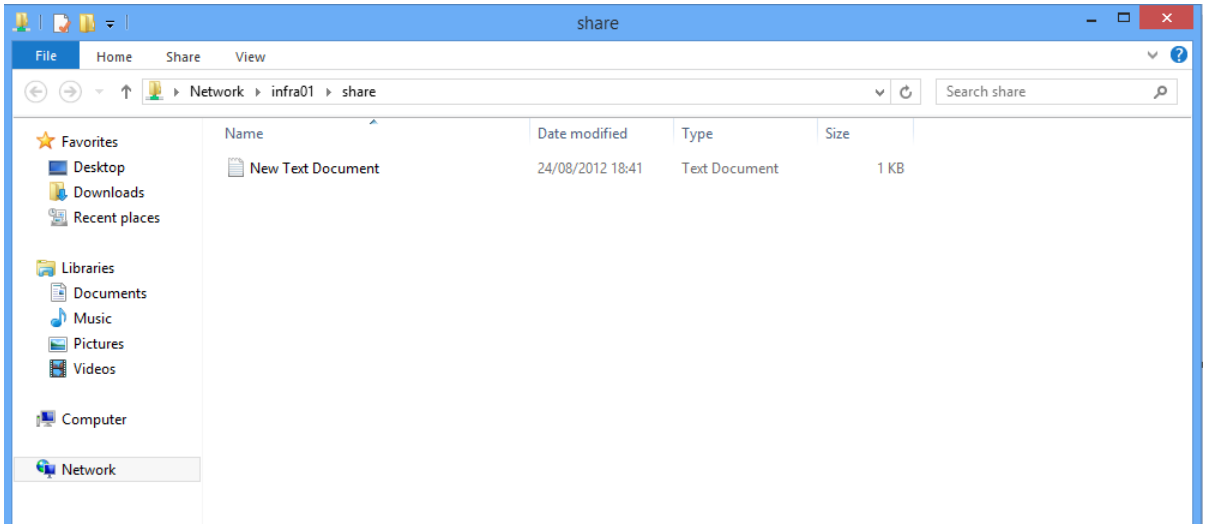
```
ping infra01
```

The response must specify an IPv6 address as illustrated hereafter.



6. Verify you can access to the shared folder named *Share* on INFRA01. On the **Start** screen, type "*infra01**Share*", and then press ENTER.

   If steps have been completed successfully, the DirectAccess connectivity should be available and you should see a folder window with the *New Text Document* file as illustrated hereafter.




Congratulations! You now have a Windows 8 corporate virtual machine protected by BitLocker and anytime connected to your workplace. This concludes this part of TLG.

If you are interested to implement the new Windows To Go feature of Windows 8, you can continue to the optional part of this lab.

# 11 Optional: Create and configure Windows To Go

Based on the previous infrastructure that has been built to implement the corporate Client Hyper-V VM scenario, it is possible, with just a few extra steps, to extend it and to experiment the Windows To Go scenario.

As previously mentioned, this scenario is also described in another TLG of the series Consumerization of IT entitled CONSUMERIZATION OF IT TEST LAB GUIDE: WINDOWS TO GO WITH DIRECTACCESS[13].

In this Windows To Go scenario, the personal laptop of the employee can be used to boot the Windows 8 corporate image from the USB drive or key, and allows a seamless and secure connection to the corporate network based on the DirectAccess technology.

In addition, the corporate image is encrypted by the BitLocker technology to avoid, in case of stolen or lost USB drive/key, access to sensitive information. This protection also imposes the knowledge of the BitLocker password to boot from the corporate image. Furthermore, in order to access to the corporate network and resources, the employee must enter their corporate credentials to open a Windows session on the corporate Active Directory domain.

Please note that, as a prerequisite to complete this section, you will need:

- **A new laptop that will be installed with Windows 8 Entreprise edition** which is the only version supporting the Windows To Go feature.
- An **external USB drive or USB Key** compatible with Windows To Go feature.

## 11.1 About Windows To Go technology

Windows To Go is a new feature in Windows 8 Enterprise Edition that enables you to provision a USB drive with a complete, managed Windows 8 system image. A user can then insert the USB drive (known as a Windows To Go workspace) into a managed or unmanaged host computer to boot and run a managed Windows 8 system.

Interestingly enough, you don't have to install any software on the host computer to use the Windows To Go workspace. For example, you might want to provide a company-owned Windows To Go workspace to a staff member who uses their own non-domain-joined computer at work. The Windows To Go workspace provides a domain-joined computer experience for this user, without modifying their personal consumer device. As another example, you might want to create a Windows To Go workspace for yourself that you can use on a home computer that isn't running Windows 8.

> **Note:**
>
> *For more information about the Windows To Go technology, please see the article WINDOWS TO GO: FEATURE OVERVIEW[14].*

[13] CONSUMERIZATION OF IT TEST LAB GUIDE: WINDOWS TO GO WITH DIRECTACCESS: http://www.microsoft.com/en-us/download/details.aspx?id=29990

[14] Windows To Go: Feature Overview: http://technet.microsoft.com/library/hh831833.aspx

## 11.2 Install the Windows 8 Enterprise laptop

As already outlined, a Windows 8 physical computer is required to install **Windows 8 Enterprise**. It will be used to generate the Windows To Go bootable drive.

Please use the information hereafter when asked for input:

1. Boot from Windows 8 Enterprise Setup and launch the install wizard.
2. When the computer reboots, enter the computer name "*W8ENT*", and then click **Next**.
3. On the **Wireless** screen, click **Connect to a wireless network later**.
4. On the **Settings** screen, click **Use express settings**.
5. On the **Sign in to your PC** screen, click **Sign in without a Microsoft account**, and then select **Local account** (This option is not proposed if the computer is not connected to a network).
6. Enter "*localadmin*" as the username and "*Pa$$w0rd*" as the password, and then click **Finish**.

> **Important note:**
>
> *Do not add the W8ENT laptop in the Contoso domain.*

## 11.3 Install the Windows To Go USB Drive

The computer that has just been installed with the Windows 8 Enterprise operating system will now be used to build a bootable USB drive corresponding to the corporate image. In a real production scenario, the image that will be copied on the drive would be a customized corporate image.

To install a Windows To Go Workspace on a compatible bootable USB Drive, proceed as follow:

1. Log on with *localadmin* account on W8ENT.
2. On the **Start** screen, type "*Windows To Go*". The results will be **No apps match your search**.
3. Click **Settings** on the right of the screen under the **Search** field.
4. Click **Windows To Go**.
5. Insert a compatible USB drive, select it in the device list, and then click **Next**.
6. On the **Choose a Windows 8 image** page, click **Add search location.**
7. Choose the location of your Windows 8 source, select **Windows 8 Enterprise** in the list, and then click **Next**.

   If you have at your disposal the Windows 8 Enterprise .iso file, just mount using a right-click and then select the mounted unit as source location.
8. On the **Set BitLocker password (optional)** page, check **Use BitLocker with my Windows To Go workspace**, and then enter "*Pas$$w0rd*" twice and click **Next**.
9. On the **Ready to create your Windows To Go workspace** page click **Create.** (This might take a while).
10. On the **Choose a boot option** page select **Yes** to allow the PC to reboot on the Windows To Go Drive then click **Save and close.**

At this stage, the Windows To Go Workspace device is ready to use and the W8ENT laptop is configured to automatically start on the USB device when it is connected.

## 11.4 Start on the Windows To Go USB Drive

Now that the USB drive is built to host the corporate Windows 8 image, the laptop that has been used to generate the USB device will be used as the personal employee PC.

To boot the personal PC with the corporate image, proceed as follows:

1. Connect the Windows To Go USB Drive on the W8ENT laptop.
2. Start the laptop. It should automatically boot on the USB Drive.

> **Important note:**
>
> *If your computer does not boot automatically on the Windows To Go Workspace, please appropriately change the boot order on your BIOS.*

3. On the **BitLocker drive encryption** screen, type "*Pa$$w0rd*" and press ENTER. (Please remember that the BitLocker password you will have to enter at each boot of the machine uses a QWERTY keyboard).
4. Wait for the "*Getting devices ready*" phase to complete. This phase will execute only the first time the OS boots on this laptop to allow devices detection.
5. The laptop will reboot and you will be asked again for the BitLocker password.
6. On the **Licence terms** screen, check **I accept the license terms for using Windows**, and then click **Accept**.
7. Enter the computer name "*CLIENT02*", and then click **Next**.
8. On the **Wireless** screen, click **Connect to a wireless network later**.
9. On the **Settings** screen, click **Use express settings**.
10. On the **Sign in to your PC** screen, select **Sign in without a Microsoft account** and then click **Local account**. (This option is not proposed if the computer is not connected to a network).
11. Enter "*localadmin*" as the username and "*Pa$$w0rd*" as the password, and click **Finish**.

## 11.5 Join the Windows To Go computer to the contoso.com domain

The corporate image needs now to be joined the Active Directory domain in order to be managed as a regular corporate computer and because this is also a prerequisite to benefit from a DirectAccess connection.

To join CLIENT02 to the *contoso.com* domain, proceed as follows:

1. Check that the laptop network cable is connected to the Hyper-V server network card corresponding to the ContosoLan virtual network.
2. Log on with the local admin account.
3. On the **Start** screen, type "*PowerShell*", right-click **Windows PowerShell**, and then click **Run as administrator**. If a **User Account Control** prompt appears, click **Yes**.

4. Type the following command and then press ENTER:

```
Add-Computer –DomainName contoso.com –Restart
```

5. Enter "*Administrator*" as username and "*Pa$$w0rd"* as password, and then click **OK**.
6. The machine will reboot.

## 11.6 Add the Windows To Go computer account to the DA_Group

The corporate image computer account must be added to the DA_Group so that the DirectAccess GPO could be applied to allow DirectAccess connection to be effective.

To add CLIENT02 to the DA_Group, proceed as follows:

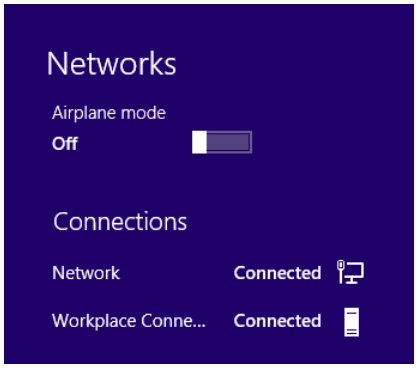
1. Log on to INFRA01 with the contoso admin account.
2. On the **Server Manager Dashboard**, select **Tools** and then **Active Directory Users and Computers**.
3. Navigate to the OU *contoso.com\Computers*, right-click **CLIENT02** and click **Add Group**…
4. Enter **DA_Group** and then click **OK** to validate.
5. On the **Start** screen, type "*PowerShell*", right-click **Windows PowerShell**, and then click **Run as administrator.** If a **User Account Control** prompt appears, click **Yes**.

# 12 Test the Windows To Go connection

If all previous steps have been completed successfully, the DirectAccess connection between the corporate Windows To Go Workspace and the Contoso corporate network can now be tested.

To test the connection on CLIENT02, proceed as follows:

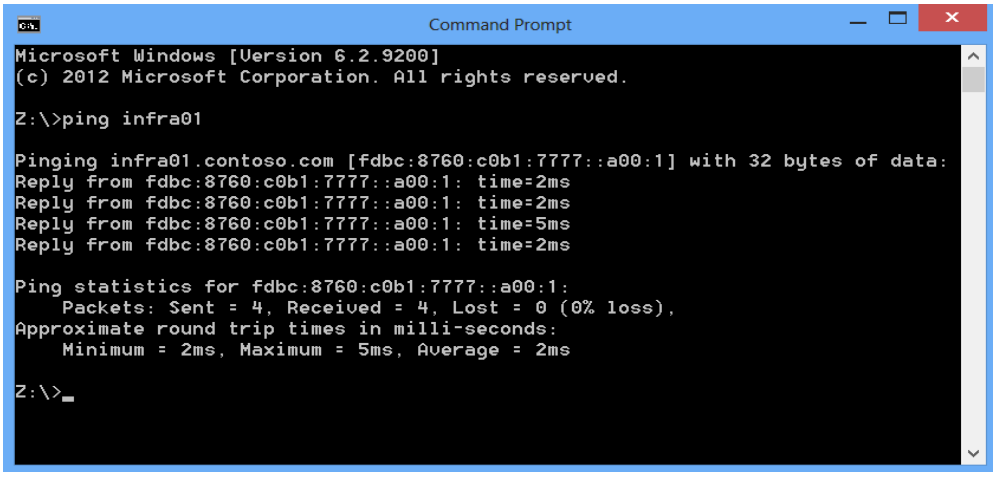
1. Ensure that the network cable is always connected to the Hyper-V server network card corresponding to the ContosoLan virtual network.
2. Restart the laptop with the Windows To Go Workspace USB device connected.
3. Specify the BitLocker password when prompted. After this reboot, the CLIENT02 computer will received the DirectAccess GPO targeted to computer accounts belonging to the DA_Group.
4. Log on with the *User1* account in the CONTOSO domain.
5. Disconnect the Ethernet cable from Hyper-V server network card corresponding to the **ContosoLan** virtual network and connect it to the NIC bound to the **ContosoWAN** virtual network.
6. Wait for the network detection.
7. Check that the **Workplace Connection** has a **Connected** status by clicking the **Networks icon** in the **notification area**.




8. Verify you can ping the domain controller: open the **Start** screen, then type "*cmd*" and press ENTER.
9. On the command prompt, type the following command and press ENTER:

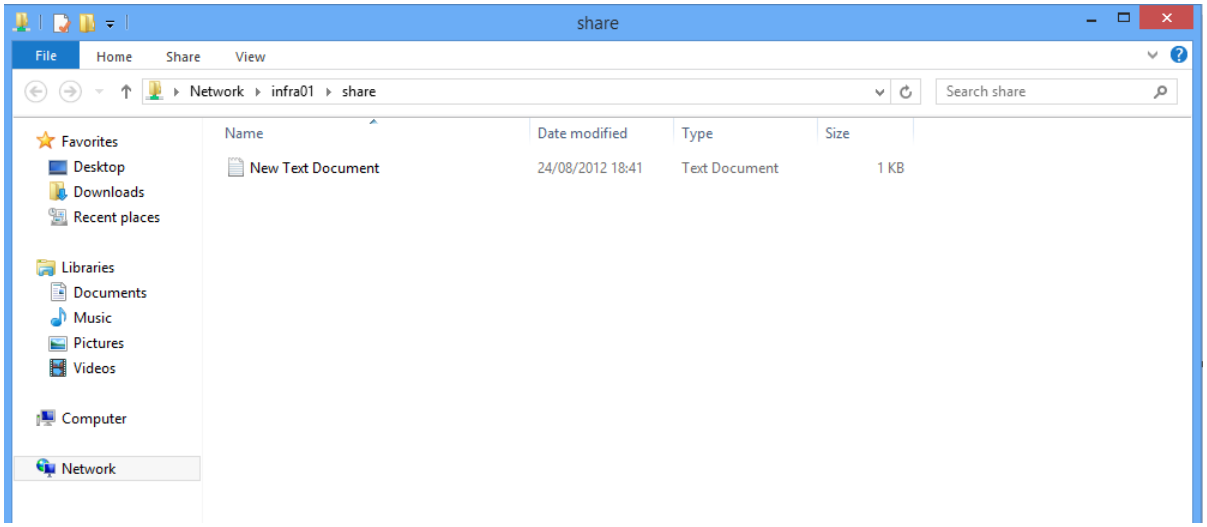
```
ping infra01
```

The response must specify an IPv6 address as illustrated hereafter.




10. Verify you can access to the shared folder named *Share* on INFRA01. On the **Start** screen, type "*infra01**Share*", and then press ENTER.

    If steps have been completed successfully, the DirectAccess connectivity should be available and you should see a folder window with the New Text Document file.




Congratulations! You have implemented a scenario where a with a Windows 8 bootable USB drive protected by BitLocker, can be used to boot from a personal PC to offer a corporate Windows 8 system connected by DirectAccess to the corporate network.

This concludes this TLG.