

INSTALL AGENT IN SILENT MODE

Version 6.0

January 2, 2024



Legal Notice

Copyright© 2023 DigiCert, Inc. All rights reserved. DigiCert and its logo are registered trademarks of DigiCert, Inc. Other names may be trademarks of their respective owners.

The product described in this document is provided by DigiCert, Inc. and distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of DigiCert, Inc. and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. DIGICERT, INC. SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The licensed software and documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the licensed software and documentation by the U.S. Government shall be solely in accordance with the terms of this documentation.

DigiCert, Inc.
2801 North Thanksgiving Way, Suite 500
Lehi, UT 84043
<https://www.digicert.com>

Table of Contents

INSTALLING THE AGENT IN SILENT MODE ON WINDOWS OR LINUX	4
OVERVIEW	4
KEY-BASED AUTHENTICATION	4
WHY USE A COMPANION APPLICATION?	4
PREREQUISITES.....	5
BUILD THE COMPANION APPLICATION ON WINDOWS OR LINUX.....	5
BUILD AND DEPLOY A GLOBAL POLICY OBJECT (GPO) MSI BUNDLE ON WINDOWS	6
WINDOWS: INSTALL AGENT.....	8
LINUX: INSTALL AGENT	8
1. Prepare the package	8
2. Install the agent	8
APPENDIX A: GROUP POLICY OBJECT (GPO)	10
DEPLOY AGENTS THROUGH GROUP OBJECT POLICY	10
1. Create a distribution point.....	11
2. Create a Group Object Policy.....	11
3. Logon scripts for Group Object Policy	11
APPENDIX B: AUTOMATE AGENT DEPLOYMENT USING ANSIBLE	13
OVERVIEW	13
PREREQUISITES.....	13
DEPLOY AGENT THROUGH ANSIBLE	14
1. Install the Ansible.....	14
2. Verify the version.....	14
3. Update the configuration files	14
4. Install the agent	17
APPENDIX C: PSEXEC BASED AGENT PUSH FOR WINDOWS.....	19
PREREQUISITES.....	19
PSEXEC COMMANDS FOR AGENT PUSH	19

Installing the agent in silent mode on Windows or Linux

The objective of this guide is to provide you with instructions and critical considerations for deploying an agent silently on multiple servers.

Overview

Our goal is to simplify the agent installation on multiple servers with minimal user intervention.

DigiCert CertCentral automation agent installation is a two-step process:

1. Unpack and deploy the software on the server.
2. Authenticate the agent to a CertCentral account to provision for automation.

Key-based authentication

You can use key-based authentication as an alternative to username and password authentication. Instead of requiring username and password, users can confirm their identity using authentication keys.

An authentication key, also called an API key, is a combination of encrypted alphanumeric characters that have user details and permissions associated with the account.

An API key is only required to validate the request to provision the agent. It can be revoked once the agent is provisioned and running.

Note: The API key is only shown once to protect the user's identity and prevent misuse.

Why use a companion application?

A companion application reduces the number of steps involved in provisioning the agent and starting the agent's service. The companion application securely provisions the agent without exposing the account's authentication key.

Prerequisites

You must have the latest version of Go installed. To download and install Go, refer to <https://golang.org/doc/install>.

Note: Windows (Win10 and above) or Linux (CentOS 7 and above) with 64-bit version must have **go1.15.2 or above** installed.

The process requires you to build the companion application to provision the agent from the codes provided.

Note: To use the scripts listed in this document, save this document to your computer to retain the script format and alignment.

Build the companion application on Windows or Linux

To build the companion application, you need a CertCentral account with Automation enabled.

1. Download the companion application build codes package (**Digicert-ADM-Agent-Deployment-Companion.zip**) from CertCentral and unzip it. Be sure to note its location.
2. Create an API key for the agent's deployment. Go to **Automation > API keys**, select **Add API Key**, fill in the fields, and then select **Add API Key** button. Copy the key to a secure location. You will populate DEVKEY with this value.
3. Open the command prompt or terminal and navigate to the **Digicert-ADM-Agent-Deployment-Companion** folder.
4. Run the companion build commands and provide the API key.

On Windows:

```
> (set GOARCH=amd64) && (set GOOS=windows) && go build -o digicert-agent-deployment-companion.exe -trimpath -ldflags="-s -w -X 'main.devkey={DEVKEY}'"
```

Replace DEVKEY with your API key.

For example:

```
> (set GOARCH=amd64) && (set GOOS=windows) && go build -o digicert-agent-deployment-companion.exe -trimpath -ldflags="-s -w -X 'main.devkey=IWMDAWMDAWWHCNMJEWMT5MJM10TU5WJBXMQSWCQYDVQGEWJVUZEXMBUGA1UECHMOVMVYAVNPZ24SIEL'"
```

On Linux:

```
> (set GOARCH=amd64) && (set GOOS=linux) && go build -o digicert-agent-deployment-companion -trimpath -ldflags="-s -w -X 'main.devkey={DEVKEY}'"
```

Replace DEVKEY with your API key.

For example:

```
> (set GOARCH=amd64) && (set GOOS=linux) && go build -o digicert-agent-deployment-companion -trimpath -ldflags="-s -w -X 'main.devkey=IWMDAWMDAWWHCNMJEWMTE5MJM10TU5WJBXMQSWCQYDVQQGEJVUZEXMBUGA1UECHMOVMVYAVNPZ24SIEL '"
```

You can find the associated output companion build files as:

- **Windows:** digicert-agent-deployment-companion.exe
- **Linux:** digicert-agent-deployment-companion

Note: You are not required to install the agent and generate a companion application build from the same computer where you plan to install the agent.

Build and deploy a Global Policy Object (GPO) MSI bundle on Windows

Use one of the popular mechanisms to distribute the agent and companion application as described. Deployment is performed with the GPO push through the active directory configuration. For more information, see [Appendix A: Group Object Policy \(GPO\)](#) or [Appendix C: PsExec based agent push for Windows](#).

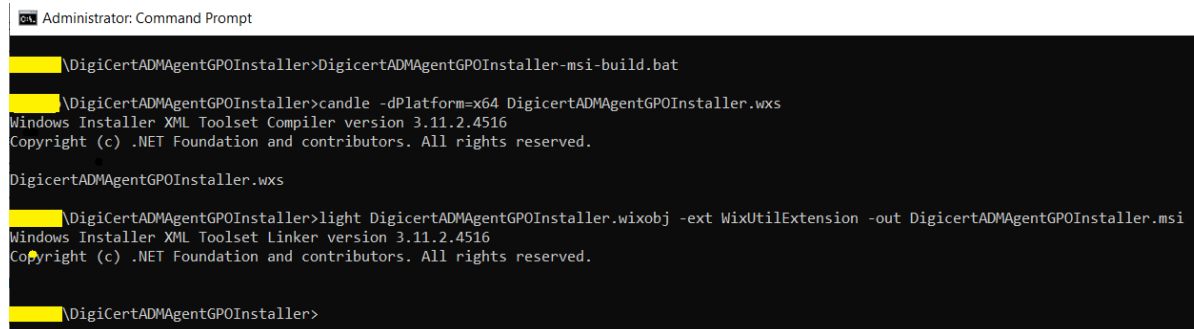
Note: You can also deploy the DigiCert agent through any third-party software deployment system.

To generate the MSI bundle for GPO deployment:

1. Download and install the WiX Toolset (v3.11.2 or above). Refer to <https://wixtoolset.org/> or use the download URL: <https://github.com/wixtoolset/wix3/releases/download/wix3112rtm/wix311.exe>
2. Set the WiX installation path `\bin` to the system path.
3. Download the agent deployment codes package (**DigiCertADMAgentGPOInstaller.zip**) from CertCentral and unzip it. Be sure to note its location.
4. Move the **digicert-agent-deployment-companion.exe** file into the **DigiCertADMAgentGPOInstaller** folder.
5. Download the latest agent installer package (**adm_agent_x.x.x_win64.zip**) from CertCentral.
6. Extract the **DigiCert ADM Agent.exe** file.

7. Move the **DigiCert ADM Agent.exe** file into the **DigiCertADMAGentGPOInstaller** folder.
8. Run the **DigiCertADMAGentGPOInstaller-msi-build.bat** file from the DOS prompt to generate the **.MSI** bundle for GPO.

On successful build, the DOS output looks like:



```
Administrator: Command Prompt

\DigiCertADMAGentGPOInstaller>DigiCertADMAGentGPOInstaller-msi-build.bat

\DigiCertADMAGentGPOInstaller>candle -dPlatform=x64 DigiCertADMAGentGPOInstaller.wxs
Windows Installer XML Toolset Compiler version 3.11.2.4516
Copyright (c) .NET Foundation and contributors. All rights reserved.

DigiCertADMAGentGPOInstaller.wxs

\DigiCertADMAGentGPOInstaller>light DigiCertADMAGentGPOInstaller.wixobj -ext WixUtilExtension -out DigiCertADMAGentGPOInstaller.msi
Windows Installer XML Toolset Linker version 3.11.2.4516
Copyright (c) .NET Foundation and contributors. All rights reserved.

\DigiCertADMAGentGPOInstaller>
```

Note: **DigiCertADMAGentGPOInstaller.msi** installer file will be available in **DigiCertADMAGentGPOInstaller** folder.

To prepare the launch script to install the MSI bundle, use the **DigiCertAgentGPOInstaller.bat** file provided in the **DigiCertADMAGentGPOInstaller.zip** archive. Configure the variable parameters at the top of this script by replacing the **{SHARED_PATH}**, **{DIVISION_ID}**, and **{PROXY}** placeholders with actual values, as described below.

Configuration parameters:

- **shared-path** (required): The shared network path where you will place the **DigiCertADMAGentGPOInstaller.msi** file.
- **division_id** (required): The division ID number for the CertCentral account the agents belong to.
- **proxy**(optional): Proxy settings for the agents. Leave empty if your agents don't use a proxy to connect to CertCentral.

Valid proxy formats:

<http://proxyIP:proxyPort>

<http://username:password@proxyIP:proxyPort>

Examples of setting these variables in the **DigiCertAgentGPOInstaller.bat** file:

```
1 @echo off
2
3 set shared_path="\\silent-gpo.com\NETLOGON"
4 set division_id=123456
5 set proxy=""
6
```

```
1 @echo off
2
3 set shared_path="\\silent-gpo.com\NETLOGON"
4 set division_id=123456
5 set proxy="http://192.168.56.1:3232"
6
```

Note: The provided **DigiCertAgentGPOInstaller.bat** script assumes the Windows operating system on node systems is running from the **C:** drive. If not, update the script to replace any references to the **C:** drive with the applicable drive letter where Windows is running.

Windows: Install agent

Once the GPO bundle is set up to push **DigiCertADMAgentGPOInstaller.msi**, install and provision the **DigiCert ADM Agent.exe** to the client machines. For instructions, refer to [Appendix A: Group Object Policy \(GPO\)](#) or [Appendix C: PsExec based agent push for Windows](#).

The installed agent will be listed in **CertCentral > Automation > Manage automation**. The agent name matches the GPO client machine hostname where the agent is installed.

Linux: Install agent

Important: You must have **root** or **sudo** privileges.

For GPO like deployment of agent, you need to prepare a distribution package (**DigiCertADMAgentGPOInstaller.tar.gz**) and then run the agent installation command. The package includes:

1. **adm_agent_X.X.XX_linux64.tar.gz**
2. **digicert-agent-deployment-companion**
3. **silentInstaller-by-companion-lnx.sh**

You can also automate the agent deployment using Ansible. For more information, see [Appendix B: Automate agent deployment using Ansible](#).

1. Prepare the package

- a) Download the agent installer package (**adm_agent_X.X.XX_linux64.tar.gz**) from CertCentral.
- b) Get the Linux companion build file **digicert-agent-deployment-companion**.
- c) Download the agent deployment codes file (**silentInstaller-by-companion-lnx.sh**) from CertCentral.
- d) Create a package (**DigiCertADMAgentGPOInstaller.tar.gz**) containing these files.

2. Install the agent

- a) Copy the package (**DigiCertADMAgentGPOInstaller.tar.gz**) to the targeted machine.
- b) Extract the contents of the package.
- c) Run the agent installation command and provide the provisioning information.

```
./silentInstaller-by-companion-lnx.sh
AGENT_BUNDLE_NAME="{agentBundleName}" DIVISION="{divisionId}"
ALIASNAME="{agent alias name}"
```

For example:


```
./silentInstaller-by-companion-lnx.sh  
AGENT_BUNDLE_NAME="adm_agent_2.0.0_linux64.tar.gz" DIVISION="716494"  
ALIASNAME="AbcLnxMassInstall151" PROXY="http://125.125.125.125:3333"
```

Configuration parameters:

- **AGENT_BUNDLE_NAME** (required): Filename of the agent installer package.
- **DIVISION** (required): The division ID number for the CertCentral account the agents belong to.
- **ALIASNAME** (optional): User-friendly name for the agents. Omit this to name the agents with the license key by default.
- **PROXY** (optional): Proxy settings for the agents. Omit this if your agents don't use a proxy to connect to CertCentral.

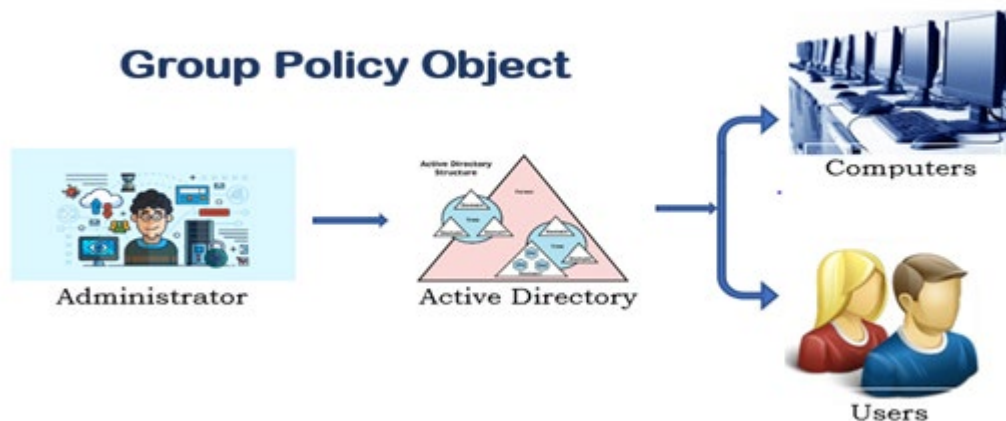
Valid proxy formats:

<http://proxyIP:proxyPort>

<http://username:password@proxyIP:proxyPort>

Appendix A: Group Policy Object (GPO)

Microsoft's Group Policy Object (GPO) is a collection of Group Policy settings that defines what a system will look like and how it will behave for a defined group of users.



Microsoft provides a program snap-in that allows you to use the Group Policy Management Console (GPMC). The selections result in a Group Policy Object. The GPO is associated with selected Active Directory containers, such as sites, domains, or organizational units (OU). The GPMC allows you to create a GPO that defines registry-based policies, security options, software installation and maintenance options, script options, and folder redirection options.

Group Policy allows an administrator to **assign and publish** software to client computers. The computers then install the software when the AD user signs in and receives the assignment. The computers must be members of an Active Directory domain to do this.

Deploy agents through Group Object Policy

To use Group Policy to automatically distribute programs to client computers (AD users):

1. Create a distribution point
2. Create a Group Object Policy
3. Logon scripts for Group Object Policy

Note: Group Policy is applied when the user signs in.

For the Group Policy Deployment of the Windows Agent to function properly, the user must have Active Directory installed on the supported operating system.

For example:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

1. Create a distribution point

To publish or assign a computer program, you must create a distribution point on the publishing server:

- a) Sign in to the server as an administrator.
- b) Create a shared network folder where you will put the Windows Installer package (**.msi file**) that you want to distribute.
- c) Set permissions on the share to allow access to the distribution package.
- d) Copy the package to the distribution point.

2. Create a Group Object Policy

To create a Group Policy Object (GPO) to use to distribute the software package:

- a) Start the Group Policy Management snap-in. Select **Start**, navigate to **Administrative Tools**, and select **Group Policy Management**.
- b) In the console tree, right-click your domain, and then select **Create a GPO in this domain, and Link it here...**
- c) Enter a name for this new policy, and then select **OK**.

3. Logon scripts for Group Object Policy

Once you have GPO bundle created, you can push the policy with the user configuration. User configuration scripts will run when the domain user signs in to the node machine.

Use batch file **DigiCertAgentGPOInstaller.bat** as the Logon script to install the agent.

Logon script

To use the scripts as Logon at **User Configurations** to apply policy to the domain user login into the node:

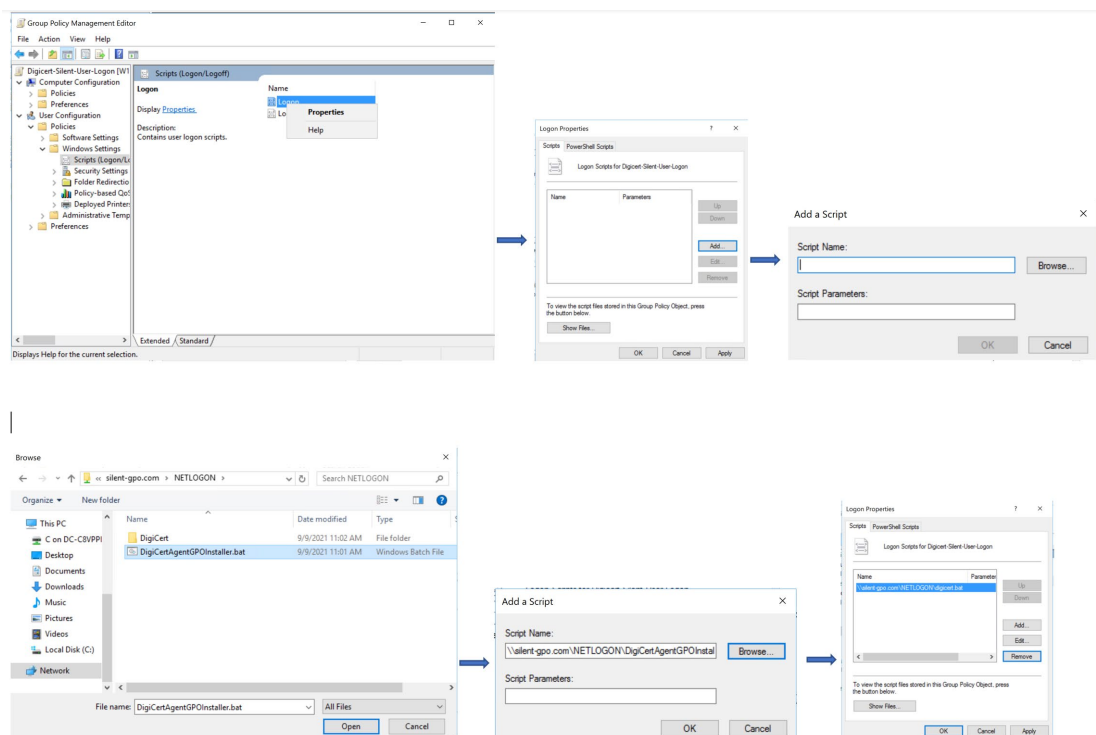
1. Start the Group Policy Management snap-in. Select **Start**, navigate to **Administrative Tools**, and then select **Group Policy Management**.

INSTALL AGENT IN SILENT MODE

2. In the console tree, under your domain, right-click on the GPO created, and then select **Edit**.
3. Expand **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)**.
4. Right-click **Logon** and select **Properties**.
5. In the Logon Properties window, in the Scripts tab, select **Add**.
6. In the Add a Script window, select **Browse** to add **DigiCertAgentGPOInstaller.bat** from the shared path (Universal Naming Convention path).

Note: Do not use the **Browse** button to access the location. Use the UNC path of the shared installer package.

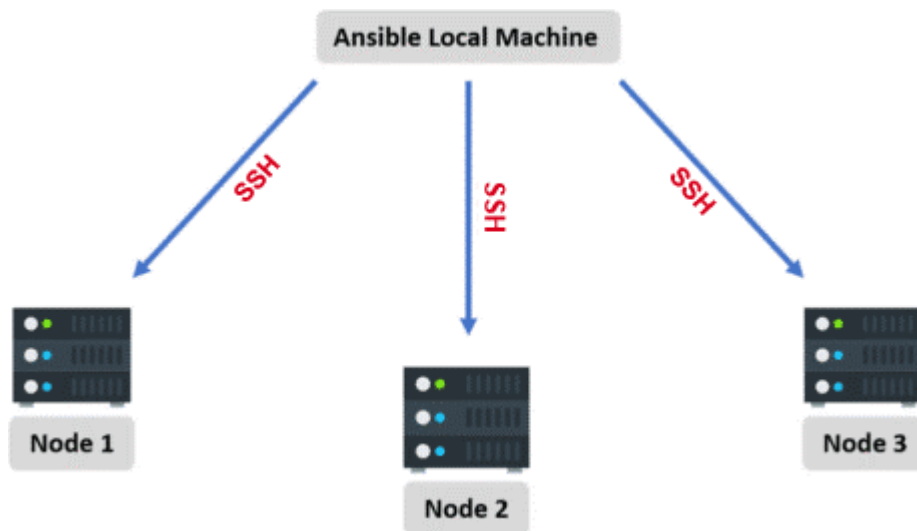
7. Select **Open** and then select **OK**.
8. Select **Apply** and then select **OK** to close the Logon Properties window.
9. Close the **Group Policy Management Editor** and then **Group Policy Management** snap-in.
10. When the client computer starts, the startup script will run and install the application.



Appendix B: Automate agent deployment using Ansible

Ansible is a powerful automation tool used for provisioning, configuring, and deploying applications on remote computers.

Overview



1. The ansible local machine is the local server, where the Ansible and its scripts (playbooks) are configured.
2. The local server must have SSH access to each node (client's computer), where you want to deploy the agent.
3. Move the agent installer (**tar.gz** file) downloaded from the CertCentral in the local server to each node.
4. Create a variable file (**var.yml**) with all the required parameters and pass them to the Ansible playbooks. Sensitive variables, like passwords and tokens, are passed through Ansible vaults. These vaults are password protected.
5. Once the **tar.gz** file is copied on each node, extract the contents and execute the script with the required parameters as passed in the variable file.

Prerequisites

1. Must have Ansible installed on the client's computer.
2. Must have passwordless SSH access to the client's computer.
3. Must have port 22 open to establish secure communication between local server and client's computer.

Deploy agent through Ansible

1. Install the Ansible

Run the `yum install ansible -y` command to install the Ansible into your local server.

2. Verify the version

Run the `ansible --version` command to verify the Ansible version.

```
[root@ansible-ws-ap ~]# ansible --version
ansible 2.9.15

  config file = /etc/ansible/ansible.cfg
  configured module search path =
[u'/root/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']

  ansible python module location = /usr/lib/python2.7/site-
packages/ansible

  executable location = /usr/bin/ansible

  python version = 2.7.5 (default, Nov 16 2020, 22:23:17) [GCC
4.8.5 20150623 (Red Hat 4.8.5-44)]
```

3. Update the configuration files

There are two important configuration files:

- **ansible.cfg**, as its name implies, contains all the configurations related to the Ansible. Located in `/etc/ansible/ansible.cfg`.
- **hosts** file contains a list of all the host files with information about the nodes that were configured. Located in `/etc/hosts`.

To update the configuration files:

- a) Create an installation directory.

For example:

```
mkdir /app/sensor
```

- b) Move the **ansible.cfg** and **hosts** file into the installation directory.

```
mkdir /app/sensor

# Copy the ansible.cfg file and the hosts file into this folder
cp /etc/ansible/ansible.cfg /app/sensor
cp /etc/ansible/hosts /app/sensor
```

- c) Copy the details of the nodes in the **hosts** file to connect the nodes through hostname.

```
IP1 ansible-n1-ap.sbolab.blu.digicert.com ansible-n1-ap
IP2 ansible-n2-ap.sbolab.blu.digicert.com ansible-n2-ap
```

- d) Enter the username and password of SSH or SSH ID to the nodes.

```
ssh-copy-id ansible-n1-ap
ssh-copy-id ansible-n2-ap
```

Ansible configures these nodes through SSH.

- e) Add the nodes into the hosts file to establish a connection.

```
[nodes]
ansible-n1-ap.sbolab.blu.digicert.com
ansible-n2-ap.sbolab.blu.digicert.com
```

- f) Edit the **ansible.cfg** file with the updated **hosts** file.

```
# config file for ansible -- https://ansible.com/
# =====

# nearly all parameters can be overridden in ansible-playbook
# or with command line flags.  ansible will read ANSIBLE_CONFIG,
# ansible.cfg in the current working directory, .ansible.cfg in
# the home directory or /etc/ansible/ansible.cfg, whichever it
# finds first

[defaults]

# some basic default values...

inventory      = ./hosts # line10
<...truncated>
host_key_checking = False # line 61
<... truncated>
```

- g) Run the **ad-hoc** command to verify nodes connections.

```
[root@ansible-ws-ap sensor]# ansible nodes -m ping
ansible-n2-ap.sbolab.blu.digicert.com | SUCCESS => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python"
  },
  "changed": false,
  "ping": "pong"
}
ansible-n1-ap.sbolab.blu.digicert.com | SUCCESS => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python"
  },
  "changed": false,
  "ping": "pong"
}
```

Note: **nodes** is the name of the node group that you plan to install the agent into.

4. Install the agent

Before you start:

- The IPs of the nodes have a connection established.
- Tarball of the agent must be in **gzip** format.

Note: A tarball or tarfile is the name of a group or archive of files bundled together using the tar command.

To complete the setup and install the agent:

- a) Update the variables file **var.yml** with the parameters:
 - IP address of the nodes. Nodes should have the same IP address as the nodes in the hosts file.
 - Options, containing divisionID, proxy, bundle_name, and alias_name.
- b) Run the `ansible-playbook main.yml` command to install the agent.

The main.yml file looks like:

```
- hosts: localhost
  gather_facts: no
  vars_files: var.yml
  tasks:
    - name: "Creating a directory if it doesn't exists"
      raw: "ssh {{ item }} mkdir -p /opt/digicert"
      loop: "{{ nodes }}"
    - name: "Uninstalling the tar on remote machines"
      raw: "scp -r DigiCertADMAgentGPOInstaller.tar.gz {{ item
    }}:/opt/digicert"
      loop: "{{ nodes }}"
    - name: "Extracting the tar on the remote machine"
      raw: "ssh {{ item }} tar -xvzf
/opt/digicert/DigiCertADMAgentGPOInstaller.tar.gz -C
/opt/digicert"
      loop: "{{ nodes }}"
    - name: "Making the script executable"
      raw: "ssh {{ item }} chmod +x
/opt/digicert/silentInstaller-by-companion-lnx.sh "
      loop: "{{ nodes }}"
    - name: "Executing the script on the remote machine"
      raw: "ssh {{ item }} /opt/digicert/silentInstaller-by-
companion-lnx.sh AGENT_BUNDLE_NAME={{ options['bundle_name'] }}
DIVISION={{ options['divisionID'] }} ALIASNAME={{
options['alias_name'] }} PROXY= {{ options['proxy'] }}"
      loop: "{{ nodes }}"
      register: out
    - debug:
      var: out
```

Appendix C: PsExec based agent push for Windows

PsExec is a light-weight telnet replacement that lets you execute processes on other systems without manually installing the client software.

Prerequisites

- All machines you plan to install **DigiCert ADM Agent.exe** to must be members of an active directory domain.
- An active directory user with domain admin privilege.
- Set up a distribution point (shared path) that is accessible from all targeted node machines.
- For PsExec based approach, download the PSTools bundle (PSTools.zip) from the Microsoft site. Refer to <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>.

Extract **PSTools.zip** and copy **PsExec64.exe** onto your executable path for the command-based mass installation of an agent in windows machines.

- Execute PsExec command from AD server machine which has reachability to all node machines by resolving node machine name.
- Place **DigiCertADMAgentGPOInstaller.msi** and **DigiCertAgentGPOInstaller.bat** in the distribution point (shared path), accessible from the node machines where you expect the agent to get installed. For example:

Name	Date modified	Type	Size
DigiCertADMAgentGPOInstaller	03-09-2021 00:03	Windows Installer ...	4,384 KB
DigiCertAgentGPOInstaller	10-09-2021 06:58	Windows Batch File	4 KB

where the shared path to the file is **\\VBOXSVR\VMShare\GPO**.

PsExec commands for agent push

For single agent deployment:

```
PsExec64.exe -h -d -i \\{targetMachineName} -u {ADdomain}\Administrator -p {password} "{SHARED_PATH}\DigiCertAgentGPOInstaller.bat" -accepteula -nobanner
```

For example:


```
C:\Softwares\PSTools>PsExec64.exe -h -d -i \\WS2012node1 -u gpo-domain\Administrator -p AdDomain09
"\\VBOXSVR\VMShare\GPO\DigiCertAgentGPOInstaller.bat" -accepteula -nobanner
```

- **\\{targetMachineName}**– Name of AD machine (node machine).

- {ADdomain}\Administrator and {password} – Active directory administrator credentials.
- {SHARED_PATH} – Location where **DigiCertAgentGPOInstaller.bat** and **DigiCertADMAgentGPOInstaller.msi** are placed.

For bulk agent deployment:

Replace the `\\{targetMachineName}` with a text file containing a list of AD computer names as shown below.

 **computers.txt - Notepad**

File Edit Format View Help

```
WS2012node1  
WS2012node2
```

```
PsExec64.exe -h -d -i @computers.txt -u {ADdomain}\Administrator -p {password}  
"{SHARED_PATH}\DigiCertAgentGPOInstaller.bat" -accepteula -nobanner
```

For example:

```
C:\Softwares\PSTools>PsExec64.exe -h -d -i @donainlist.txt -u gpo-  
domain\Administrator -p AdDomain09  
"\\VBOXSVR\VMShare\GPO\DigiCertAgentGPOInstaller.bat" -accepteula -nobanner
```

- computer.txt – File which contains a list of AD domain computer names where **DigiCert ADM Agent.exe** needs to be installed.
- {ADdomain}\Administrator and {password} – Active directory administrator credentials.
- {SHARED_PATH} – Location where **DigiCertAgentGPOInstaller.bat** and **DigiCertADMAgentGPOInstaller.msi** are placed.

After successful execution, agents will be listed in **CertCentral > Automation > Manage automation**.

Note: The script execution log is available at **C:\DigiCertAgentLogs\AgentScriptExecutor.log** of node machines for further verification.
