Gestion d'infrastructure Datacenter

Tamara Crétard - 20.06.2025

Sommaire:

1. Contexte

Dans le cadre du stage de première année du BTS SIO option SISR, effectué au sein de la société Agentil SA à Genève (Suisse), plusieurs missions liées à la gestion de l'infrastructure informatique ont été menées. Ce document présente trois axes majeurs du travail réalisé: le câblage physique du datacenter, la mise à jour des firmwares des serveurs (compute nodes) et la découverte du réseau FortiGate.

Ces activités s'inscrivent dans un contexte de migration et de restructuration du datacenter d'Agentil, visant à améliorer la disponibilité, la sécurité et la maintenabilité de l'infrastructure.

2. Environnement de travail

2.1. Présentation d'Agentil SA

Agentil SA est une société informatique basée en Suisse. Son activité principale consiste à fournir des services d'hébergement et de gestion d'ERP (Enterprise Resource Planning) SAP à ses clients. Elle met à disposition des machines virtuelles (VM) sur lesquelles sont déployés SAP Business One ou SAP S/4HANA, avec une base de données SAP HANA stockant les données à la fois sur disque et en mémoire vive (RAM) pour des accès ultra-rapides.

Configuration de l'environnement	
Société	Agentil SA
Localisation	Genève, Suisse
Activité	Hébergement et gestion d'ERP SAP pour clients entreprise
Hyperviseur	VMware vSphere (ESXi)
Outils principaux	Confluence, Jira, Keeper, Citrix, Zabbix, Agentil IPAM
Sécurité réseau	Firewall Fortinet FortiGate (x2), Switches Fortinet
Stockage	SAN (Storage Area Network), RAID 5+1, PureStorage
Supervision	Zabbix (serveur + 2 proxies), Lenovo XClarity Administrator

2.2. Infrastructure datacenter existante

Au moment du stage, Agentil disposait d'un datacenter en cours de restructuration. L'objectif était de migrer une partie de l'infrastructure vers un nouveau site. Le datacenter comprenait notamment:

- 2 firewalls Fortinet FortiGate
- Des switches Fortinet (intégration native avec les FortiGate)
- Des compute nodes (serveurs physiques) hébergeant les VM via VMware vSphere
- Un système de stockage en SAN avec baies PureStorage
- 2 SAN switches Cisco (fabric) pour la connectivité Fibre Channel

- Un système de supervision Zabbix avec base de données PostgreSQL et TimescaleDB

Note : La ventilation du datacenter avait évolué — les anciens climatiseurs avaient été remplacés par une évacuation d'air par le toit avec ventilateurs et portes ouvertes, point à surveiller pour les températures critiques.

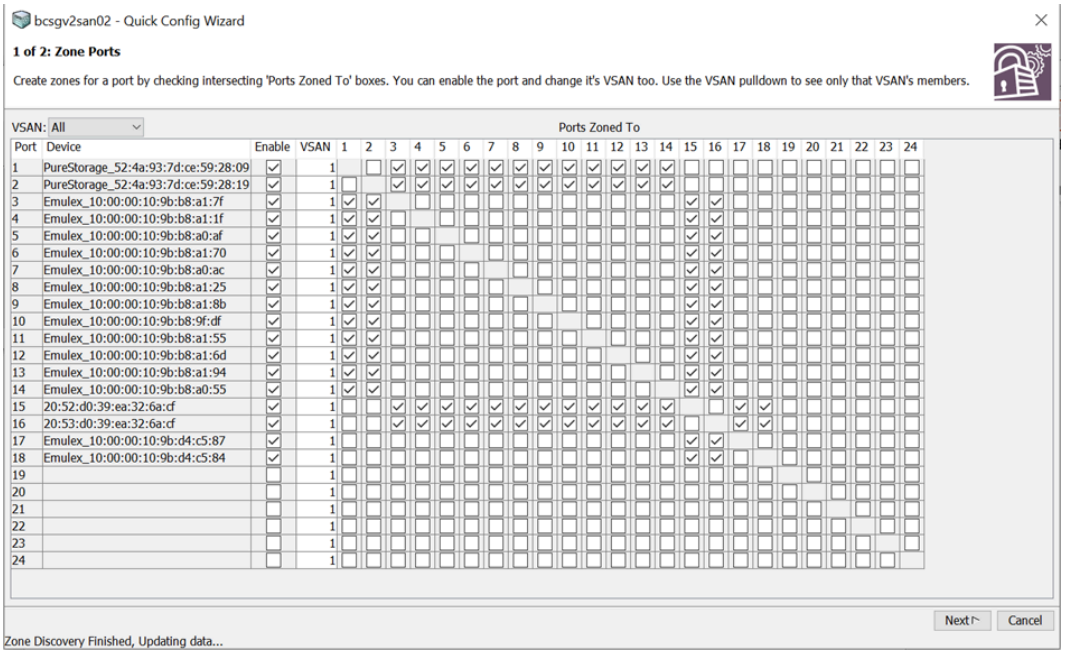

Figure 1 : Configuration du zoning sur le SAN switch Cisco (bcsgv2san02 - Quick Config Wizard)

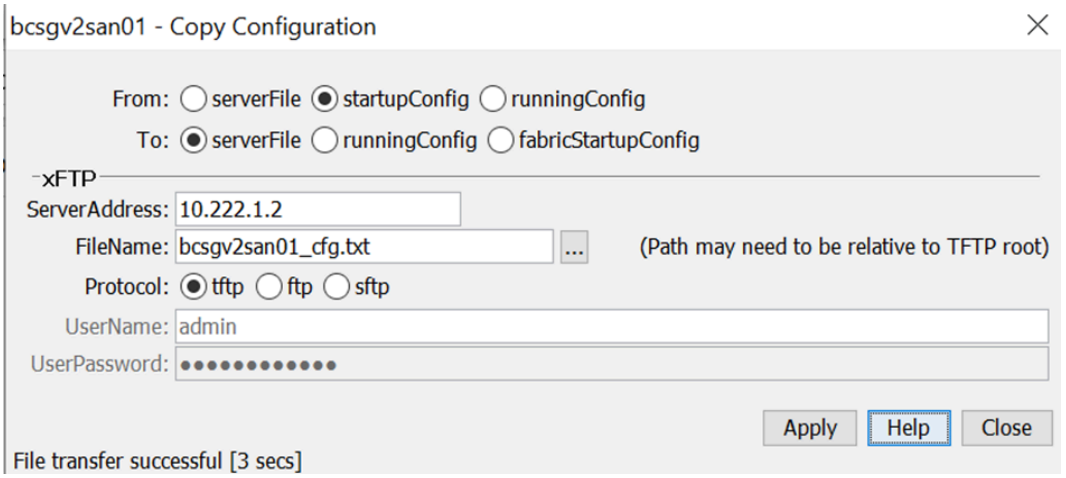

Figure 2 : Sauvegarde de la configuration startup via TFTP (bcsgv2san01 - Copy Configuration)

3. Câblage du datacenter

3.1. Objectif

Une des premières missions confiées consistait à documenter le câblage des deux armoires réseau du datacenter. L'objectif était de créer un tableau recensant, pour chaque câble, la

source (équipement et port) et la destination (équipement et port). Ce travail de documentation est essentiel pour faciliter les interventions futures et assurer la traçabilité des connexions physiques.

3.2. Tableaux de câblage

Les tableaux de câblage ont été réalisé sous Excel. Ils recensent l'ensemble des connexions des deux armoires (racks) du datacenter. Chaque ligne correspond à un câble et indique:

- L'équipement source et son port
- L'équipement de destination et son port
- Des observations éventuelles

Ce tableau constitue un référentiel physique indispensable pour toute opération de maintenance ou d'extension du datacenter. Ils ont été partagés avec l'équipe IT.

AGLGE TELECOM

Équipement source	Port source	Port destination	Équipement destination
AGLGHUB02 - 10.5.9.100	2	4.26	Systimax
	3	4.25	
	4	4.29	
	5	4.82	
	6	4.87	
	7	4.05	
	8	4.102	
	9	4.02	
	10	4.51	
	11	4.53	
	12	4.42	
	13	4.76	
	14	4.14	
	15	4.04	
	17	4.12	
	18	MUR	
	19	MUR	
	20	4.13	Systimax
	21	4.23	
	25	4.16	
	27	4.86	
	28	4.37	
	29	4.38	
	30	4.39	
	31	4.63	
	32	4.18	
	35	4.07	
	36	4.84	
	37	4.4	

Équipement source	Port source	Port destination	Équipement destination
	38	4.27	
	42	4.15	
	43	4.61	
	45	4.59	
	46	4.6	
	47	4.19	
	G50	24	AGLGERTRDGW01 - 10.5.9.254
	Mini GBIC	G51/S3	AGLGEHUB10 - 10.5.9.213
Liaison entre rack	3	1	bas01.gva1768
	4		
AGLGERTRDGW01 - 10.5.9.254	1	1	AGL-NW-0013
	2	1	AGL-NW-0012
	3	23T	AGLGEHUB04
	4	4	aglgefw05
	5	3	AGL-NW-0013
	6	3	AGL-NW-0012
	7	Wifi Hall Aile gauche	
	8	Wifi Central Station APØ2	
	9	4	agfgefw06
	10	Wifi Open Space	
	11	4.06	Systimax
	12	4.07	
	13	4.03	
	14	FingerPrint Sensor	
	15	4.101	Systimax
	16	4.85	
	17	4.83	
	18	4.11	
	19	4.11	
	20	4.01	
	21	3	Box Wifi
	22	4.58	Systimax
	23	4.115	
	24	G50	AGLGEHUB02 - 10.5.9.100
bas01.gva1768	3 (NA-63891)	RJ45 B	
	1	3 & 4	Liaison entre rack
GVA-ET-00204	RJ45 A (GVA/GVA/IA-196497)	6	AGLGEHUB04
	RJ45 B	3 (NA-63891)	bas01.gva1768
AGLGEHUB10 - 10.5.9.213	27		BELKIN
	G51/S3	Mini GBIC	AGLGEHUB02 - 10.5.9.100
AGLGEHUB04	1	1SG	Box Wifi
	3	WAN2	aglgefw05
	5	WAN1	aglgefw06
	6	RJ45 A	GVA-ET-00204
	7	2	aglgefw05

Équipement source	Port source	Port destination	Équipement destination
	15	1	aglgefw05
	16	8	aglgefw05
	19	MGMT	aglgefw06
	23T	3	AGLGERTRDGW01 - 10.5.9.254
	24T	23T	AGLGEHUB05
AGLGEHUB05	1	WAN2	aglgefw06
	5	WAN1	aglgefw05
	7	2	aglgefw06
	12	Ethernet	UPS
	15	1	aglgefw06
	16	8	aglgefw06
	19	MGMT	aglgefw05
	23T	24T	AGLGEHUB04
AGLGEHUB21	25	X1	aglgefw05
	26	X1	aglgefw06
aglgefw06	Console	Pas Branché	
	MGMT	19	AGLGEHUB04
	WAN1	5	
	WAN2	1	AGLGEHUB05
	HA1	HA1	aglgefw05
	HA2	HA2	aglgefw05
	1	15	AGLGEHUB05
	2	7	
	4	9	AGLGERTRDGW01 - 10.5.9.254
	8	16	AGLGEHUB05
	X1	26	AGLGEHUB21
	18	4.107	Systimax
	20	4.113	
aglgefw05	MGMT	19	AGLGEHUB05
	WAN1	5	
	WAN2	3	AGLGEHUB04
	HA1	HA1	aglgefw06
	HA2	HA2	aglgefw06
	1	15	AGLGEHUB04
	2	7	
	4	4	AGLGERTRDGW01 - 10.5.9.254
	8	16	AGLGEHUB04
	X1	25	AGLGEHUB21
	18	4.106	Systimax
	20	4.112	
AGL-NW-0012	3	6	AGLGERTRDGW01 - 10.5.9.254
	2	2	AGL-NW-0013
	1	2	AGLGERTRDGW01 - 10.5.9.254
AGL-NW-0013	3	5	AGLGERTRDGW01 - 10.5.9.254
	2	2	AGL-NW-0012
	1	1	AGLGERTRDGW01 - 10.5.9.254

AGLGE SERVEUR

Équipement source	Port source	Port destination	Équipement destination
LENOVO RACK SWITCH 67052	1	4.112	MUR
	2	4.113	
	3	IMM	BCSaggESXØ1
	4	IMM	
	5	1	BCSaggSTOØ1 - droite
	6	1	BCSaggSTOØ1 - gauche
	13	1	BCSaggESXØ2
	14	1	BCSaggESXØ1
	15	3	BCSaggESXØ2
	16	3	BCSaggESXØ1
	31	4.106	MUR
	32	4.107	
	33	2	BCSaggESXØ1
	34	2	BCSaggESXØ2
	37	Pas Branché	
	38	Pas Branché	
	40	Pas Branché	
	41	Pas Branché	
	42	Pas Branché	
	45	Pas Branché	
	46	Pas Branché	
AGLGEHUB03	1	IMM	ESX09 LAB
	5	4	AGLGESRVESX10
	6	3	
	7	3	ESX09 LAB
	8	1	AGLGESRVESX10
	10	Ethernet	UPS
	11	IMM	AGLGESRVESX08
	12	IMM	AGLGESRVESX10
	13	1	AGLGELABSTO02 - gauche
	14	1	AGLGELABSTO02 - droite
	15	2	AGLGELABSTO02 - gauche
	16	2	AGLGELABSTO02 - droite
	17	3	AGLGESRVESX08
	18	4.115	MUR
	21	4	AGLGESRVESX08
	22	4	ESX09 LAB
	23	1	ALGESRVESX08
	24	1	ESX09 LAB
ESX09 LAB	IMM	1	AGLGEHUB03
	1 (premier)	3	AGLGELABSTO02 - gauche
	1 (deuxième)	3	AGLGELABSTO02 - droite
	1	24	AGLGEHUB03
	3	7	

Équipement source	Port source	Port destination	Équipement destination
	4	22	
AGLGESRVESX08	IMM	11	
	1 (premier)	2	AGLGELABSTO02 - gauche
	1 (deuxième)	2	AGLGELABSTO02 - droite
	1	23	AGLGEHUB03
	3	17	
	4	21	
AGLGESRVESX10	IMM	12	
	1 (premier)	1	AGLGELABSTO02 - gauche
	1 (deuxième)	1	AGLGELABSTO02 - droite
	1	8	AGLGEHUB03
	3	6	
	4	5	
AGLGELABSTO02	1 gauche	13	
	2 gauche	15	
	1 gauche	1 (premier)	AGLGESRVESX10
	2 gauche	1 (premier)	AGLGESRVESX08
	3 gauche	1 (premier)	ESX09 LAB
	1 droite	14	AGLGEHUB03
	2 droite	16	
	1 droite	1 (deuxième)	AGLGESRVESX10
	2 droite	1 (deuxième)	AGLGESRVESX08
	3 droite	1 (deuxième)	ESX09 LAB
BCSaggESXØ2	IMM	3	LENOVO RACK SWITCH
	1	13	
	2	34	
	3	15	
	3 (premier)	2	BCSaggSTOØ1 - gauche
	3 (deuxième)	2	BCSaggSTOØ1 - droite
BCSaggESXØ1	IMM	4	LENOVO RACK SWITCH
	1	14	
	2	33	
	3	16	
	3 (premier)	1	BCSaggSTOØ1 - gauche
	3 (deuxième)	1	BCSaggSTOØ1 - droite
BCSaggSTOØ1	1 gauche	6	LENOVO RACK SWITCH
	1 gauche	3 (premier)	BCSaggESXØ1
	2 gauche	3 (premier)	BCSaggESXØ2
	1 droite	5	LENOVO RACK SWITCH
	1 droite	3 (deuxième)	BCSaggESXØ1
	2 droite	3 (deuxième)	BCSaggESXØ2
UPS	Ethernet	10	AGLGEHUB03
	Settings/Sensor	Pas Branché	

3.3. Connexion des ESXi aux SAN switches

Dans le cadre de la migration vers le nouveau site Equinix, une intervention physique dans le datacenter a été réalisée pour recâbler les serveurs ESXi vers les SAN switches. L'objectif était de connecter les serveurs de virtualisation au réseau de stockage Fibre Channel, en respectant une architecture redondante.

La logique de câblage retenue était la suivante :

- Chaque serveur ESXi possède 2 cartes Fibre Channel (HBA)
- Le port 1 de chaque HBA est connecté au SAN switch 1 (fabric 1)
- Le port 2 de chaque HBA est connecté au SAN switch 2 (fabric 2)
- Les baies de stockage PureStorage sont également connectées aux deux SAN switches pour la redondance

Étape	Description
1	Identifier les ports disponibles sur chaque ESXi et SAN switch à l'aide de Lenovo XClarity Administrator et de la documentation existante.
2	Connecter les câbles fibre optique OM3 entre les HBA des ESXi et les ports des SAN switches, en respectant la séparation fabric 1/fabric 2.
3	Configurer le zoning sur les SAN switches Cisco via Device Manager: créer les zones (une par fabric) en associant les WWN des HBA ESXi aux ports de stockage PureStorage.
4	Vérifier la connectivité: les baies PureStorage se sont reconnectées au SAN sans nécessiter d'arrêt des ESXi (reconnexion en ligne, 2025-06-25).

Point technique : La configuration du zoning a été réalisée dans Device Manager (Cisco SAN switch). Les configurations startup ont été sauvegardées via TFTP vers un serveur local (Tftpd64) pour permettre une restauration rapide en cas d'incident.

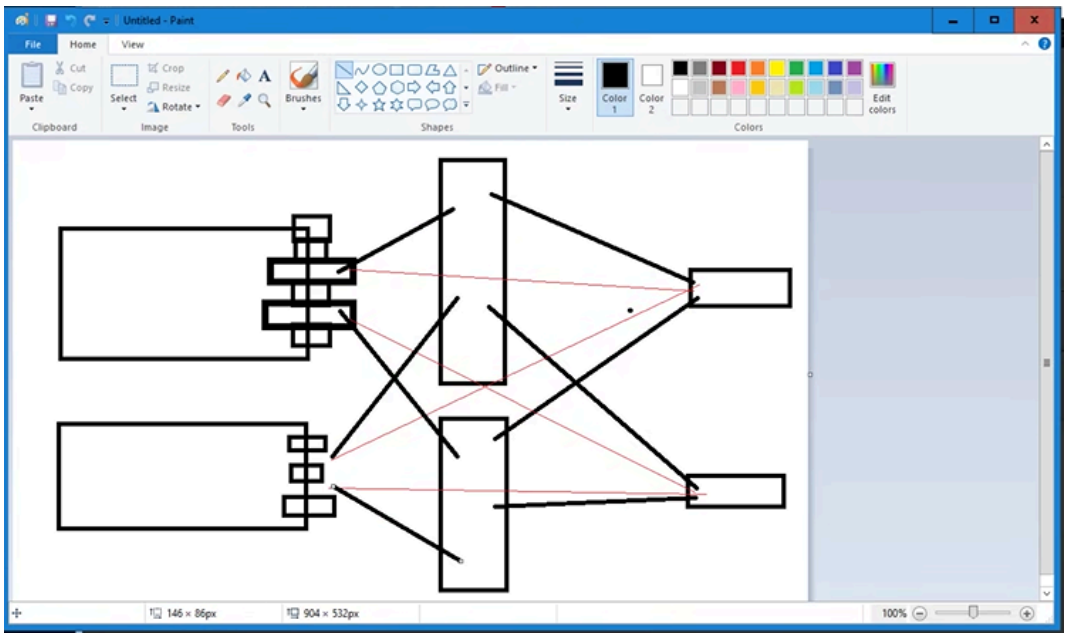

Figure 3 — Schéma de câblage des ESXi vers les SAN switches (deux fabrics)

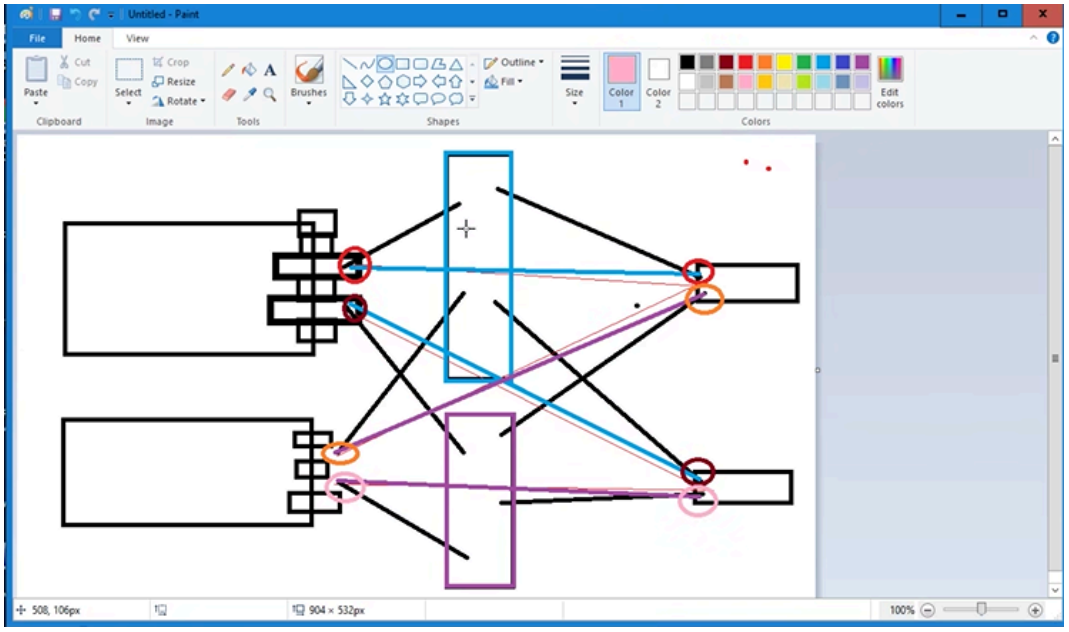

Figure 4 — Schéma de zoning : fabric 1 (bleu) et fabric 2 (violet)

4. Mise à jour des firmwares des noeuds BCS

4.1. Outil utilisé : Lenovo XClarity Administrator

Les serveurs physiques (compute nodes) du datacenter BCS sont des serveurs Lenovo. Leur gestion centralisée, incluant la mise à jour des firmwares, est assurée via Lenovo XClarity Administrator (LXCA), une interface web qui permet de superviser et provisionner l'ensemble du parc serveur.

Caractéristiques de l'outil	
Outil	Lenovo XClarity Administrator (LXCA)
Accès	Interface web — https://[ip-lxca]
Serveurs gérés	19 serveurs (compute nodes BCS)
Fonction principale	Inventaire, supervision, provisioning, mise à jour firmware
Données visibles	CPU, RAM, disques, cartes réseau, firmwares installés, alertes

XClarity Administrator permet notamment de consulter, pour chaque serveur, les firmwares actuellement installés (BIOS, BMC, cartes réseau, HBA) et de les comparer aux versions disponibles dans le catalogue officiel Lenovo.

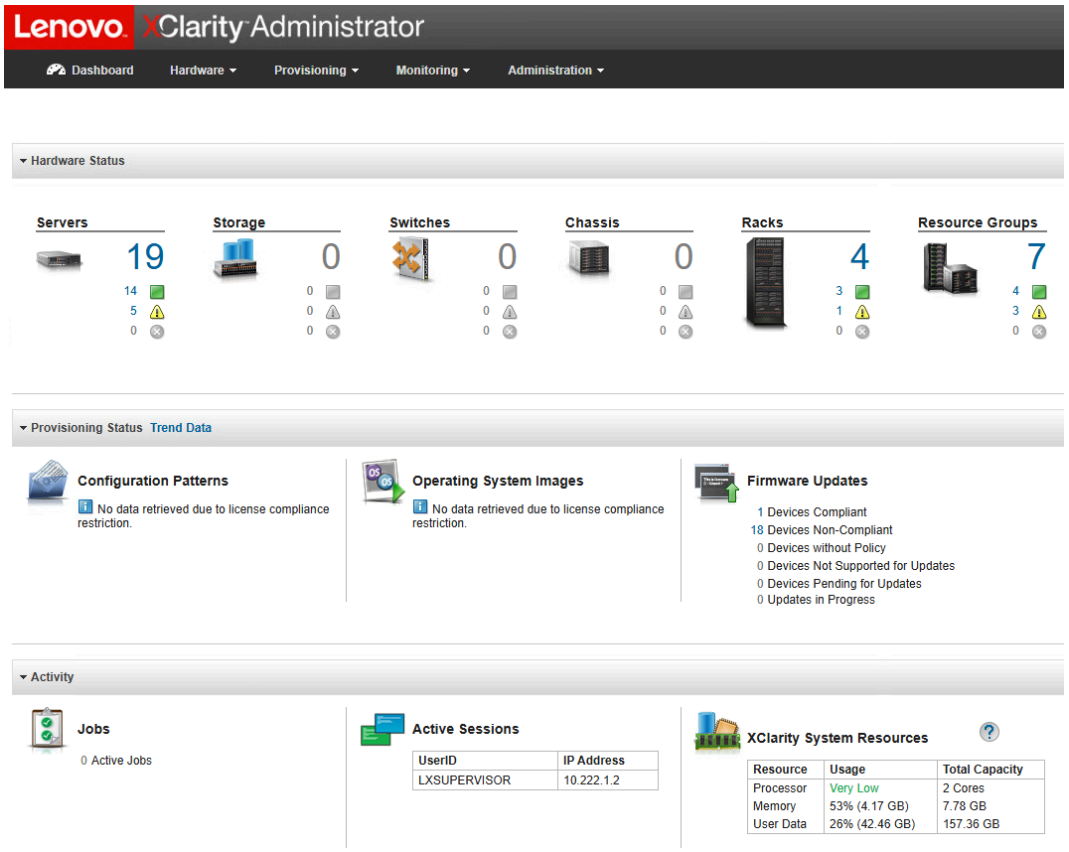

Figure 5 — Dashboard Lenovo XClarity Administrator : vue globale du parc (19 serveurs)

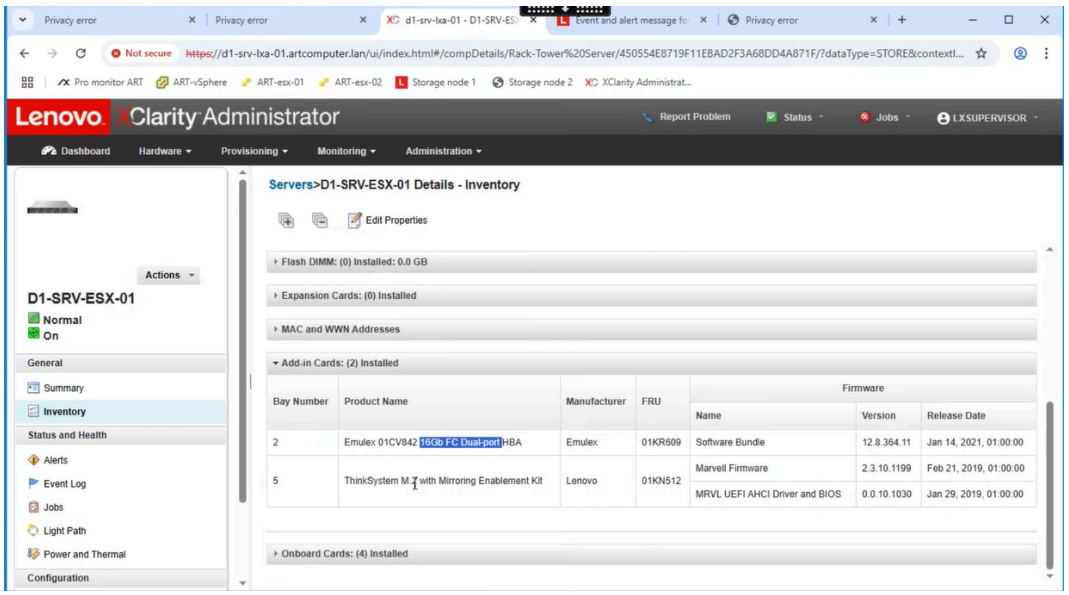

Figure 6 — XClarity : inventaire du serveur D1-SRV-ESX-01 (cartes HBA Emulex 16Gb FC)

4.2. Procédure de mise à jour des firmwares

La mise à jour des firmwares suit une procédure précise pour éviter toute interruption de service non planifiée. Les serveurs BCS hébergent des VM de production: il est donc impératif de coordonner les mises à jour avec l'équipe (libération de l'ESXi concerné par Philippe avant intervention).

Étape	Description
1	**Rafraîchir le repository et le catalogue** Dans LXCA : Provisioning > Firmware Updates > Repository. Cliquer sur « Refresh Repository » puis « Refresh Catalog ». Sélectionner « Managed machine types only » pour limiter les résultats.
2	**Identifier les firmwares disponibles** Les éléments non encore téléchargés apparaissent dans la liste. Sélectionner les firmwares les plus récents pour chaque serveur et les télécharger dans le repository local.
3	**Vérifier l'inventaire serveur** Dans Hardware > Servers, consulter la fiche de chaque serveur (onglet Inventory) pour voir les firmwares actuels (BIOS, BMC, cartes réseau). XClarity indique également l'état de conformité (Compliant / Non-Compliant).
4	**Appliquer les mises à jour (Provisioning > Apply/Activate)** Sélectionner le serveur à mettre à jour (après confirmation que l'ESXi est libre). Choisir les firmwares à appliquer et lancer le déploiement. Un redémarrage du serveur peut être nécessaire selon le composant mis à jour.

Remarque : Pour les serveurs Lenovo vendus aux clients (PC de travail), la procédure de mise à jour firmware passait par le logiciel Lenovo System Update, disponible sur le site support.lenovo.com. Les firmwares étaient téléchargés manuellement puis installés.

5. Réseau FortiGate

5.1. Architecture firewall

L'infrastructure réseau d'Agentil repose sur des équipements Fortinet: deux firewalls FortiGate et des switches Fortinet. L'homogénéité du parc présente un avantage opérationnel majeur : lorsqu'une règle ou une configuration est modifiée sur un FortiGate, les switches Fortinet associés se mettent automatiquement à jour.

Les firewalls FortiGate utilisés sont des firewalls dits « explicites »: toute communication doit être explicitement autorisée par une règle. Par défaut, tout trafic non couvert par une règle est bloqué. Cette approche est opposée aux firewalls « implicites » où tout est autorisé par défaut.

Architecture FortiGate	
Type de firewall	FortiGate (Fortinet) — mode explicite (deny all par défaut)
Nombre de firewalls	2 (haute disponibilité)
Interface de gestion	Interface web FortiGate (GUI centralisée)
Gestion des adresses IP	Agentil IPAM (gestion des plages IP, DNS, Gateway)
VPN supportés	Tunnels IPSec permanents + SSL VPN (type FortiClient)
Intégration switches	Switches Fortinet — mise à jour automatique lors des changements FortiGate

5.2. Création de VLANs et règles de filtrage

La création d'un VLAN et des règles associées suit une procédure structurée, passant d'abord par l'outil IPAM pour la validation de l'adressage, puis par la configuration du FortiGate.

Étape	**Description**
1	**Déclarer le VLAN dans Agentil IPAM** Avant toute configuration réseau, le VLAN est créé dans IPAM avec son plan d'adressage (réseau, masque, gateway, DNS). IPAM détecte les conflits d'adresses et valide la cohérence.
2	**Créer l'interface VLAN sur le FortiGate**

	Dans l'interface web FortiGate, sélectionner le firewall concerné et créer une nouvelle interface VLAN avec le tag VLAN ID correspondant et l'adresse IP de gateway.
3	**Créer les règles de filtrage (Firewall Policies)** Pour chaque flux autorisé, créer une règle avec : nom, interface entrante, interface sortante, source (IP ou groupe), destination, services (ports : HTTPS, FTP, etc.), action (accepter/refuser), et configuration du NAT.

Concernant le NAT: pour un flux interne vers interne (trafic entre VLANs internes), le NAT est désactivé. Le NAT n'est activé que pour les flux sortant vers Internet ou des réseaux externes.

5.3. Tunnels VPN

L'infrastructure d'Agentil utilise deux types de VPN pour connecter les différents sites et permettre l'accès distant des utilisateurs :

Types de VPN utilisés	
VPN IPSec (tunnel permanent)	Connexion site-à-site permanente entre les infrastructures Agentil (ex : liaison entre BCS et AGLCH). Le tunnel est établi automatiquement et maintenu en permanence.
SSL VPN (FortiClient)	Accès distant des utilisateurs et collaborateurs. Similaire à un VPN client classique. L'interface entrante des règles firewall associées est de type « tunnel SSL VPN ».

Observation : De nombreuses règles de filtrage avaient comme interface entrante un tunnel SSL VPN vers une autre interface interne, permettant aux utilisateurs distants d'accéder aux ressources internes via le VPN, avec filtrage granulaire des flux autorisés.