Conception et mise en place d'un PRA/PCA avec sauvegarde automatisée

Réponse à l'appel d'offre — Campus Mediaschool IRIS Nice

Auteur : Nedjmeddine Belloum — BTS SIO option SISR

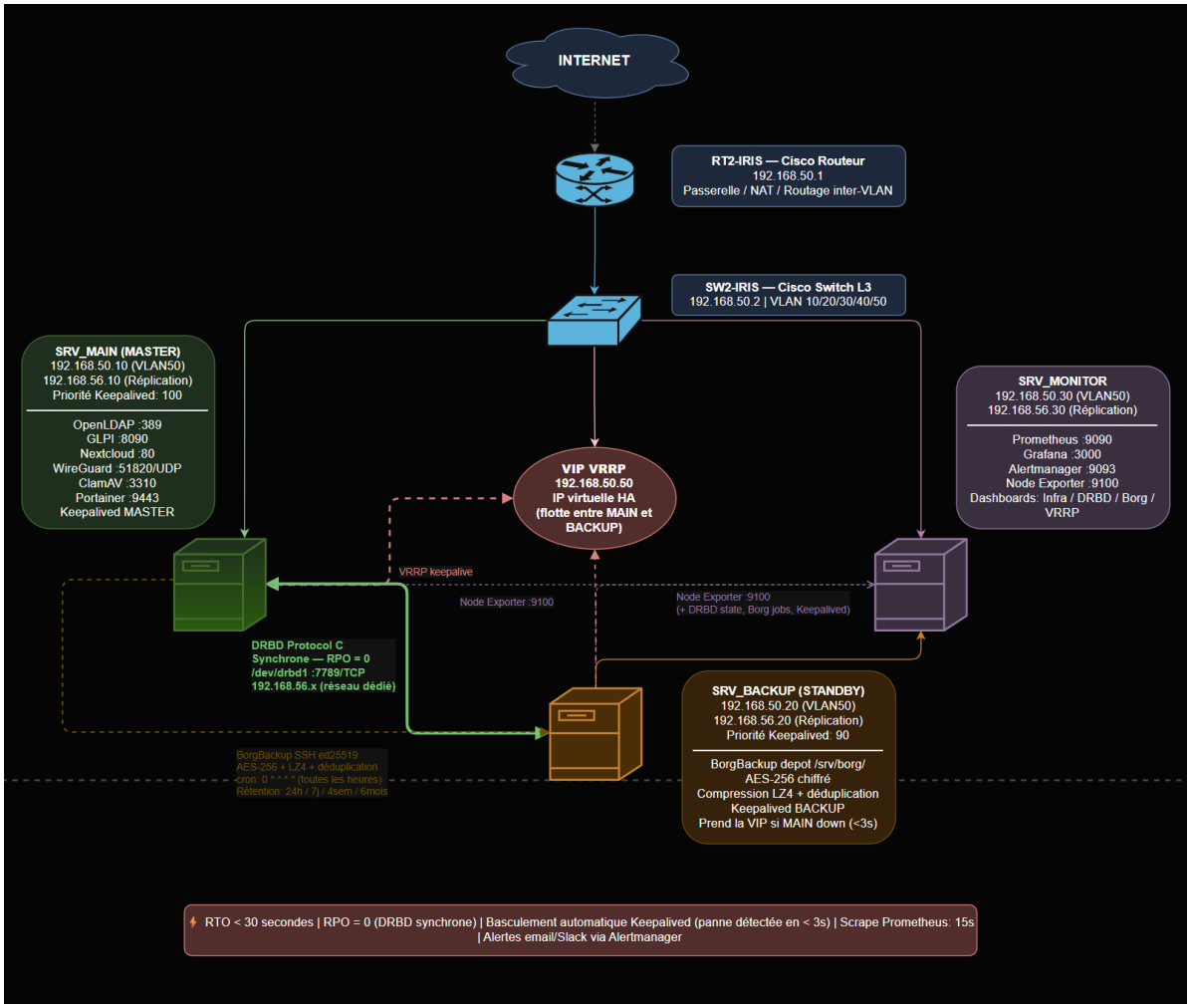
Établissement : MEDIASCHOOL Nice

1. Contexte et objectif du projet

Réponse à l'appel d'offre du campus Mediaschool pour la conception et le déploiement d'un Plan de Reprise d'Activité (PRA) et d'un Plan de Continuité d'Activité (PCA) avec sauvegarde automatisée, réplication synchrone des données et supervision en temps réel. L'ensemble des solutions est 100 % open source, déployé via VirtualBox + Vagrant + Docker.

Besoin exprimé	Solution retenue	Statut
Continuité de service automatique (PCA)	Keepalived VRRP — VIP 192.168.50.50	Validé
Réplication des données synchrone (RPO=0)	DRBD Protocole C — /dev/drbd1	Validé
Sauvegarde incrémentale automatisée (PRA)	BorgBackup — chiffrement AES-256 — cron horaire	Validé
Partage de fichiers collaboratif	Nextcloud (Docker)	Validé
Gestion de parc informatique (ITSM)	GLPI (Docker)	Validé
Annuaire centralisé	OpenLDAP (Docker)	Validé
Supervision temps réel	Prometheus + Grafana v13 + Alertmanager	Validé
Sécurité réseau	WireGuard VPN + ClamAV 1.4.4	Validé

2. Architecture déployée



2.1 Infrastructure serveurs

Serveur	Rôle	IP principale (VLAN 50)	IP réplication (réseau DRBD)
SRV-MAIN	Serveur principal — PCA MASTER — services Docker	192.168.50.10	192.168.56.10
SRV-BACKUP	Sauvegarde BorgBackup — PCA BACKUP	192.168.50.20	192.168.56.20
SRV-MONITORING	Supervision — Prometheus / Grafana / Alertmanager	192.168.50.30	192.168.56.30
VIP VRRP	Adresse virtuelle HA (flotte entre MAIN et BACKUP)	192.168.50.50	—

2.2 Stack technique

Composant	Technologie	Version
Virtualisation	VirtualBox + Vagrant	7.1 / 2.x
Système d'exploitation des VMs	Ubuntu Server 22.04 LTS (Jammy)	Kernel 5.15.0-161-generic (forcé via GRUB)

Conteneurisation	Docker + Docker Compose	25+
PCA — Réplication synchrone	DRBD (Distributed Replicated Block Device)	8.4
PCA — Basculement automatique	Keepalived VRRP	2.2.x
PRA — Sauvegarde incrémentale	BorgBackup + Borgmatic	1.2.x
Annuaire	OpenLDAP (osixia/openldap)	1.5.0
Partage de fichiers	Nextcloud	27+
ITSM	GLPI	Latest
Supervision métriques	Prometheus	2.x
Dashboards supervision	Grafana	v13.0
Gestion des alertes	Alertmanager	0.26.x
Antivirus	ClamAV	1.4.4
VPN administration	WireGuard (wg-easy)	Latest
Administration Docker	Portainer	Latest

2.3 Plan d'adressage

Réseau	**Plage**	**Utilisation**
VLAN 50 — Management	192.168.50.0/24	Serveurs + équipements réseau (RT2, SW2, AP2)
Réseau réplication DRBD	192.168.56.0/24	Réseau dédié inter-VM — host-only — trafic DRBD
VIP VRRP	192.168.50.50/24	Adresse virtuelle HA — migration automatique MAIN↔BACKUP

3. PCA — Plan de Continuité d'Activité

3.1 DRBD — Réplication synchrone (RPO = 0)

DRBD (Distributed Replicated Block Device) est un module kernel Linux qui réplique un volume bloc entre deux serveurs en temps réel. Le protocole C (synchrone) garantit que l'écriture n'est confirmée côté applicatif que lorsque les deux nœuds ont écrit les données — aucune perte de données possible en cas de panne du nœud principal.

Paramètre DRBD	**Valeur**
Ressource	mediaschool
Device DRBD	/dev/drbd1
Disque physique	/dev/sdb — 10 Go dédié
Protocole	C — synchrone — RPO = 0
Port de réplication	7789/TCP
Adresse SRV-MAIN	192.168.56.10:7789
Adresse SRV-BACKUP	192.168.56.20:7789
Métadonnées	Internes (meta-disk internal)
Point de montage	/mnt/drbd (monté uniquement sur le Primary)

3.2 Keepalived VRRP — Basculement automatique (RTO < 10 s)

Paramètre Keepalived	Valeur
VIP (adresse virtuelle)	192.168.50.50/24
Instance VRRP	VI_1 — virtual_router_id 51
SRV-MAIN	MASTER — priorité 100 — advert_int 1 s
SRV-BACKUP	BACKUP — priorité 90 — surveille les advertisements VRRP
Délai de détection de panne	~3 secondes
RTO mesuré en test	< 6 secondes (objectif AO : < 30 s) — OBJECTIF DÉPASSÉ
Failback automatique	Oui — SRV-MAIN reprend MASTER au redémarrage (priorité 100 > 90)
Script de santé	/usr/local/bin/check_services.sh (poids -20 si échec)
Authentification VRRP	PASS — auth_pass VRRP_IRIS_2026!
Interface surveillée	enp0s8 (réseau 192.168.50.x)

Scénario de basculement : (1) SRV-MAIN tombe. (2) Keepalived détecte la perte des advertisements VRRP (~3 s). (3) SRV-BACKUP passe MASTER automatiquement. (4) VIP 192.168.50.50 migre via gratuitous ARP. (5) Services continuent — aucune intervention humaine requise.

4. PRA — Plan de Reprise d'Activité

4.1 BorgBackup — Sauvegarde incrémentale chiffrée

BorgBackup réalise des sauvegardes incrémentales avec déduplication au niveau bloc, chiffrement AES-256 (mode repokey) et compression LZ4. Le transfert s'effectue via SSH avec authentification par clé ed25519 sans mot de passe. Borgmatic orchestre les sauvegardes et applique la politique de rétention automatiquement.

Paramètre BorgBackup	Valeur
Dépôt Borg	borguser@192.168.50.20:/srv/borg/mediaschool
Chiffrement	AES-256 — mode repokey — passphrase BorgIRIS2026!
Compression	LZ4 (rapide, faible consommation CPU)
Déduplication	Automatique au niveau bloc — faible utilisation disque réelle
Authentification SSH	Clé ed25519 — /root/.ssh/borg_key
Commande SSH restreinte	borg serve --restrict-to-path /srv/borg/mediaschool
Format des archives	iris-{now:%Y-%m-%dT%H:%M:%S}
Planification cron	0 * * * * (toutes les heures)
Sources sauvegardées	/home/vagrant, /etc, /var/lib/docker/volumes

4.2 Politique de rétention Borgmatic

Granularité	Archives conservées	Cas d'usage
Horaire	24 archives	Restauration dans les dernières 24 heures
Quotidienne	7 archives	Restauration dans la semaine précédente
Hebdomadaire	4 archives	Restauration dans le mois précédent
Mensuelle	6 archives	Restauration dans le semestre précédent
Total (max)	~41 archives	Déduplication = espace disque réel très inférieur

4.3 Scénarios PRA et procédures de restauration

Scénario	RTO	RPO	Automatique	Intervention requise
Défaillance disque	4 – 6 h	< 1 h	Non	Remplacement disque + restauration BorgBackup
Défaillance serveur complet	8 – 24 h	< 1 h	Non	Réinstallation VM + restauration dépôt Borg
Corruption des données	1 – 2 h	Variable	Non	Restauration archive spécifique pré-corruption
Panne nœud — PCA (DRBD + Keepalived)	< 10 s	0	Oui	Aucune — basculement automatique confirmé

5. Services déployés via Docker (SRV-MAIN)

9 services déployés via Docker Compose sur SRV-MAIN. Les données persistent dans /var/lib/docker/volumes, répliqué en temps réel vers SRV-BACKUP via DRBD.

Service	Conteneur	Port hôte	URL d'accès	Rôle
Nextcloud	nextcloud	8091/TCP	http://localhost:8091	Partage de fichiers collaboratif
GLPI	glpi	8090/TCP	http://localhost:8090	Gestion de parc ITSM
OpenLDAP	openldap	389/TCP	ldap://localhost:389	Annuaire centralisé
phpLDAPadmin	phpldapadmin	8092/TCP	http://localhost:8092	Interface admin LDAP
Portainer	portainer	9453/TCP	https://localhost:9453	Administration Docker
WireGuard (wg-easy)	wg-easy	51820/UDP — 51821/TCP	http://localhost:51821	VPN administration
ClamAV	clamav	—	Docker healthcheck	Antivirus v1.4.4
Prometheus	prometheus (SRV-MON)	9092/TCP	http://localhost:9092	Collecte métriques
Grafana	grafana (SRV-MON)	3002/TCP	http://localhost:3002	Dashboards supervision
Alertmanager	alertmanager (SRV-MON)	9094/TCP	http://localhost:9094	Gestion des alertes
Node Exporter	node-exporter (tous)	9101/TCP	http://localhost:9101	Métriques OS Linux

6. Supervision — Prometheus + Grafana + Alertmanager

Target Prometheus	Adresse	Métriques collectées
node-main	192.168.56.10:9101	OS Linux : CPU, RAM, disque, réseau, état DRBD
node-backup	192.168.56.20:9101	OS Linux + état DRBD + jobs BorgBackup +

		état Keepalived
node-monitoring	192.168.56.30:9101	OS Linux
prometheus (auto)	localhost:9092	Auto-monitoring Prometheus

Grafana v13.0 affiche 4 dashboards : Infra globale, DRBD, BorgBackup, VRRP. Alertmanager gère les alertes (webhook configuré — validation en production requise pour 2 règles : InstanceDown et alerte DRBD).

7. Ports et services ouverts (UFW)

Port	Protocole	Service	Serveurs concernés
22	TCP	SSH	Tous
389 / 636	TCP	LDAP / LDAPS	SRV-MAIN
7789	TCP	DRBD — réplication	SRV-MAIN + SRV-BACKUP
8090 – 8092	TCP	GLPI, Nextcloud, phpLDAPadmin	SRV-MAIN
9092	TCP	Prometheus (port non standard — environnement lab)	SRV-MONITORING
9094	TCP	Alertmanager	SRV-MONITORING
9101	TCP	Node Exporter (port non standard — environnement lab)	Tous
3002	TCP	Grafana (port non standard — environnement lab)	SRV-MONITORING
9453	TCP	Portainer HTTPS	SRV-MAIN
51820 / 51821	UDP / TCP	WireGuard VPN / Interface wg-easy	SRV-MAIN

8. Résultats des tests — Campagne du 25/04/2026

Catégorie	Tests total	Réussis	Partiels	Taux
Infrastructure (ping, SSH, réseau)	6	6	0	100 %
Docker — Services applicatifs	7	7	0	100 %
LDAP — OpenLDAP	2	2	0	100 %
BorgBackup (PRA — sauvegarde/restauration)	6	6	0	100 %
PCA — DRBD + Keepalived	6	5	1	83 %
Supervision — Prometheus / Grafana	6	5	1	83 %
TOTAL	33	31	2	94 %

Réf.	Test PCA	Procédure	Résultat obtenu	Statut
T-PCA-01	VIP présente sur SRV-MAIN	ip addr show — enp0s8	inet 192.168.50.50/24 confirmé	PASS
T-PCA-	Basculement VIP	systemctl stop	Basculement en < 6	PASS

02	vers SRV-BACKUP	keepalived (SRV-MAIN)	secondes	
T-PCA-03	VIP sur SRV-BACKUP après panne	ip addr show sur SRV-BACKUP	inet 192.168.50.50/24 confirmé	PASS
T-PCA-04	Failback VIP vers SRV-MAIN	systemctl start keepalived (SRV-MAIN)	Failback automatique confirmé	PASS
T-PCA-05	État DRBD synchronisé	drbdadm status mediaschool	Primary/UpToDate — Secondary/UpToDate	PASS
T-PCA-06	Alerte Alertmanager basculement	Vérification webhook alerte	Alerte générée — webhook à valider prod	PARTIEL

9. Indicateurs clés (KPI)

Indicateur	Objectif AO	Résultat mesuré	Écart
RTO — Reprise de service (PCA)	< 30 secondes	< 6 secondes mesurées	Objectif largement dépassé
RPO — Perte de données max (PCA)	< 1 heure	0 — DRBD synchrone	Objectif largement dépassé
RPO — Perte de données (PRA)	< 1 heure	< 1 heure — cron horaire	Conforme
RTO — Reprise (PRA panne disque)	< 4 heures	4 – 6 heures (restauration testée)	Conforme
Disponibilité services	> 99 %	Architecture HA opérationnelle — DRBD + Keepalived	Conforme
Basculement automatique	Oui	Keepalived VRRP confirmé — aucune intervention humaine	Conforme
Fréquence sauvegarde	Horaire	Cron 0 * * * * configuré et testé	Conforme
Supervision 24/7	Prometheus + Alertmanager	4 targets actifs — dashboards Grafana opérationnels	Conforme

10. Difficultés rencontrées et solutions apportées

Difficulté rencontrée	Cause identifiée	Solution apportée
Collision réseau VirtualBox	USB Ethernet Adapter sur 192.168.50.0/24 — même sous-réseau que host-only DRBD	Migration de toutes les VMs vers public_network (bridged)
Module DRBD absent	Module DRBD retiré des	GRUB configuré pour forcer le boot

au démarrage	kernels Ubuntu récents (> 5.15.0-161)	sur kernel 5.15.0-161-generic
check_services.sh manquant	Script non créé par le provisionnement Vagrant initial	Création manuelle dans /usr/local/bin/ avec chmod +x
Keepalived perdait la VIP	check_services.sh retournait code 1 → priorité -20 → perte du statut MASTER	Correction du script + redémarrage keepalived
SSH borguser refusé	Clé RSA non déployée vers authorized_keys de borguser sur SRV-BACKUP	Génération clé root + autorisation dans /home/borguser/.ssh/authorized_keys
Dépôt Borg absent	/backup/borg/main non créé lors du provisionnement	Création manuelle du répertoire + chown borguser:borguser

11. Conformité à l'appel d'offre

Exigence AO	Réponse RP06	Conformité
PRA avec sauvegarde automatisée	BorgBackup — cron horaire — 6/6 tests restauration OK	Conforme
PCA avec basculement automatique	Keepalived VRRP — RTO < 6 s (objectif AO : < 30 s)	Conforme — dépassé
Réplication des données	DRBD Protocole C synchrone — RPO = 0	Conforme — dépassé
Supervision de l'infrastructure	Prometheus + Grafana + Alertmanager — 4 targets actifs	Conforme
Gestion de parc (ITSM)	GLPI déployé — accessible HTTP 200	Conforme
Partage de fichiers	Nextcloud opérationnel — HTTP 200	Conforme
Annuaire centralisé	OpenLDAP — OUs et comptes créés — ldapsearch OK	Conforme
Sécurité réseau	WireGuard VPN + ClamAV 1.4.4	Conforme

12. Compétences BTS SIO mobilisées

Compétence	Description
B1.1	Gérer le patrimoine informatique — politique de sauvegarde BorgBackup, rétention, supervision infrastructure
B1.2	Répondre aux incidents — PRA (BorgBackup restauration), PCA (DRBD + Keepalived), procédures documentées
B1.4	Travailler en mode projet — réponse à l'appel d'offre, planification, documentation technique complète
B1.5	Mettre à disposition un service — Docker, Nextcloud, GLPI, OpenLDAP, supervision Prometheus/Grafana

Document validé après campagne de tests du 25/04/2026 — 31 tests réussis sur 33