DOCUMENTATION TECHNIQUE

Infrastructure réseau et systèmes

Entreprise JDC

BTS SIO – Option SISR
Session 2026

Solutions d'infrastructure, systèmes et réseaux
Administration des systèmes et des réseaux

Date : Avril 2026

Table des matières

1. Présentation du projet et contexte entreprise

1.1 Contexte de l'entreprise JDC

JDC est une entreprise spécialisée dans les solutions d'encaissement et d'équipements de point de vente (caisses enregistreuses, terminaux de paiement électronique (TPE), balances, logiciels de caisse, etc.). L'entreprise accompagne ses clients professionnels dans l'installation, la configuration et la maintenance de l'ensemble de leurs équipements d'encaissement.

Dans le cadre de la modernisation de son infrastructure informatique, JDC souhaite mettre en place un environnement réseau sécurisé, segmenté et supervisé, permettant de garantir la disponibilité et la sécurité de ses services internes ainsi que de ses solutions déployées chez les clients.

1.2 Objectifs du projet

- Mettre en place une infrastructure réseau segmentée en VLANs pour isoler les flux de données
- Déployer un domaine Active Directory (JDC.local) avec redondance (DC principal + réplica)
- Configurer un pare-feu pfSense avec règles de filtrage inter-VLAN et accès VPN distant
- Installer un système de supervision Zabbix pour surveiller l'état de l'infrastructure
- Déployer GLPI pour la gestion du parc informatique et la gestion des incidents
- Installer un hyperviseur Proxmox VE pour la gestion de la virtualisation
- Appliquer des stratégies de groupe (GPO) adaptées au contexte métier (sécurité POS)
- Configurer un accès VPN sécurisé (OpenVPN) pour les interventions à distance

1.3 Environnement technologique

Composant	Technologie	Version
Hyperviseur physique	VMware Workstation Pro	17.x
Pare-feu / Routeur	pfSense	2.7.2
Serveur principal	Windows Server	2022
Serveur réplica	Windows Server	2022
Supervision	Zabbix sur Debian 12	7.0 LTS
Gestion de parc	GLPI sur Debian 12	10.x
Virtualisation	Proxmox VE sur Debian 12	8.x

Clients	Windows 10/11 Pro	22H2+
VPN	OpenVPN (pfSense)	2.6.x

2. Architecture réseau

2.1 Schéma réseau global

L'infrastructure réseau de JDC repose sur une architecture virtualisée sous VMware Workstation Pro. Le routage et la sécurité sont assurés par pfSense, qui gère trois VLANs distincts permettant de segmenter les flux selon les usages.

[Le schéma réseau est fourni en annexe sous forme d'image séparée]

2.2 Plan d'adressage IP

L'adressage IP est organisé en trois sous-réseaux correspondant aux trois VLANs. Le réseau WAN connecte pfSense au réseau physique via le NAT VMware.

Réseau	VLAN ID	Sous-réseau	Passerelle	Plage DHCP	Usage
WAN	-	192.168.23.0/24	VMware NAT	-	Accès Internet
Serveurs	VLAN 10	172.16.10.0/24	172.16.10.254	-	Serveurs (IP fixes)
Clients	VLAN 20	172.16.20.0/24	172.16.20.254	.10 à .50	Postes utilisateurs
Admin	VLAN 30	172.16.30.0/24	172.16.30.254	-	Administration

Adressage des machines

Machine	Hostname	VLAN	Adresse IP	Rôle
pfSense	pfsense.jdc.local	Toutes	.254 sur chaque VLAN	Pare-feu / Routeur / VPN
Serveur principal	WIN-SRV-01	VLAN 10	172.16.10.1	AD DS / DNS / DHCP (DC1)
Serveur réplica	WIN-SRV-02	VLAN 10	172.16.10.2	AD DS réplica (DC2)
Serveur Zabbix	SRV-ZABBIX	VLAN 10	172.16.10.3	Supervision réseau
Serveur GLPI	SRV-GLPI	VLAN 10	172.16.10.4	Gestion de parc / Tickets
Serveur Proxmox	SRV-PROXMOX	VLAN 10	172.16.10.5	Hyperviseur Proxmox VE

Client RH	WIN-CLIENT-RH	VLAN 20	DHCP	Poste utilisateur RH
Client Tech	WIN-CLIENT-TECH	VLAN 20	DHCP	Poste technicien + logiciel caisse

2.3 Configuration des VLANs

La segmentation réseau en VLANs permet d'isoler les flux entre les serveurs, les postes clients et l'administration. pfSense assure le routage inter-VLAN et applique des règles de filtrage pour contrôler les communications autorisées.

VLAN	ID	Interface pfSense	Sous-réseau	Description
Serveurs	10	em1.10 (OPT1)	172.16.10.0/24	Serveurs Windows, Debian, Proxmox
Clients	20	em1.20 (OPT2)	172.16.20.0/24	Postes utilisateurs (RH, Tech)
Admin	30	em1.30 (OPT3)	172.16.30.0/24	Administration réseau

Matrice de flux inter-VLAN

Source	Destination	Protocoles autorisés	Justification
VLAN 20 (Clients)	VLAN 10 (Serveurs)	DNS, DHCP, LDAP, Kerberos, SMB, HTTP/S	Accès aux services AD, fichiers, GLPI
VLAN 30 (Admin)	VLAN 10 (Serveurs)	Tous	Administration complète des serveurs
VLAN 30 (Admin)	VLAN 20 (Clients)	RDP, ICMP, WMI	Prise en main et supervision des postes
VLAN 10 (Serveurs)	VLAN 20 (Clients)	ICMP, Zabbix Agent (10050)	Supervision des postes par Zabbix
VLAN 20 (Clients)	VLAN 30 (Admin)	Bloqué	Les clients ne doivent pas accéder à l'admin
Tous VLANs	WAN	HTTP/S, DNS	Accès Internet filtré

3. Hyperviseur – VMware Workstation Pro

3.1 Configuration des machines virtuelles

L'ensemble de l'infrastructure est virtualisée sur VMware Workstation Pro. Le PC hôte dispose de 32 Go de RAM, ce qui permet d'allouer 20 Go aux VMs tout en conservant 12 Go pour le système hôte.

VM	OS	RAM	vCPU	Disque	Réseau VMware
pfSense	FreeBSD 14	1 Go	1	20 Go	NAT + VMnet2
WIN-SRV-01	Windows Server 2022	4 Go	2	60 Go	VMnet2
WIN-SRV-02	Windows Server 2022	3 Go	2	60 Go	VMnet2
SRV-ZABBIX	Debian 12	2 Go	2	30 Go	VMnet2
SRV-GLPI	Debian 12	2 Go	2	30 Go	VMnet2
SRV-PROXMOX	Debian 12	4 Go	2	50 Go	VMnet2
WIN-CLIENT-RH	Windows 10/11	2 Go	2	50 Go	VMnet2
WIN-CLIENT-TECH	Windows 10/11	2 Go	2	50 Go	VMnet2

3.2 Configuration réseau VMware

Dans VMware Workstation, la segmentation VLAN est simulée via l'interface LAN unique de pfSense (em1) connectée au VMnet2 (Host-Only). pfSense crée des sous-interfaces VLAN (em1.10, em1.20, em1.30) et assure le routage inter-VLAN. Toutes les VMs sont connectées au VMnet2 et pfSense leur attribue le bon sous-réseau via DHCP ou configuration statique.

VMnet	Type	Sous-réseau	Usage
VMnet8 (NAT)	NAT	192.168.23.0/24	WAN pfSense → Internet
VMnet2	Host-Only	172.16.x.0/24	LAN trunk → VLANs 10, 20, 30

4. Pare-feu et routage – pfSense

4.1 Installation et configuration initiale

pfSense 2.7.2 est installé comme pare-feu/routeur principal de l'infrastructure. Il assure le routage inter-VLAN, le filtrage du trafic, le NAT vers Internet et le service VPN (OpenVPN).

Interfaces réseau

Interface	Assignation	Adresse IP	Rôle
em0	WAN	192.168.23.132/24 (DHCP)	Accès Internet via NAT VMware
em1	LAN (trunk)	-	Interface trunk pour les VLANs
em1.10	OPT1 (VLAN_SERVEURS)	172.16.10.254/24	Passerelle VLAN Serveurs
em1.20	OPT2 (VLAN_CLIENTS)	172.16.20.254/24	Passerelle VLAN Clients
em1.30	OPT3 (VLAN_ADMIN)	172.16.30.254/24	Passerelle VLAN Admin

4.2 Procédure de configuration des VLANs sur pfSense

- Accéder à l'interface web de pfSense (https://172.16.37.254 actuellement)
- Aller dans Interfaces > Assignments > VLANs
- Cliquer sur "+ Add" pour créer chaque VLAN :

  - Parent Interface : em1 | VLAN Tag : 10 | Description : VLAN_SERVEURS

  - Parent Interface : em1 | VLAN Tag : 20 | Description : VLAN_CLIENTS

  - Parent Interface : em1 | VLAN Tag : 30 | Description : VLAN_ADMIN

- Aller dans Interfaces > Assignments et assigner chaque VLAN à une interface (OPT1, OPT2, OPT3)
- Configurer chaque interface avec son adresse IP statique :

  - OPT1 (VLAN 10) : 172.16.10.254/24 | Activée

  - OPT2 (VLAN 20) : 172.16.20.254/24 | Activée

  - OPT3 (VLAN 30) : 172.16.30.254/24 | Activée

- Sauvegarder et appliquer les modifications

4.3 Règles de pare-feu

Les règles de pare-feu sont configurées par interface VLAN pour contrôler les flux autorisés entre les segments réseau. Le principe appliqué est celui du moindre privilège : tout est bloqué par défaut, seuls les flux nécessaires sont explicitement autorisés.

Règles VLAN 10 – Serveurs

Action	Source	Destination	Port	Description
Pass	VLAN10 net	Any	53 (DNS)	Résolution DNS vers Internet
Pass	VLAN10 net	Any	80, 443	Accès HTTP/S (mises à jour)
Pass	VLAN10 net	VLAN20 net	10050	Zabbix Agent vers clients
Pass	VLAN10 net	VLAN20 net	ICMP	Ping vers clients
Block	VLAN10 net	Any	*	Bloquer le reste

Règles VLAN 20 – Clients

Action	Source	Destination	Port	Description
Pass	VLAN20 net	VLAN10 net	53	DNS vers serveur AD
Pass	VLAN20 net	VLAN10 net	88, 389, 636, 445, 135-139	Services AD/Kerberos/LDAP/SMB
Pass	VLAN20 net	VLAN10 net	80, 443	Accès GLPI et Zabbix WebUI
Pass	VLAN20 net	VLAN10 net	67-68	DHCP
Pass	VLAN20 net	Any	80, 443	Navigation Internet
Block	VLAN20 net	VLAN30 net	*	Clients ne voient pas l'admin
Block	VLAN20 net	Any	*	Bloquer le reste

Règles VLAN 30 – Admin

Action	Source	Destination	Port	Description
Pass	VLAN30 net	Any	*	Accès total

				(administration)

4.4 Configuration du NAT

Le NAT sortant (Outbound NAT) est configuré en mode automatique sur pfSense. Tous les VLANs internes sont NATés via l'adresse WAN de pfSense pour accéder à Internet. Aucun NAT entrant n'est configuré car aucun service n'est exposé publiquement.

5. Active Directory – Domaine JDC.local

5.1 Contrôleur de domaine principal (WIN-SRV-01)

WIN-SRV-01 est le contrôleur de domaine principal (DC1) du domaine JDC.local. Il héberge les rôles AD DS, DNS et DHCP. Ce serveur est déjà en place et opérationnel.

Paramètre	Valeur
Hostname	WIN-SRV-01
Adresse IP	172.16.10.1/24
Passerelle	172.16.10.254
DNS primaire	127.0.0.1
DNS secondaire	172.16.10.2
Domaine	JDC.local
Rôles FSMO	Tous (Schema Master, Domain Naming, RID, PDC, Infrastructure)
Services	AD DS, DNS, DHCP

Procédure de reconfiguration IP (migration vers VLAN 10)

PowerShell – Reconfiguration IP de WIN-SRV-01

```
# Supprimer l'ancienne configuration IP
Remove-NetIPAddress -InterfaceAlias "Ethernet0" -Confirm:$false
Remove-NetRoute -InterfaceAlias "Ethernet0" -Confirm:$false

# Configurer la nouvelle IP dans le VLAN 10
New-NetIPAddress -InterfaceAlias "Ethernet0" `
    -IPAddress 172.16.10.1 `
    -PrefixLength 24 `
    -DefaultGateway 172.16.10.254

# Configurer les serveurs DNS
Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" `
    -ServerAddresses 127.0.0.1, 172.16.10.2
```

5.2 Contrôleur de domaine secondaire (WIN-SRV-02)

WIN-SRV-02 est promu en tant que contrôleur de domaine secondaire (DC2) pour assurer la redondance de l'Active Directory. En cas de défaillance de DC1, DC2 prend automatiquement le relais pour l'authentification et les services DNS.

Paramètre	Valeur
Hostname	WIN-SRV-02
Adresse IP	172.16.10.2/24
Passerelle	172.16.10.254
DNS primaire	172.16.10.1
DNS secondaire	127.0.0.1
Domaine	JDC.local
Rôle	Contrôleur de domaine réplica (DC2)

Procédure de promotion en DC réplica

PowerShell – Configuration IP statique

```
# Configurer l'IP statique
New-NetIPAddress -InterfaceAlias "Ethernet0" `
    -IPAddress 172.16.10.2 `
    -PrefixLength 24 `
    -DefaultGateway 172.16.10.254

Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" `
    -ServerAddresses 172.16.10.1
```

PowerShell – Installation du rôle AD DS et promotion

```
# Installer le rôle AD DS
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

# Promouvoir en DC réplica du domaine JDC.local
Install-ADDSDomainController `
    -DomainName "JDC.local" `
    -Credential (Get-Credential JDC\Administrateur) `
    -InstallDNS:$true `
    -DatabasePath "C:\Windows\NTDS" `
    -LogPath "C:\Windows\NTDS" `
    -SYSVOLPath "C:\Windows\SYSVOL" `
    -ReplicationSourceDC "WIN-SRV-01.JDC.local" `
    -Confirm:$false

# Le serveur redémarrera automatiquement
```

5.3 Configuration DNS

Le service DNS est intégré à Active Directory. WIN-SRV-01 est le serveur DNS principal, WIN-SRV-02 héberge une zone DNS répliquée automatiquement via AD. Les zones de recherche directe et inversée sont configurées pour le domaine JDC.local.

PowerShell – Création des zones de recherche inversée

```
# Zone inversée pour le VLAN 10 (Serveurs)
Add-DnsServerPrimaryZone -NetworkId "172.16.10.0/24" `
    -ReplicationScope "Domain" -DynamicUpdate "Secure"

# Zone inversée pour le VLAN 20 (Clients)
Add-DnsServerPrimaryZone -NetworkId "172.16.20.0/24" `
    -ReplicationScope "Domain" -DynamicUpdate "Secure"

# Zone inversée pour le VLAN 30 (Admin)
Add-DnsServerPrimaryZone -NetworkId "172.16.30.0/24" `
    -ReplicationScope "Domain" -DynamicUpdate "Secure"

# Vérification
Get-DnsServerZone
```

5.4 Configuration DHCP

Le service DHCP sur WIN-SRV-01 distribue les adresses IP aux clients du VLAN 20. Les serveurs du VLAN 10 utilisent des adresses IP statiques. Un relais DHCP (DHCP Relay) est configuré sur pfSense pour transmettre les requêtes DHCP du VLAN 20 vers WIN-SRV-01 situé dans le VLAN 10.

PowerShell – Configuration de l'étendue DHCP VLAN 20

```
# Créer l'étendue DHCP pour le VLAN 20 (Clients)
Add-DhcpServerv4Scope -Name "VLAN20_Clients" `
    -StartRange 172.16.20.10 `
    -EndRange 172.16.20.50 `
    -SubnetMask 255.255.255.0 `
    -LeaseDuration 08:00:00 `
    -State Active

# Configurer les options d'étendue
Set-DhcpServerv4OptionValue -ScopeId 172.16.20.0 `
    -Router 172.16.20.254 `
    -DnsServer 172.16.10.1, 172.16.10.2 `
    -DnsDomain "JDC.local"

# Autoriser le serveur DHCP dans AD
Add-DhcpServerInDC -DnsName "WIN-SRV-01.JDC.local" -IPAddress 172.16.10.1
```

Configuration du DHCP Relay sur pfSense

- Dans pfSense, aller dans Services > DHCP Relay
- Activer le DHCP Relay
- Sélectionner l'interface VLAN_CLIENTS (OPT2) comme interface d'écoute
- Renseigner l'adresse du serveur DHCP : 172.16.10.1
- Sauvegarder et appliquer

5.5 Structure des OU et utilisateurs

L'arborescence Active Directory est organisée en Unités d'Organisation (OU) reflétant la structure de l'entreprise JDC.

PowerShell – Création des OU et utilisateurs

```
# Création des OU principales
New-ADOrganizationalUnit -Name "JDC" -Path "DC=JDC,DC=local"
New-ADOrganizationalUnit -Name "Utilisateurs" -Path "OU=JDC,DC=JDC,DC=local"
New-ADOrganizationalUnit -Name "Ordinateurs" -Path "OU=JDC,DC=JDC,DC=local"
New-ADOrganizationalUnit -Name "Groupes" -Path "OU=JDC,DC=JDC,DC=local"

# Création des sous-OU par service
New-ADOrganizationalUnit -Name "RH" -Path "OU=Utilisateurs,OU=JDC,DC=JDC,DC=local"
New-ADOrganizationalUnit -Name "Technique" -Path
"OU=Utilisateurs,OU=JDC,DC=JDC,DC=local"
New-ADOrganizationalUnit -Name "Direction" -Path
"OU=Utilisateurs,OU=JDC,DC=JDC,DC=local"

# Création des groupes de sécurité
New-ADGroup -Name "GRP_RH" -GroupScope Global -Path "OU=Groupes,OU=JDC,DC=JDC,DC=local"
New-ADGroup -Name "GRP_Tech" -GroupScope Global -Path
"OU=Groupes,OU=JDC,DC=JDC,DC=local"
New-ADGroup -Name "GRP_Direction" -GroupScope Global -Path
"OU=Groupes,OU=JDC,DC=JDC,DC=local"

# Exemple de création d'utilisateur
New-ADUser -Name "Jean Dupont" -GivenName "Jean" -Surname "Dupont" `
    -SamAccountName "j.dupont" -UserPrincipalName "j.dupont@JDC.local" `
    -Path "OU=RH,OU=Utilisateurs,OU=JDC,DC=JDC,DC=local" `
    -AccountPassword (ConvertTo-SecureString "P@ssw0rd2026!" -AsPlainText -Force) `
    -Enabled $true -ChangePasswordAtLogon $true

Add-ADGroupMember -Identity "GRP_RH" -Members "j.dupont"
```

6. Stratégies de groupe (GPO)

Les stratégies de groupe (GPO) permettent de centraliser la gestion et la sécurité des postes et utilisateurs du domaine JDC.local. Les GPO suivantes sont adaptées au contexte métier de JDC (environnement de caisse et TPE où la sécurité des postes est critique).

6.1 GPO – Politique de mot de passe

Nom de la GPO : GPO_Securite_MDP

Chemin : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de mot de passe

Paramètre	Valeur
Longueur minimale du mot de passe	12 caractères
Le mot de passe doit respecter des exigences de complexité	Activé
Durée de vie maximale du mot de passe	90 jours
Durée de vie minimale du mot de passe	1 jour
Conserver l'historique des mots de passe	5 mots de passe
Seuil de verrouillage de compte	5 tentatives
Durée de verrouillage de compte	30 minutes

6.2 GPO – Fond d'écran entreprise JDC

Nom de la GPO : GPO_Fond_Ecran_JDC

Chemin : Configuration utilisateur > Stratégies > Modèles d'administration > Bureau > Bureau > Papier peint du Bureau

Paramètre	Valeur
Nom du papier peint	\\WIN-SRV-01\Partage\fond_jdc.jpg
Style du papier peint	Étirer
Empêcher la modification du papier peint	Activé

6.3 GPO – Restriction panneau de configuration

Nom de la GPO : GPO_Restriction_PanneauConfig

Chemin : Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration

Paramètre	Valeur
Interdire l'accès au Panneau de configuration et aux paramètres	Activé
Masquer les éléments spécifiés du Panneau de configuration	Activé

6.4 GPO – Blocage USB (sécurité POS)

Nom de la GPO : GPO_Blocage_USB

Chemin : Configuration ordinateur > Stratégies > Modèles d'administration > Système > Accès au stockage amovible

Paramètre	Valeur
Toutes les classes de stockage amovible : refuser l'accès en lecture	Activé
Toutes les classes de stockage amovible : refuser l'accès en écriture	Activé
Justification	Sécurité des postes de caisse — prévention d'exfiltration de données

6.5 GPO – Mappage lecteurs réseau

Nom de la GPO : GPO_Lecteurs_Reseau

Chemin : Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteurs

Paramètre	Valeur
Lecteur P: (Partage commun)	\\WIN-SRV-01\Partage

Lecteur R: (Service RH)	\\WIN-SRV-01\RH (filtré par groupe GRP_RH)
Lecteur T: (Service Technique)	\\WIN-SRV-01\Technique (filtré par groupe GRP_Tech)

6.6 GPO – Verrouillage automatique de session

Nom de la GPO : GPO_Verrouillage_Session

Chemin : Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration > Personnalisation

Paramètre	Valeur
Activer l'écran de veille	Activé
Délai d'activation de l'écran de veille	300 secondes (5 min)
Protéger l'écran de veille par mot de passe	Activé
Justification	Sécurité des postes de caisse en magasin

7. Supervision – Zabbix

7.1 Installation sur Debian 12

Paramètre	Valeur
Hostname	SRV-ZABBIX
OS	Debian 12 (Bookworm)
IP	172.16.10.3/24
Passerelle	172.16.10.254
DNS	172.16.10.1
Version Zabbix	7.0 LTS
Base de données	MariaDB
Serveur web	Apache2

Bash – Installation de Zabbix 7.0 LTS sur Debian 12

```
# Configuration IP statique
cat > /etc/network/interfaces.d/eth0 << EOF
auto eth0
iface eth0 inet static
    address 172.16.10.3
    netmask 255.255.255.0
    gateway 172.16.10.254
    dns-nameservers 172.16.10.1
EOF
systemctl restart networking

# Ajouter le dépôt Zabbix
wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-
release_latest_7.0+debian12_all.deb
dpkg -i zabbix-release_latest_7.0+debian12_all.deb
apt update

# Installer Zabbix Server, Frontend, Agent
apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-
scripts zabbix-agent

# Installer MariaDB
apt install -y mariadb-server
systemctl enable --now mariadb

# Créer la base de données
mysql -u root << MYSQL
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'ZabbixJDC2026!';
```

```
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
SET GLOBAL log_bin_trust_function_creators = 1;
FLUSH PRIVILEGES;
MYSQL

# Importer le schéma initial
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-
set=utf8mb4 -uzabbix -p'ZabbixJDC2026!' zabbix

# Configurer Zabbix Server
sed -i 's/# DBPassword=/DBPassword=ZabbixJDC2026!/' /etc/zabbix/zabbix_server.conf

# Démarrer les services
systemctl enable --now zabbix-server zabbix-agent apache2

# Accès WebUI : http://172.16.10.3/zabbix
# Login par défaut : Admin / zabbix
```

7.2 Configuration des hôtes supervisés

Chaque machine de l'infrastructure est ajoutée comme hôte dans Zabbix avec l'agent Zabbix installé. Les serveurs Windows utilisent l'agent Zabbix pour Windows, les serveurs Debian utilisent l'agent Linux.

Hôte	IP	Agent	Template Zabbix
WIN-SRV-01	172.16.10.1	Zabbix Agent (Windows)	Windows by Zabbix agent
WIN-SRV-02	172.16.10.2	Zabbix Agent (Windows)	Windows by Zabbix agent
SRV-GLPI	172.16.10.4	Zabbix Agent (Linux)	Linux by Zabbix agent
SRV-PROXMOX	172.16.10.5	Zabbix Agent (Linux)	Linux by Zabbix agent
pfSense	172.16.10.254	SNMP	pfSense by SNMP
WIN-CLIENT-RH	DHCP	Zabbix Agent (Windows)	Windows by Zabbix agent
WIN-CLIENT-TECH	DHCP	Zabbix Agent (Windows)	Windows by Zabbix agent

PowerShell – Installation de l'agent Zabbix sur Windows

```
# Télécharger l'agent Zabbix pour Windows
# URL : https://www.zabbix.com/download_agents

# Installation silencieuse
```

```
msiexec /i zabbix_agent-7.0.0-windows-amd64.msi /qn `
    SERVER=172.16.10.3 `
    SERVERACTIVE=172.16.10.3 `
    HOSTNAME=WIN-SRV-01

# Vérifier le service
Get-Service "Zabbix Agent"
```

7.3 Alertes et tableaux de bord

Des alertes sont configurées pour les événements critiques : espace disque faible, charge CPU élevée, service arrêté, perte de connectivité réseau. Un tableau de bord personnalisé "JDC - Infrastructure" regroupe les indicateurs clés de l'ensemble des machines supervisées.

8. Gestion de parc – GLPI

8.1 Installation sur Debian 12

Paramètre	Valeur
Hostname	SRV-GLPI
OS	Debian 12 (Bookworm)
IP	172.16.10.4/24
Passerelle	172.16.10.254
DNS	172.16.10.1
Version GLPI	10.x
Base de données	MariaDB
Serveur web	Apache2 + PHP 8.2

Bash – Installation de GLPI sur Debian 12

```
# Configuration IP statique
cat > /etc/network/interfaces.d/eth0 << EOF
auto eth0
iface eth0 inet static
    address 172.16.10.4
    netmask 255.255.255.0
    gateway 172.16.10.254
    dns-nameservers 172.16.10.1
EOF
systemctl restart networking

# Installer les prérequis
apt install -y apache2 mariadb-server php php-
{mysql,curl,gd,intl,xml,mbstring,ldap,zip,bz2} libapache2-mod-php

# Créer la base de données GLPI
mysql -u root << MYSQL
CREATE DATABASE glpi CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'glpi'@'localhost' IDENTIFIED BY 'GlpiJDC2026!';
GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost';
FLUSH PRIVILEGES;
MYSQL

# Télécharger et installer GLPI
cd /tmp
wget https://github.com/glpi-project/glpi/releases/download/10.0.16/glpi-10.0.16.tgz
tar xzf glpi-10.0.16.tgz -C /var/www/html/
chown -R www-data:www-data /var/www/html/glpi
chmod -R 755 /var/www/html/glpi
```

```
# Redémarrer Apache
systemctl restart apache2

# Accès WebUI : http://172.16.10.4/glpi
# Login par défaut : glpi / glpi
# IMPORTANT : Changer les mots de passe par défaut après installation !
```

8.2 Configuration et inventaire

GLPI est configuré pour inventorier automatiquement le parc informatique de JDC. L'agent GLPI (anciennement FusionInventory) est déployé sur chaque poste et serveur pour remonter les informations matérielles et logicielles.

8.3 Gestion des tickets

Le module de helpdesk de GLPI permet aux utilisateurs de JDC de soumettre des tickets d'incident ou de demande. Les tickets sont catégorisés (matériel de caisse, réseau, logiciel, TPE) et attribués automatiquement aux techniciens selon leur spécialité.

9. Virtualisation – Proxmox VE

9.1 Installation sur Debian 12

Paramètre	Valeur
Hostname	SRV-PROXMOX
OS	Debian 12 (Bookworm)
IP	172.16.10.5/24
Passerelle	172.16.10.254
DNS	172.16.10.1
Version Proxmox VE	8.x
RAM	4 Go
Interface web	https://172.16.10.5:8006

Bash – Installation de Proxmox VE sur Debian 12

```
# Configuration IP statique et hostname
hostnamectl set-hostname srv-proxmox
echo "172.16.10.5 srv-proxmox.jdc.local srv-proxmox" >> /etc/hosts

cat > /etc/network/interfaces.d/eth0 << EOF
auto eth0
iface eth0 inet static
    address 172.16.10.5
    netmask 255.255.255.0
    gateway 172.16.10.254
    dns-nameservers 172.16.10.1
EOF
systemctl restart networking

# Ajouter le dépôt Proxmox VE
echo "deb http://download.proxmox.com/debian/pve bookworm pve-no-subscription" >
/etc/apt/sources.list.d/pve.list

# Ajouter la clé GPG
wget https://enterprise.proxmox.com/debian/proxmox-release-bookworm.gpg -O
/etc/apt/trusted.gpg.d/proxmox-release-bookworm.gpg

# Mettre à jour et installer Proxmox VE
apt update && apt full-upgrade -y
apt install -y proxmox-ve postfix open-iscsi chrony

# Redémarrer
reboot
```

```
# Accès WebUI : https://172.16.10.5:8006
# Login : root / (mot de passe root Debian)
```

9.2 Configuration et gestion

Proxmox VE offre une interface web complète pour la gestion des machines virtuelles et des conteneurs LXC. Dans le cadre du projet JDC, Proxmox démontre la compétence en virtualisation et permet de créer des environnements de test pour les configurations de caisse avant déploiement chez les clients.

10. VPN – OpenVPN sur pfSense

10.1 Configuration du serveur OpenVPN

OpenVPN est configuré sur pfSense pour permettre aux techniciens JDC de se connecter à distance à l'infrastructure de l'entreprise. Cela permet les interventions de maintenance à distance sur les serveurs et les équipements de caisse.

- Dans pfSense, aller dans System > Cert. Manager > CAs
- Créer une autorité de certification (CA) : "JDC-CA"
    - Method : Create an internal Certificate Authority
    - Key length : 2048 bits | Digest : SHA256 | Lifetime : 3650 jours
    - CN : JDC-CA
- Créer un certificat serveur : System > Cert. Manager > Certificates
    - Method : Create an internal Certificate
    - CA : JDC-CA | Type : Server Certificate
    - CN : vpn.jdc.local
- Configurer le serveur OpenVPN : VPN > OpenVPN > Servers > + Add
    - Server mode : Remote Access (SSL/TLS + User Auth)
    - Protocol : UDP on IPv4 only | Port : 1194
    - TLS Configuration : Auto-generate TLS Key
    - Peer Certificate Authority : JDC-CA
    - Server Certificate : vpn.jdc.local
    - Tunnel Network : 10.10.10.0/24
    - Local Network : 172.16.10.0/24, 172.16.20.0/24, 172.16.30.0/24
    - DNS Server 1 : 172.16.10.1
- Créer les règles de pare-feu :
    - WAN : autoriser UDP 1194 depuis Any
    - OpenVPN : autoriser tout le trafic du tunnel
- Installer le package "openvpn-client-export" pour exporter les configs client

10.2 Réseau VPN

Paramètre	Valeur
Type	Remote Access (SSL/TLS + User Auth)

Protocole	UDP
Port	1194
Réseau tunnel	10.10.10.0/24
Réseaux accessibles	172.16.10.0/24, 172.16.20.0/24, 172.16.30.0/24
Authentification	Certificat + identifiants AD (LDAP)
Chiffrement	AES-256-GCM

11. Tests et validation

Cette section recense les tests effectués pour valider le bon fonctionnement de l'ensemble de l'infrastructure.

Test	Commande / Action	Résultat attendu	Statut
Ping inter-VLAN (Client → Serveur)	ping 172.16.10.1 depuis client	Réponse OK	☐
Résolution DNS	nslookup WIN-SRV-01.JDC.local	Résolu en 172.16.10.1	☐
Jonction au domaine (Client)	Ajouter WIN-CLIENT-TECH au domaine	Jonction réussie	☐
Authentification AD	Connexion avec j.dupont sur client	Session ouverte	☐
Réplication AD	repadmin /replsummary	0 erreurs	☐
DHCP Client	ipconfig /renew sur VLAN 20	IP dans 172.16.20.10-50	☐
Accès GLPI	http://172.16.10.4/glpi	Page de connexion	☐
Accès Zabbix	http://172.16.10.3/zabbix	Page de connexion	☐
Accès Proxmox	https://172.16.10.5:8006	Page de connexion	☐
Supervision Zabbix	Vérifier les hôtes dans Zabbix	Tous les hôtes en vert	☐
GPO fond d'écran	gpupdate /force + redémarrage	Fond JDC appliqué	☐
GPO blocage USB	Brancher clé USB	Accès refusé	☐
VPN OpenVPN	Connexion depuis client externe	Tunnel établi, accès LAN	☐
Blocage Client → Admin	ping 172.16.30.254 depuis VLAN 20	Timeout (bloqué)	☐
NAT Internet	ping 8.8.8.8 depuis VLAN 20	Réponse OK	☐

12. Annexes

Annexe A – Récapitulatif des identifiants

Service	URL / Accès	Identifiant	Mot de passe par défaut
pfSense WebUI	https://172.16.10.254	admin	pfsense (à changer)
Windows AD	WIN-SRV-01	Administrateur	(défini à l'installation)
Zabbix	http://172.16.10.3/zabbix	Admin	zabbix (à changer)
GLPI	http://172.16.10.4/glpi	glpi	glpi (à changer)
Proxmox VE	https://172.16.10.5:8006	root	(mot de passe root Debian)

Annexe B – Ports utilisés

Service	Port	Protocole	Description
DNS	53	TCP/UDP	Résolution de noms
DHCP	67-68	UDP	Attribution d'adresses IP
Kerberos	88	TCP/UDP	Authentification AD
LDAP	389	TCP	Annuaire Active Directory
LDAPS	636	TCP	LDAP sécurisé
SMB	445	TCP	Partage de fichiers
RDP	3389	TCP	Bureau à distance
HTTP	80	TCP	GLPI, Zabbix
HTTPS	443	TCP	pfSense WebUI
Proxmox	8006	TCP	Interface web Proxmox
Zabbix Agent	10050	TCP	Agent de supervision
Zabbix Server	10051	TCP	Serveur de supervision
OpenVPN	1194	UDP	VPN
SNMP	161	UDP	Supervision pfSense