IT Doc

Customer name

Written by : Yoann Gini
Last update on : 6 février 2017

ACME Consulting

Introduction

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur non libero cursus, pulvinar ipsum at, porta odio. Sed malesuada orci a nibh faucibus, id venenatis sem iaculis. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nunc eu justo nisl. Curabitur in est ipsum. Aliquam tempus, eros eleifend eleifend condimentum, nunc odio mattis tellus, eu tincidunt enim magna eget magna. In id turpis sem. Phasellus sollicitudin non enim sit amet pellentesque. Mauris consequat turpis vel mattis rhoncus. In vehicula arcu arcu, porttitor malesuada ex auctor a. Curabitur eget pellentesque quam. Quisque sodales metus fermentum, varius magna vitae, tincidunt nulla.

Sed ex urna, suscipit et ligula ut, volutpat ultrices ligula. Nullam sed neque leo. Maecenas quis velit arcu. Nunc ante lacus, ullamcorper non neque et, vehicula volutpat leo. In ultrices luctus velit, a imperdiet nibh egestas nec. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nam molestie ornare fringilla. Fusce sollicitudin, mauris nec suscipit hendrerit, est lectus mollis arcu, vitae imperdiet urna odio sit amet metus. Proin tempus nulla massa, et feugiat libero malesuada maximus. Suspendisse tempor turpis vel suscipit sollicitudin. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nulla facilisi. Vivamus elementum, libero vel pulvinar venenatis, sem ipsum blandit metus, vel eleifend nunc turpis eget risus. Etiam vehicula, orci id hendrerit hendrerit, ante nisl interdum mauris, vitae elementum lorem dui non tortor.

Skills

Curabitur iaculis arcu et eros egestas, viverra pharetra leo convallis. Fusce dui ligula, feugiat at arcu aliquet, tincidunt finibus risus. Duis vulputate fringilla rutrum. Nullam rhoncus purus nisl, et venenatis felis interdum eget. Phasellus et blandit mi. Nam dapibus nisl non nunc porttitor tempus. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aliquam ut nulla non ex feugiat ullamcorper at a sapien. Nulla tempor felis sed ornare faucibus. Phasellus scelerisque metus eu consequat cursus. Pellentesque rutrum turpis tellus. Nunc lacinia mauris et dignissim porttitor. Quisque at velit a tellus lacinia interdum quis id arcu. Proin sed augue metus. Maecenas lacus turpis, imperdiet quis consectetur vitae, tempus nec odio. Maecenas hendrerit justo ut sapien ultricies congue.

Table des matières

System Architecture

1.1 Network

1.1.1 Gateway

Main gateway used for Internet access and VPN management.

System info

Type	Cisco ASA 5516-X
OS	ASA OS 9.7.1 / ASDM 7.7.1
Location	Server Closet A42

Network info

System has the following IP addresses :

IP Address	Usage	FQDN
`192.168.0.1`	LAN	`gtw.corp.example.com`
`203.0.113.42`	WAN	`vpn.example.com`

Accounts

Available accounts are :

Username	Password	Usage
admin	**REDACTED**	Administrative access

Services

Provided services are :

- Firewall
- NAT
- IKEv2 VPN Server

Backups

Backups are manual and should be stored on the IT file sharing, backup subfolder.

1.1.2 Distribution

Switch cluster in charge of distribution role.

System info

Type	Cisco SG500X 48
OS	1.4.7.06
Location	Server Closet A42

Network info

System has the following IP addresses :

IP Address	Usage	FQDN
`192.168.0.2`	LAN	`distri.corp.example.com`
`192.168.*.1`	Subnet routing interface	

Accounts

Available accounts are :

Username	Password	Usage
cisco	**REDACTED**	Administrative access

Services

Provided services are :

- Inter VLAN routing
- Inter VLAN filtering
- DHCP relay

Backups

Backups are manual and should be stored on the IT file sharing, backup subfolder.

1.1.3 Access

All access switches share the same configuration. The documentation for each of them is unified in one section. Location of each access switch is available in the Network info section.

System info

Type	Cisco SG300
OS	1.4.7.06

Network info

System has the following IP addresses :

IP Address	Location	FQDN
`192.168.42.2`	Server Closet A42	`asw-1.corp.example.com`
`192.168.42.3`	Main Conference Room	`asw-2.corp.example.com`
`192.168.42.4`	Warehouse	`asw-3.corp.example.com`

Accounts

Available accounts are :

Username	Password	Usage
cisco	**REDACTED**	Administrative access

Services

Provided services are :

- Endpoint network access with 802.1x
- VLAN tagging
- PoE for IP Phone and Wireless access points

Backups

Backups are manual and should be stored on the IT file sharing, backup subfolder.

1.1.4 WiFi

All WiFi access point share the same management configuration. The documentation for each of them is unified in one section. Location of each access point is available in the Network info section.

System info

Type	Cisco Aironet 1850i
OS	15.3.3-JD

Network info

System has the following IP addresses :

IP Address	Location	FQDN
`192.168.43.2`	Open Space	`ap-1.corp.example.com`
`192.168.43.3`	Main Conference Room	`ap-2.corp.example.com`
`192.168.43.4`	Warehouse	`ap-3.corp.example.com`

Accounts

Available accounts are :

Username	Password	Usage
cisco	**REDACTED**	Administrative access

Services

Provided services are :

- Endpoint wireless network access with 802.1x
- Guest access on guest VLAN

Backups

Backups are manual and should be stored on the IT file sharing, backup subfolder.

1.2 Virtualization Farm

1.2.1 Central Management

Central management for virtual environment is provided by VMware VCenter and accessible via the VMware vSphere Web Client.

System info

Type	VMware vCenter
OS	6.5
Location	Virtual Cluster A

Network info

System has the following IP addresses :

IP Address	Usage	FQDN
`192.168.41.2`	LAN	`vsphere.corp.example.com`

Accounts

Available accounts are :

Username	Password	Usage
administrator@vsphere.example.com	**REDACTED**	Administrative access

Services

Provided services are :

- ESXi management
- vSphere Orchestrator

Backups

Backups are manual and should be stored on the IT file sharing, backup subfolder.

1.2.2 Hypervisors

All hypervisors share the same configuration. The documentation for each of them is unified in one section. Location of each access switch is available in the Network info section.

System info

Type	MacPro
OS	ESXi 6.5

Network info

System has the following IP addresses :

IP Address	Name & location	FQDN
10.0.40.2	ESXi-1, Server Closet A42	esxi-1.corp.example.com
10.0.40.3	ESXi-1, Server Closet A42	esxi-2.corp.example.com
10.0.40.4	ESXi-1, Server Closet B12	esxi-3.corp.example.com
10.0.40.5	ESXi-1, Server Closet B12	esxi-4.corp.example.com

Accounts

Available accounts are :

Username	Password	Usage
root	**REDACTED**	ESXi system management

Services

Provided services are :

- virtualization ;
- hypervisor management.

Backups

Backups are manual and should be stored on the IT file sharing, backup subfolder.

1.2.3 Storage

Virtual storage is hosted by a Promise VTrak SAN system.

System info

Type	Promise VTrak
OS	unknown
Location	Server Closet A42

Network info

System has the following IP addresses :

IP Address	Usage	FQDN
192.168.42.5	System management	san1.corp.example.com

Accounts

Available accounts are :

Username	Password	Usage
Administrator	**REDACTED**	System management

Services

Provided services are :

- Fibre Channel storage ;
- Storage management.

Backups

RAID configuration is stored on the IT file sharing, backup subfolder. Data themselves are backuped by the virtual layer.

1.2.4 Storage Network

All Fibre Channel switches share the same setup. The documentation for each of them is unified in one section. Location of each switch is available in the Network info section.

System info

Type	QLogic 5802V
OS	unknown

Network info

System has the following IP addresses :

IP Address	Location	FQDN
`192.168.42.6`	Server Closet A42	`fcsw-1.corp.example.com`

Accounts

Available accounts are :

Username	Password	Usage
admin	**REDACTED**	Management

Services

Provided services are :

— Fibre Channel Fabric.

Backups

Backups are manual and should be stored on the IT file sharing, backup subfolder.

1.3 Servers

1.3.1 Domain Controllers

All domains controller use the same setup and provide the same services

System info

Type	VM
OS	Windows 2012 R2
Location	Virtualization farm

Network info

System has the following IP addresses :

IP Address	Usage	FQDN
`192.168.0.2`	DC1	`dc1.corp.example.com`
`192.168.0.3`	DC2	`dc2.corp.example.com`

Accounts

Available accounts are :

Username	Password	Usage
administrator@corp.example.com	**REDACTED**	AD main admin account
-	**REDACTED**	DSRM password

Services

Provided services are :

- Domain Controller ;
- DNS Server ;
- DHCP Server.

Backups

Backups are handled at the virutal level.

1.3.2 MDM

MDM service is handled by Profile Manager on macOS Server.

System info

Type	VM
OS	macOS 10.12.3 / Server 5.2
Location	Virtualization farm

Network info

System has the following IP addresses :

IP Address	Usage	FQDN
`192.168.0.12`	LAN	`mdm.corp.example.com`

Apple ID

This server require an Apple ID to handle macOS Server licence. Here are all the info used during the Apple ID creation.

E-mail	appleid.mdmserver@example.com
Password	**REDACTED**
Firstname	macOS
Lastname	Server
Birth date	**REDACTED**
2FA phone number	0123456789
Security question 1	Best friends
Answer 1	**REDACTED**
Security question 2	Favorit job
Answer 2	**REDACTED**
Security question 3	First boss
Answer 3	**REDACTED**

Accounts

Available accounts are :

Username	Password	Usage
ladmin	**REDACTED**	System management

Services

Provided services are :

- Caching service ;
- MDM.

Backups

Backups are handled at the virtual level.

Basics Process

2.1 User management

2.1.1 Account creation

Creating an account require admin rights and a formal ticket filled by N+1 or HR departments on the support portal.

This ticket will provide you the followed info :

- Firstname
- Lastname
- Requested e-mail address
- Functional groups
- Specific authorization for VPN accessible resources

Regarding e-mail, the demander will be in charge to follow the company template but still have the right to do small change if the final e-mail created create an unwanted result.

To create the account, you will have to connect via RDP to the IT management environment on the IT server with your `adm-` account and use the `Users and computers` Active Directory management tool.

Accounts must be created in the organization unit `Employees`, `Consultants`, `Externals` located in `corp.example.com/Members`.

Specials `adm-` accounts are located in the `Privileged` organization unit.

2.1.2 Account deactivation

During the off-boarding process, HR or N+1 will issue a formal deactivation ticket on the support portal. The ticket will tell you which account need to be disabled when. Account deactivation requested are sent before the last day of work to let you organize your work.

Deactivation steps are :

- Reset the password to a random and undocumented one
- Rename the display name with to add `Z -` in front
- Move the account in `corp.example.com/Disabled`
- Remove the user from all groups
- Disable the account

2.1.3 Service account

Creating a service account require admin rights. Account name will be service-*servicename* and must be located in `corp.example.com/Managed Services Accounts`.

Password must be unable to change and never expire.

Password must be generated with the command line `openssl rand -base64 42`.

Service password must be documented in the IT password documentation system.

2.2 System Deployment

2.2.1 Workstation

macOS

All macOS workstations are registered in the DEP process.

You just have to boot the computer with network available to automatically set everything.

After the first boot, computer will be enrolled to MDM, bound to AD, and updated by Munki.

The computer is ready to be used when it displays the login window with login/password fields instead of list of users and the name of the company just behind.

Windows

Windows workstations aren't allowed for now.

Linux

Linux workstations aren't allowed for now.

2.2.2 Servers

macOS

All macOS servers are deployed as VM on the virtualized environment. You need to create a new macOS VM with NetBoot enabled for the next boot only.

The NetBoot will lead you to the `Imagr` deployment shell. You will just have to select the requested server version.

In the end, your new server will be set with default password **REDACTED** for the `ladmin` account and linked to the server-gen Munki's manifest.

Active Directory bind isn't made by default. You will have to do it with your `adm-` account if needed.

Windows

Windows servers are created from virtual template. After deployment the Administrator account has password **REDACTED** and nothing else is done.

Active Directory bind isn't made by default. You will have to do it with your `adm-` account if needed.

Linux

Linux servers are created from virtual template. After deployment the root account has password **REDACTED** and nothing else is done.

Active Directory bind isn't made by default. You will have to it with sssd and your `adm-` account if needed.

2.2.3 Service Devices (Printers, etc.)

All new network services must use AD authentication with SAML or LDAP bind. Please refer to the service documentation.