PAGE DE GARDE DU DOSSIER PROFESSIONNEL

BREVET DE TECHNICIEN SUPÉRIEUR SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2026

DOSSIER PROFESSIONNEL

NOM : CHAUVEL

Prénom : Corentin

Établissement de formation (sur un seul des deux exemplaires du dossier)

Visa du représentant de l'équipe pédagogique attestant la réalité des activités professionnelles décrites dans le dossier (sur un seul des deux exemplaires du dossier) :

Nom et qualité du signataire	Date	Signature

Attestation sur l'honneur pour les candidats individuels (sur un seul des deux exemplaires du dossier) :

Je soussigné(e), CHAUVEL , Corentin , certifie que les activités décrites ainsi que les différentes informations reproduites dans ce dossier reflètent les activités professionnelles que j'ai personnellement réalisées au cours de ma formation.

Fait à Bouguenais
Date 22/04/2026

Signature

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
Nom, prénom : CHAUVEL Corentin	**N° candidat : 02542581385**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 29 / 05 /2026

Organisation support de la réalisation professionnelle
Entreprise fictive **Oasis** et prestataire **NTxSystem**

Intitulé de la réalisation professionnelle
Mise en place de la supervision avec Centreon

Période de réalisation : 2024 – 2026 Lieu : CFA Fab'Academy Bouguenais (UIMM)
Modalité : ☐ *Seul(e)* ☒ *En équipe*

Compétences travaillées
- ☒ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)
Mise en place d'une solution de Supervision et monitoring de l'infrastructure. Afin de répondre aux exigences de OASIS. La solution doit permettre d'assurer la supervision de l'infrastructures virtualisées et sécurisées, de services essentiels.

Description des ressources documentaires, matérielles et logicielles utilisées[2]
Différentes ressources ont été utilisées pour la mise en place de la solution de sauvegarde, tout d'abord pour les ressources documentaires, la ressource principale utilisée a été la documentation officielle de Centreon, pour les ressources matérielles, un Serveur HP en tant qu'hyperviseur, pour les ressources logicielles, ESXI VMware, Centreon.

Modalités d'accès aux productions[3] et à leur documentation[4]
L'ensemble des documents liés à l'infrastructure est disponible sur le partage réseau accessible depuis le réseau BTS SIO. Cet emplacement est dédié au stockage des informations relatives à la section. Il contient notamment des documentations sur l'environnement virtuel déployé, l'ensemble de la configuration de l'infrastructure mise en place, les différentes solutions étudiées, le plan d'adressage ainsi que les différents schémas réalisés de l'infrastructure. L'ensemble des mots de passe de l'infrastructure sont conservés dans notre gestionnaire de mot de passe Bitwarden.

Partage Réseau Documentation NTxSystem : \\partage.btssio.nte\fichiers\BAIES-PEDA\NTXSYSTEM

Identifiant Bitwarden : ntxsystem@proton.me
Mot de passe Bitwarden : NTxbitwarden44.
Lien Bitwarden : https://vault.bitwarden.com

---

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

Fiche descriptive de réalisation professionnelle
(verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

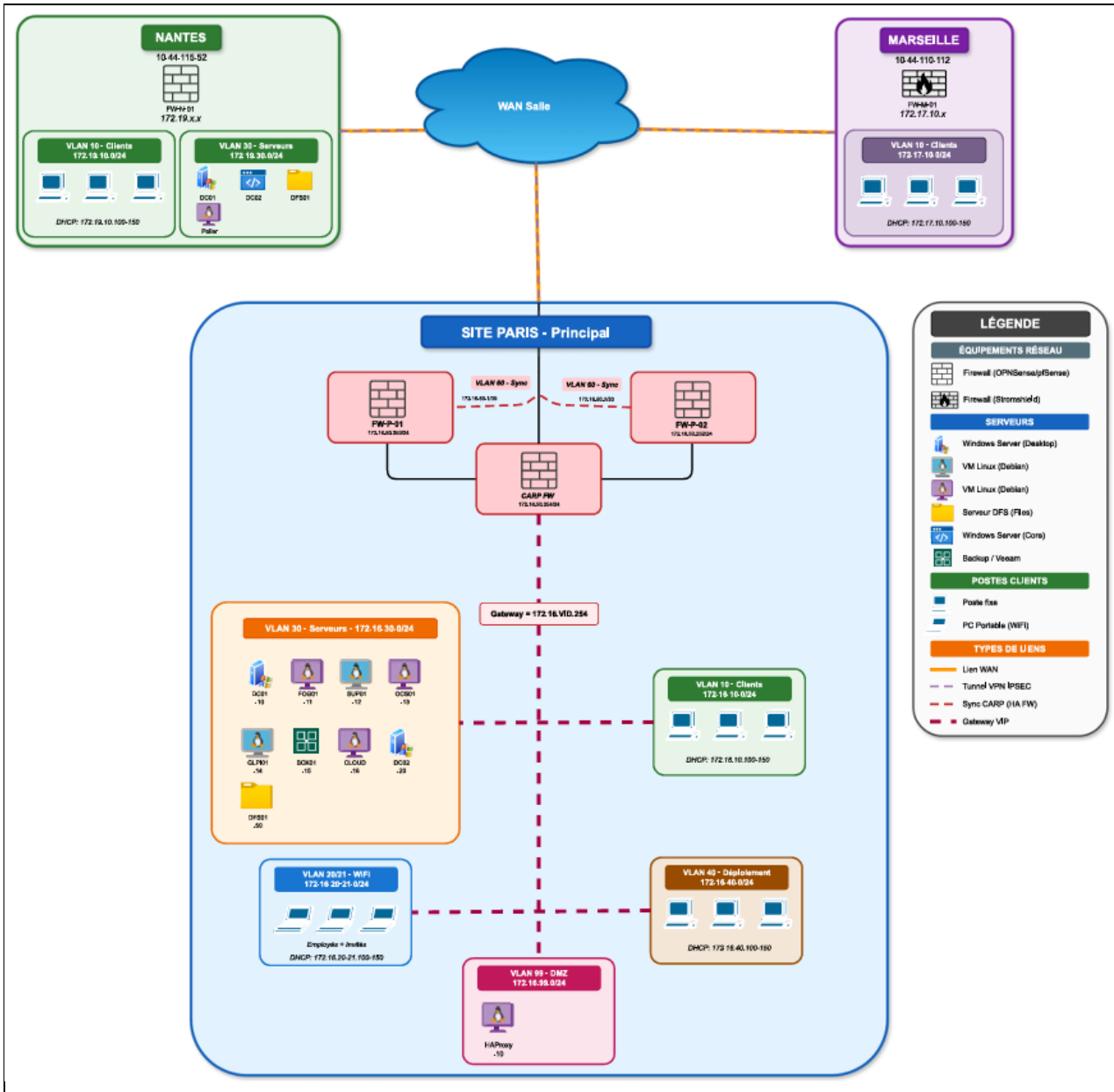
A travers cette réalisation professionnelle portant sur la supervision, différents outils ont été monté au sein de l'infrastructure, tout l'environnement est virtualisé sur deux serveurs HP utilisant VMware ESXI et il y a différentes machines virtuelles dédiées à différents services.

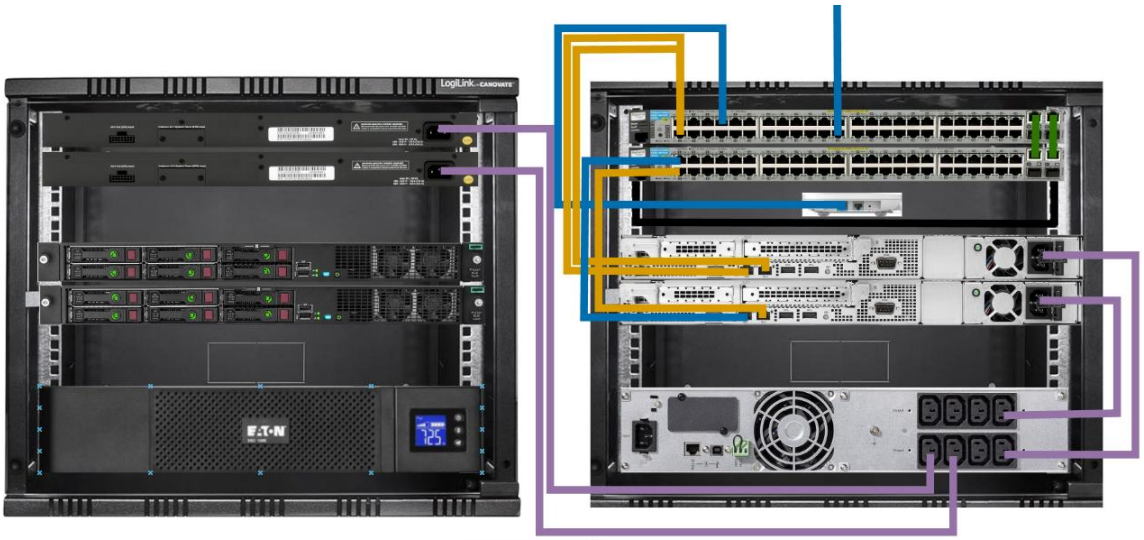
Cette infrastructure a été construire sur trois sites, le premier correspondant au site commun au groupe NTxSystem, le site de paris, le second le site de Marseille et le dernier le site de Nantes.

L'objectif était de mettre en place une solution de supervision centralisée permettant de surveiller l'ensemble des équipements, services et infrastructures répartis sur ces différents sites. Grâce à Centreon, il est possible de suivre en temps réel l'état des systèmes, de détecter rapidement les anomalies.

Cette solution s'appuie sur la configuration de contrôles réguliers, la gestion des seuils d'alerte et la centralisation des données de supervision. Elle permet ainsi d'améliorer la visibilité sur l'infrastructure, d'optimiser les interventions et de garantir une meilleure disponibilité des services.

Ci-dessous les schémas logique et physique ainsi que le plan d'adressage de l'infrastructure.





Pour plus de détails, les deux schémas montrant l'ensemble de l'infrastructure peuvent être trouvés en Annexe n°4 pour le schéma logique et schéma physique.

Paris :

VLAN 10

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.10.252	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-01 VLAN 10
FW-P-01	172.16.10.253	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-02 VLAN 10
CARP Firewall	172.16.10.254	255.255.255.0	172.16.10.0	172.16.10.254	Passerelle du VLAN 10

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.10.100-150	172.16.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Paris

VLAN 20

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
B-P-WIFI	172.16.20.50	255.255.255.0	172.16.20.0	172.16.20.254	Administration borne Wifi
FW-P-02	172.16.20.252	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-02 VLAN 20
FW-P-01	172.16.20.253	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-01 VLAN 20
CARP Firewall	172.16.20.254	255.255.255.0	172.16.20.0	172.16.20.254	Passerelle du VLAN 20

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.20.100-150	172.16.20.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Employés

VLAN 21

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.21.252	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-02 VLAN 21
FW-P-01	172.16.21.253	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-01 VLAN 21
CARP Firewall	172.16.21.254	255.255.255.0	172.16.21.0	172.16.21.254	Passerelle du VLAN 21

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.21.100-150	172.16.21.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Invité

VLAN 30

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-DC01	172.16.30.10	255.255.255.0	172.16.30.0	172.16.30.254	DC 1
SRV-P-DC02	172.16.30.20	255.255.255.0	172.16.30.0	172.16.30.254	DC 2
SRV-P-DFS01	172.16.30.50	255.255.255.0	172.16.30.0	172.16.30.254	DFS01
SRV-P-FOG01	172.16.30.11	255.255.255.0	172.16.30.0	172.16.30.254	Fog
SRV-P-OCS01	172.16.30.13	255.255.255.0	172.16.30.0	172.16.30.254	OCS Inventory
SRV-P-GLPI01	172.16.30.14	255.255.255.0	172.16.30.0	172.16.30.254	GLPI
SRV-P-BCK01	172.16.30.15	255.255.255.0	172.16.30.0	172.16.30.254	Veeam
SRV-P-CLOUD01	172.16.30.16	255.255.255.0	172.16.30.0	172.16.30.254	Nextcloud
SRV-P-RSAT-T0	172.16.30.30	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T0
SRV-P-RSAT-T1	172.16.30.31	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T1
SRV-P-RSAT-T2	172.16.30.32	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T2
SRV-P-EDR01	172.16.30.19	255.255.255.0	172.16.30.0	172.16.30.254	EDR
SRV-P-ANS01	172.16.30.21	255.255.255.0	172.16.30.0	172.16.30.254	Ansible Lille
SRV-P-NETBOX01	172.16.30.22	255.255.255.0	172.16.30.0	172.16.30.254	Outil d'infrastructure
SRV-P-POL01	172.16.30.25	255.255.255.0	172.16.30.0	172.16.30.254	Centreon Poller
FW-P-02	172.16.30.252	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-02 VLAN 30
FW-P-01	172.16.30.253	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-01 VLAN 30
CARP Firewall	172.16.30.254	255.255.255.0	172.16.30.0	172.16.30.254	Passerelle du VLAN 30

VLAN 40

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.40.252	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-02 VLAN 40
FW-P-01	172.16.40.253	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-01 VLAN 40
CARP Firewall	172.16.40.254	255.255.255.0	172.16.40.0	172.16.40.254	Passerelle du VLAN 40

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.40.100-150	172.16.40.254	172.16.30.10	172.16.30.20	Plage DHCP Déploiement

VLAN 50

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SW-P-01	172.16.50.1	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 1 Paris
SW-P-02	172.16.50.2	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 2 Paris
SRV-P-ESXI01	172.16.50.10	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
SRV-P-ESXI02	172.16.50.20	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
PAW-P-T0	172.16.50.50	255.255.255.0	172.16.50.0	172.16.50.254	Machine d'administration
FW-P-02	172.16.50.252	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-02 VLAN 50
FW-P-01	172.16.50.253	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-01 VLAN 50
CARP Firewall	172.16.50.254	255.255.255.0	172.16.50.0	172.16.50.254	Passerelle du VLAN 50

VLAN 60

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-01	172.16.60.1	255.255.255.252	172.16.60.0	-	IP FW-P-01 VLAN 60
FW-P-02	172.16.60.2	255.255.255.252	172.16.60.0	-	IP FW-P-02 VLAN 60

VLAN 99

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-HAProxy	172.16.99.10	255.255.255.0	172.16.99.0	172.16.99.254	HAProxy
FW-P-02	172.16.99.252	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-02 VLAN 99
FW-P-01	172.16.99.253	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-01 VLAN 99
CARP Firewall	172.16.99.254	255.255.255.0	172.16.99.0	172.16.99.254	Passerelle du VLAN 99

Marseille :

Marseille

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-M-01	172.17.10.254	255.255.255.0	172.17.10.0	172.17.10.254	IP FW-M-01 VLAN 10 Marseille
FW-M-01	10.44.110.112	255.255.255.0	10.44.110.0	10.44.110.254	IP WAN Marseille

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.17.10.100-150	172.17.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Marseille

Nantes :

Nantes

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-N-DC01	172.19.30.10	255.255.255.0	172.19.30.0	172.19.30.254	DC1 Nantes
SRV-N-DC02	172.19.30.11	255.255.255.0	172.19.30.0	172.19.30.254	DC2 Core Nantes
SRV-N-SUP01	172.19.30.12	255.255.255.0	172.19.30.0	172.19.30.254	Centreon Central
SRV-N-POL01	172.19.30.25	255.255.255.0	172.19.30.0	172.19.30.254	Centreon Poller
FW-N-01	172.19.10.254	255.255.255.0	172.19.10.0	172.19.10.254	IP FW-N-01 NAN Nantes
FW-N-01	172.19.30.254	255.255.255.0	172.19.30.0	172.19.30.254	IP FW-N-01 SRV Nantes
FW-N-01	172.19.99.254	255.255.255.0	172.19.99.0	172.19.99.254	IP FW-N-01 DMZ Nantes
FW-N-01	10.44.115.52	255.255.255.0	10.44.115.0	10.44.115.254	IP WAN Nantes

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.19.10.100-150	172.19.10.254	172.19.30.10	172.19.30.20	Plage DHCP Client Nantes

BTS Services informatiques aux organisations SESSION 2026
ANNEXE 10-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate
Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE
En référence à l'annexe II.E – « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification[5]	Fab'Academy, 9 Rue de l'Halbrane, 44340 Bouguenais	**SISR**

1. Environnement commun aux deux options
1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un service d'authentification	**Active Directory Windows**	
Un SGBD	**MySQL / MariaDB**	
Un accès sécurisé à internet	**Firewall OPNsense**	
Un environnement de travail collaboratif	**Nextcloud**	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	**GLPI (Debian), Windows Server 2022**	

[5] Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution de sauvegarde	Veeam B&R	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Nextcloud, DFS/R	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	Tablette / PC Portable via connexion Wifi	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Gestion des incidents	GLPI	
Détection et prévention des intrusions	Wazuh, Stormshield	
Chiffrement	TLS, IPsec, SSH, PKI	
Analyse de trafic	Wireshark	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : « *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un réseau comportant plusieurs périmètres de sécurité	Segmentation VLANs via Switch	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Partage Réseau avec droits d'accès via DFS/R suivant méthode AGDLP	
Un logiciel d'analyse de trames	Wireshark	
Un logiciel de gestion des configurations	Ansible, GPO	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	SSH, RDP, HTTPS	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Centreon	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Firewall OPNsense, HaProxy, VPN	

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution garantissant la continuité d'un service	**Veeam B&R, Haute disponibilité OPNsense**	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	**RAID 1, redondance switch et Firewall OPNsense**	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	**DFS/R , DHCP, DNS, Firewall OPNsense**	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	**VPN IPsec**	
Une solution permettant le déploiement des solutions techniques d'accès	**FOG, Ansible**	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	**Ansible, Batch GPO**	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	**Stormshield IPS, Wazuh**	

Table des matières

1. Introduction

Dans le cadre de ma formation en BTS SIO, j'ai eu l'opportunité d'intervenir sur un projet de mise en place d'une solution de supervision pour l'entreprise Oasis.

Ce projet consiste à accompagner Oasis dans la surveillance et le suivi de son infrastructure informatique, afin de garantir le bon fonctionnement des équipements et des services sur l'ensemble de ses sites. L'objectif est de mettre en place une supervision centralisée permettant de détecter rapidement les anomalies et d'assurer une réactivité optimale en cas d'incident.

Pour répondre à ces besoins, j'ai été amené à déployer une solution de supervision basée sur Centreon. Cette solution permet de superviser les différents équipements (serveurs, équipements réseau, bornes Wi-Fi) et de centraliser les informations, tout en assurant une remontée d'alertes en temps réel afin de garantir la disponibilité et la performance du système d'information.

2. Présentation de l'entreprise NTxSYSTEM

NTxSystem est une entreprise prestataire spécialisée dans les solutions informatiques pour les professionnels. Dans le cadre de l'expansion d'Oasis, NTxSystem a été chargé de concevoir et déployer l'ensemble de l'infrastructure réseau des agences de Paris et Marseille.

Les enjeux de ce projet sont multiples : centralisation des services, virtualisation des ressources, gestion des utilisateurs, sécurisation des communications inter-sites et mise en place d'un environnement stable et évolutif.

Pour répondre aux différentes exigences d'Oasis, l'ensemble de l'infrastructure est déployé dans un environnement virtualisé VMware ESXi.

3. Présentation de l'entreprise OASIS

L'entreprise Oasis est une société parisienne spécialisée dans la conception de voyages sur mesure pour une clientèle exigeante, à la recherche d'expériences uniques, loin des circuits touristiques classiques.

Créé en 2017, elle s'est rapidement imposée comme un acteur innovant dans le secteur du tourisme personnalisé, grâce à une approche centrée sur l'écoute client, la

connaissance culturelle approfondie des destinations, et un réseau de partenaires locaux dans plus de 30 pays.

Après plusieurs années de forte croissance, Oasis a décidé d'ouvrir une nouvelle agence à Marseille, pour mieux couvrir le sud de la France et répondre à une demande croissante dans cette zone. L'agence parisienne reste le siège social et le cœur de la stratégie de conception et de relation client haut de gamme.

En 2024, Oasis a atteint un chiffre d'affaires de 2,3 millions d'euros, et ambitionne désormais de renforcer sa structure numérique afin d'améliorer la coordination entre les sites, la sécurité des données clients, et la fluidité de l'expérience interne.

C'est dans ce contexte de croissance que NTxSystem a été sollicitée pour concevoir et déployer une infrastructure informatique adaptée aux besoins d'Oasis que ce soit pour l'agence parisienne, le siège social ou pour l'agence de Marseille

4. Projet Supervision

4.1. Contexte du projet

Dans le cadre de la mission pour Oasis, nous intervenons en tant que prestataire informatique pour accompagner l'entreprise dans la conception et la mise en place de son infrastructure. La direction technique attend une centralisation des services, la virtualisation des ressources, la gestion des utilisateurs, la communication inter-sites, ainsi qu'un environnement stable, évolutif et sécurisé, d'abord testé dans un environnement isolé avant déploiement réel.

L'infrastructure d'Oasis est répartie sur plusieurs sites géographiques : Paris (site principal), Marseille et Nantes. Elle comprend :

- Plusieurs machines virtuelles (VM)
- Des switches HP
- Une borne Wi-Fi
- Des équipements réseau interconnectés entre les sites

L'entreprise dispose désormais :

- D'infrastructures virtualisées et sécurisées
- De services essentiels tels que l'authentification, le partage de fichiers, la sauvegarde, le VPN et le Wi-Fi
- D'une redondance réseau garantissant la haute disponibilité

Avec l'augmentation du nombre d'équipements et de services hébergés, ainsi que la complexité croissante du système d'information, le suivi manuel de l'état des serveurs,

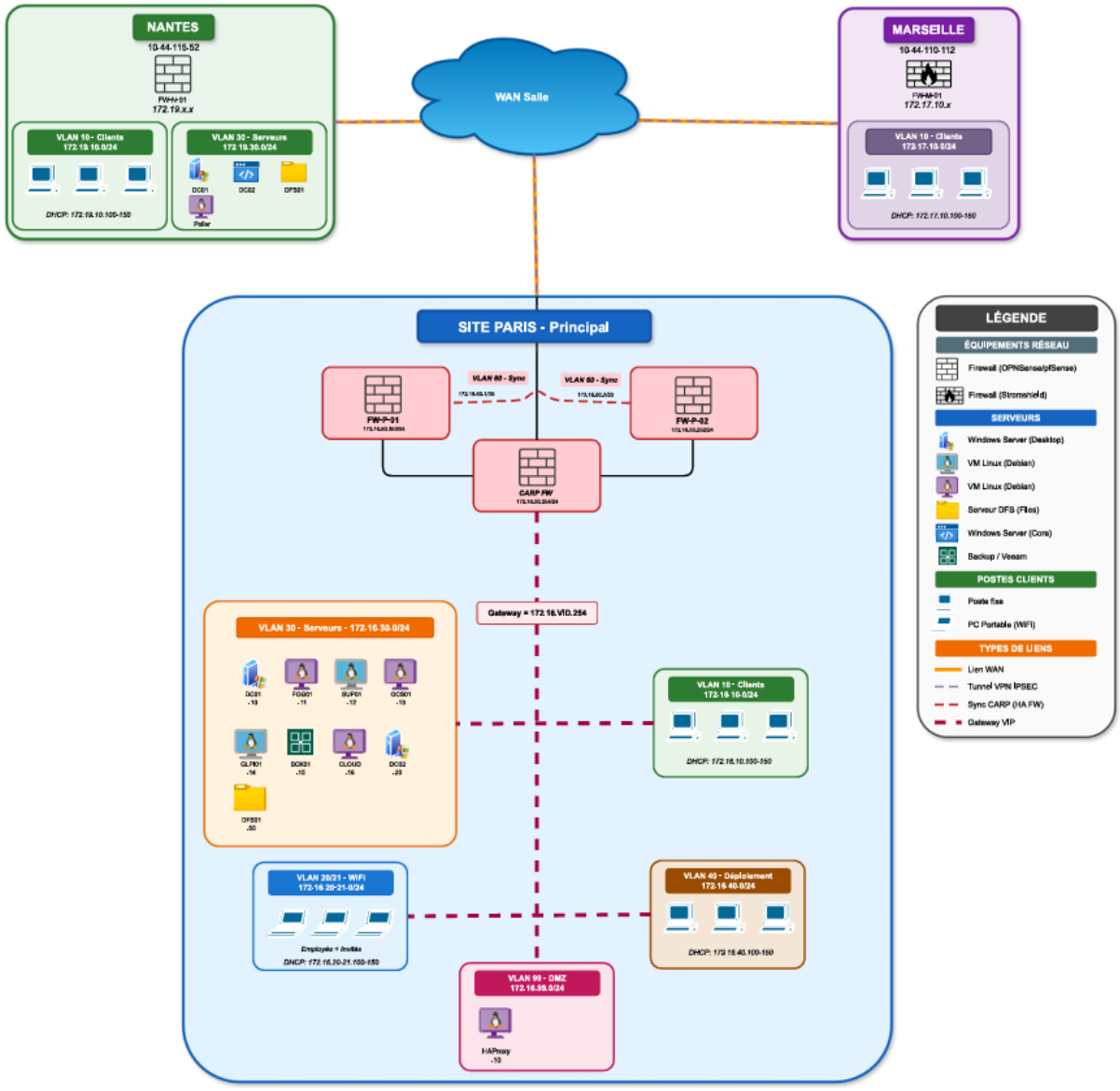
des équipements et des services devient difficile. Il devient donc indispensable de mettre en place une solution de supervision centralisée. Cette solution doit permettre :

- La surveillance en temps réel des éléments critiques de l'infrastructure
- La détection automatique des anomalies
- L'alerte immédiate des équipes techniques en cas d'incident
- Un pilotage global de la maquette Oasis incluant les deux agences

Cette supervision doit être préventive, sécurisée et évolutive, afin de garantir la continuité des services en cas de panne ou d'attaque, et d'assurer une visibilité complète sur l'ensemble de l'infrastructure avant tout déploiement réel.

4.2. Schéma du réseau d'OASIS

Voici le schéma :



4.2.1. Couche la plus haute : Réseau WAN

La couche supérieure représente le réseau WAN (Wide Area Network), qui interconnecte les différents sites géographiques : Paris (site principal), Nantes et Marseille.

Les lignes orange représentent donc le réseau WAN principal.

4.2.2. Les sites distants

- Nantes
- Marseille

Le site de Nantes est autonome en ce qui concerne l'accès à Internet ainsi que les services AD, DHCP et DNS.

4.2.3. Les tunnels VPN / synchronisation inter-sites

Les lignes violettes pointillées représentent : VPN Site-to-Site

Ces tunnels servent à connecter tous les sites au site principal.

4.2.4. Site principale Paris

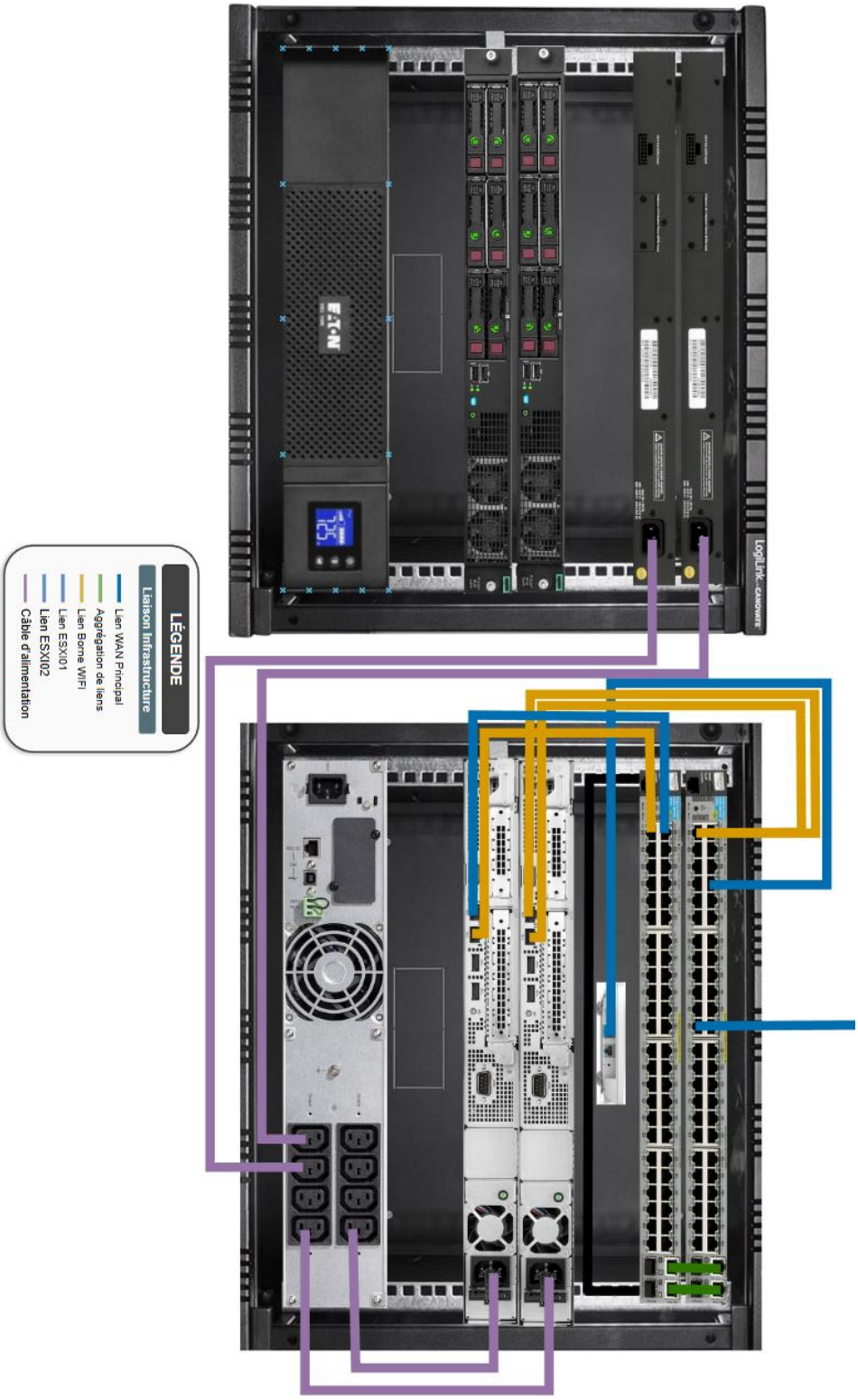
Un cluster de firewall pour avoir de la haute disponibilité, ils sont reliés avec le VLAN 50-Sync. Ce VLAN sert à la synchronisation des firewalls, l'état des sessions, réplication de configuration.

4.2.5. Segmentation réseau par VLAN

VLAN séparés pour :

- CLIENTS
- WIFI
- WIFI CLIENTS
- SERVEUR
- DEPLOIEMENT
- ADMIN
- DMZ
- SYNC
- NATIF

4.3. Schéma Physique du site Paris



4.4. Etude de Faisabilité

4.4.1. Analyse des besoins

Les besoins identifiés sont donc les suivants :

- Superviser l'ensemble des équipements réseau (switches, borne Wi-Fi).
- Surveiller les performances des machines virtuelles (CPU, RAM, stockage).
- Contrôler la disponibilité des services critiques.
- Recevoir des alertes automatiques en cas de panne ou dépassement de seuil.
- Disposer d'une vision centralisée et en temps réel de l'infrastructure.
- Mettre en place une solution adaptée à un environnement multi-sites.

4.4.2. Étude des solutions

4.4.2.1. Solution 1 : Centreon

Centreon est une solution de supervision créée en 2005. Elle permet de superviser les infrastructures réseau, les serveurs et les services applicatifs.

Il s'agit d'une solution Open Source sous licence GNU GPL. Toutefois, l'éditeur propose également des extensions commerciales offrant des fonctionnalités avancées ainsi qu'un support professionnel.

Centreon repose historiquement sur le moteur de supervision Nagios, reconnu pour sa robustesse et sa fiabilité. L'outil propose une interface web moderne et intuitive facilitant la configuration et la visualisation des équipements supervisés.

Son architecture distribuée, basée sur un serveur central et des pollers distants, constitue un atout majeur dans le cadre d'une infrastructure multi-sites. Les pollers permettent d'effectuer les contrôles localement et de remonter les informations vers le serveur central.

Centreon offre également une bonne compatibilité avec le protocole SNMP, ce qui le rend particulièrement adapté à la supervision des switches HP et de la borne Wi-Fi présents dans l'infrastructure.

Cependant, sa mise en place nécessite des compétences techniques, notamment en environnement Linux, et certaines fonctionnalités avancées peuvent être payantes.

4.4.2.2. Solution 2 : Zabbix

Zabbix est une solution de supervision Open Source créée en 2001. Elle permet de superviser les réseaux, les serveurs, les environnements cloud ainsi que divers services applicatifs.

L’outil dispose d’un moteur intégré et d’une interface web complète permettant la configuration, la visualisation et la gestion des alertes. Zabbix est particulièrement reconnu pour son système de déclencheurs (triggers), qui permet d’envoyer des notifications automatiques en cas de dépassement de seuil ou de détection d’une panne.

Il prend en charge les agents installés sur les serveurs ainsi que la supervision via SNMP pour les équipements réseau.

Toutefois, dans un contexte multi-sites, la mise en place d’une architecture distribuée peut être plus complexe. De plus, sur des infrastructures importantes, l’outil peut devenir plus exigeant en ressources système. Sa configuration avancée peut également représenter une courbe d’apprentissage importante.

4.4.2.3. Solution 3 : Prometheus

Prometheus est une solution Open Source créée en 2012. Elle est principalement utilisée dans les environnements modernes orientés DevOps et cloud natif.

Elle est fortement intégrée avec Kubernetes et s’appuie généralement sur Grafana pour l’affichage des tableaux de bord.

Prometheus fonctionne principalement sur un système de collecte de métriques et de séries temporelles. Elle est très performante dans les environnements conteneurisés et les architectures microservices.

Cependant, dans le cadre d’une infrastructure classique composée de machines virtuelles, switches et bornes Wi-Fi, Prometheus est moins adapté. Il ne propose pas nativement certaines fonctionnalités d’actions automatiques ou de gestion d’événements avancée comme Centreon ou Zabbix. De plus, son utilisation nécessite une approche plus orientée développement et automatisation.

4.4.3. Synthèse des solutions

EF : Synthèse des solutions

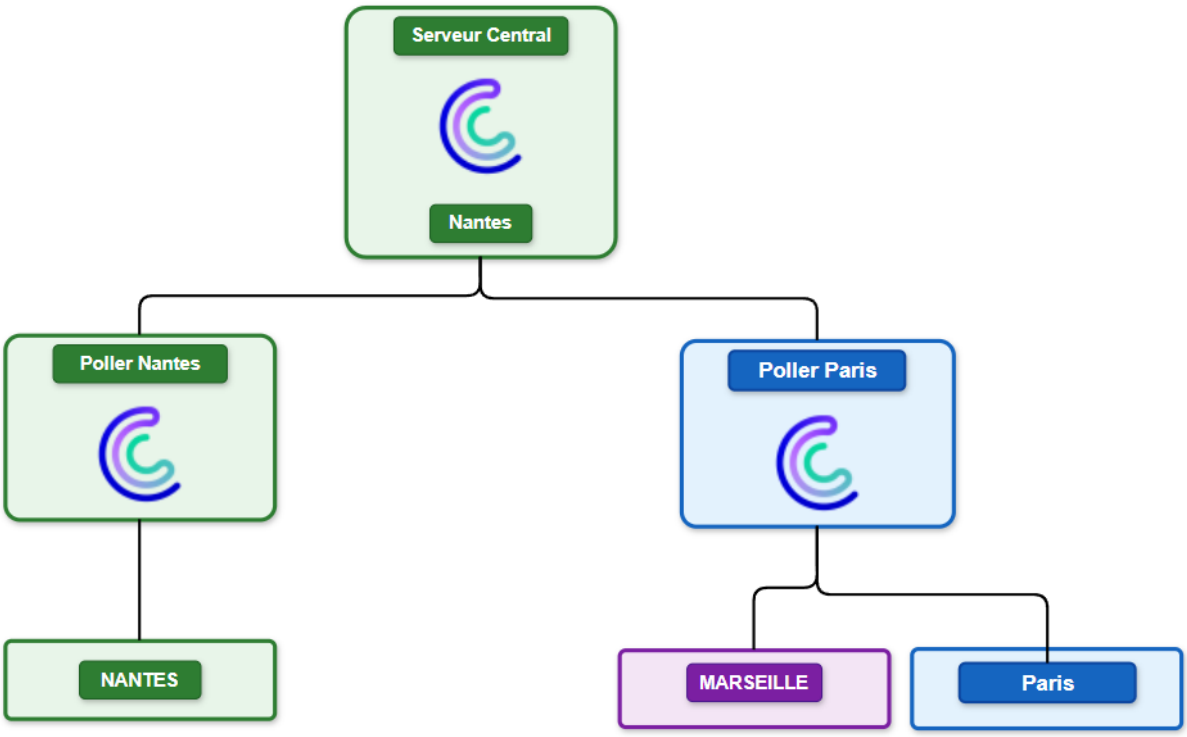
Les solutions	Solution 1	Solution 2	Solution 3
Intitulé	Centreon	Zabbix	Prometheus
Faisabilité technique *(Oui / Non, en précisant pourquoi)*	Oui – Installation bien documentée, nombreux plugins disponibles	Oui – 100% open source, très flexible mais plus technique	Oui, l'installation et l'utilisation de l'outil est possible
Besoins RH *(Internes et/ou Externes)*	Interne	Interne	Interne
Besoin Matériel et Immatériel	VM, accès réseau aux équipements, Licence Centreon	VM, accès réseau aux équipements , Licence Zabbix	VM, accès réseau aux équipements , Licence Prometheus
Coût total estimé	0	0	0
Temps Jours / Hommes	1	2	2
Durée de réalisation estimée	5h	8h	5,5h
Points forts **Points faibles**	• PF: Interface moderne, packs prêts à l'emploi, communauté francophone • Pf: Open Source, Moins flexible	• PF: Très personnalisable, 100% open source, scalable • Pf: Interface moins intuitive, courbe d'apprentissage plus élevée	• PF: Interface moderne, nombreux plugins • Pf: Installation complexe, pas d'actions automatisé, utilisation plus complexe, Open Source

4.4.4. Conclusion de l'étude de faisabilité

Au terme de l'analyse technique, financière et organisationnelle, la solution Centreon a été retenue.

Elle répond aux besoins identifiés, s'adapte à l'architecture multisites et permet une supervision efficace des machines virtuelles, des switches HP et de la borne Wi-Fi. La mise en place de cette solution constitue donc un choix pertinent et réalisable pour améliorer la disponibilité et la fiabilité de l'infrastructure informatique.

4.5. Schéma de l'infrastructure Centreon



4.5.1. Explication de l'architecture

Le serveur central, situé à Nantes centralise l'ensemble des données de supervision :

- Interface web
- Base de données
- Configuration globale
- Gestion des alertes

Il reçoit les informations des deux pollers.

Le poller de Nantes supervise :

- Les équipements du site de Nantes

Il effectue les contrôles localement puis transmet les résultats au serveur central.

Et le poller de Paris supervise :

- Les équipements du site de Paris
- Les équipements du site de Marseille

Cette répartition permet une meilleure répartition de la charge, une réduction du trafic inter-sites et une supervision plus rapide et plus stable.

4.6. Planification du projet :

Une fois toutes les informations recueillies, j'ai pu débuter la planification des différents créneaux d'intervention. Pour cela, j'ai structuré l'avancement sous forme de projet dans un fichier Excel, présenté au format diagramme de Gantt.

Mise en place Centreon

NTxSYSTEM
Chef de projet : Corentin CHAUVEL

Début du projet : 01/12/2025
Semaine d'affichage : 1

DIAGRAMME DE GANTT

TÂCHE	ATTRIBUÉE À	AVANCEMENT	DÉBUT	FIN	DUREE
Phase 1 - Préparation					
Analyse du besoin	Corentin CHAUVEL	100%	1/12/25	3/12/25	2
Etude de solutions	Corentin CHAUVEL	100%	3/12/25	6/12/25	3
Planification du projet	Corentin CHAUVEL	100%	1/12/25	1/12/25	1
Présentation des solutions au client	Corentin CHAUVEL	100%	8/12/25	8/12/25	1
Phase 2 - Intervention technique					
Mise en place du Serveur Centreon	Corentin CHAUVEL	100%	9/12/25	9/12/25	0,5
Installation / configuration de Centreon	Corentin CHAUVEL	100%	10/12/25	10/12/25	1
Installation / configuration des Poller	Corentin CHAUVEL	100%	11/12/25	11/12/25	1
Mise en place de la supervision	Corentin CHAUVEL	100%	12/12/25	15/12/25	07:30:00
Serveurs Windows	Corentin CHAUVEL	100%	12/12/25	12/12/25	02:00
Serveurs Windows Core	Corentin CHAUVEL	100%	12/12/25	12/12/25	00:30
Serveurs Linux	Corentin CHAUVEL	100%	15/12/25	15/12/25	01:00
Switchs	Corentin CHAUVEL	100%	15/12/25	15/12/25	01:00
Les FW	Corentin CHAUVEL	100%	15/12/25	15/12/25	02:00
Borne Wifi	Corentin CHAUVEL	100%	15/12/25	15/12/25	01:00
Test et ajustements finaux	Corentin CHAUVEL	100%	16/12/25	16/12/25	1
Phase 3 - Validation & Clôture					
Vérification post-intervention	Corentin CHAUVEL	100%	22/12/25	30/12/25	6

4.7. Mise en production de la solution

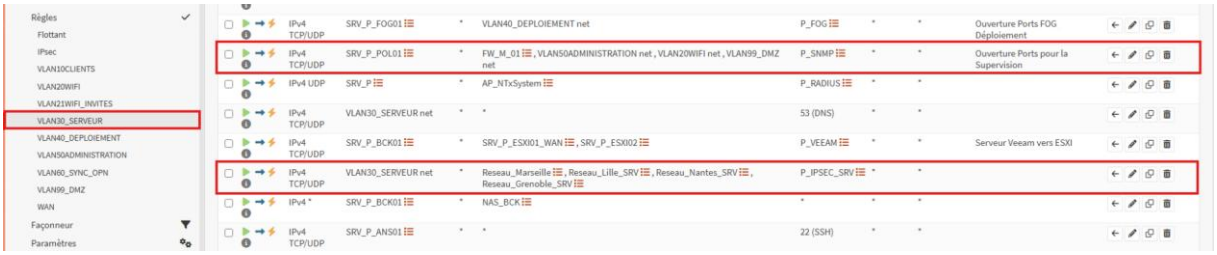
4.7.1. Règle Firewall

Dans un premier temps, il est nécessaire d'ouvrir les ports requis afin de permettre au poller de communiquer avec le serveur central et d'assurer le bon fonctionnement des requêtes SNMP vers les équipements supervisés.

Firewall de Paris (OPNsense) :

Règle 1 sur l'interface VLAN30_SERVEUR : SRV_P_POL01 > VLANs ADMIN / WIFI / DMZ et FW_M_01 > P_SNMP (161, 162). Cette règle permet au poller de Paris de superviser l'ensemble des équipements du site de Paris ainsi que le firewall de Marseille via le protocole SNMP.

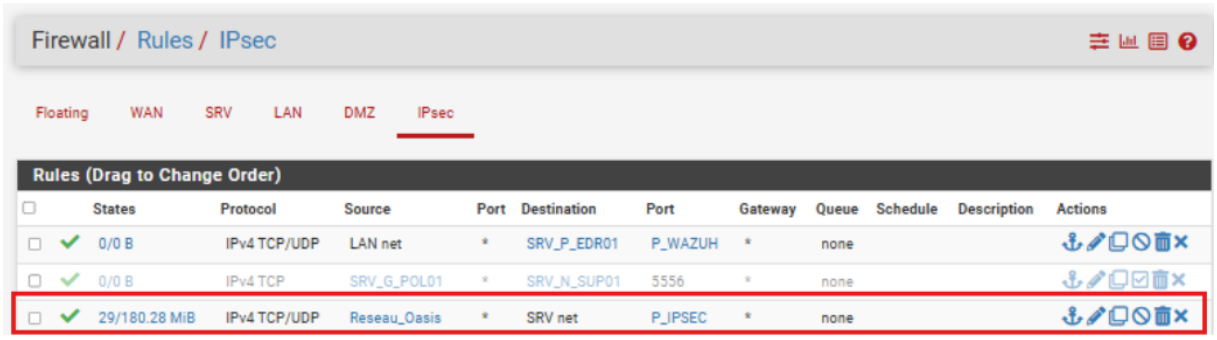
Règle 2 sur l'interface VLAN30_SERVEUR : VLAN30_SERVEUR > Réseaux distants (Nantes, Marseille)> P_IPSEC_SRV. Cette règle permet d'autoriser le passage des flux via le tunnel IPsec, notamment les ports SNMP (161, 162), ainsi que les ports nécessaires à la communication entre le poller et le serveur central situé à Nantes (5669, 5556, 3306, 5670).



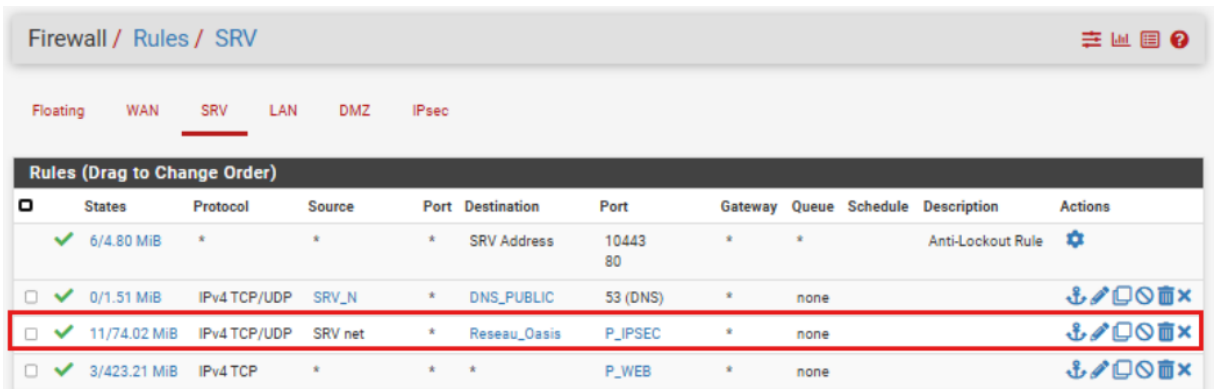
Règle 3 sur l'interface IPsec : Reseau_OASIS_SRV > VLAN30_SERVEURnet > P_IPSEC_SRV. Cette règle autorise la communication entre les différents sites.

Firewall de Nantes (PFsense) :

Règle 1 sur l'interface IPsec : Reseau_Oasis (Paris) > SRV net > P_IPSEC(notamment 161,162, 5669, 5556, 3306, 5670). Cette règle permet d'autoriser le transit des différents protocoles entre les sites.

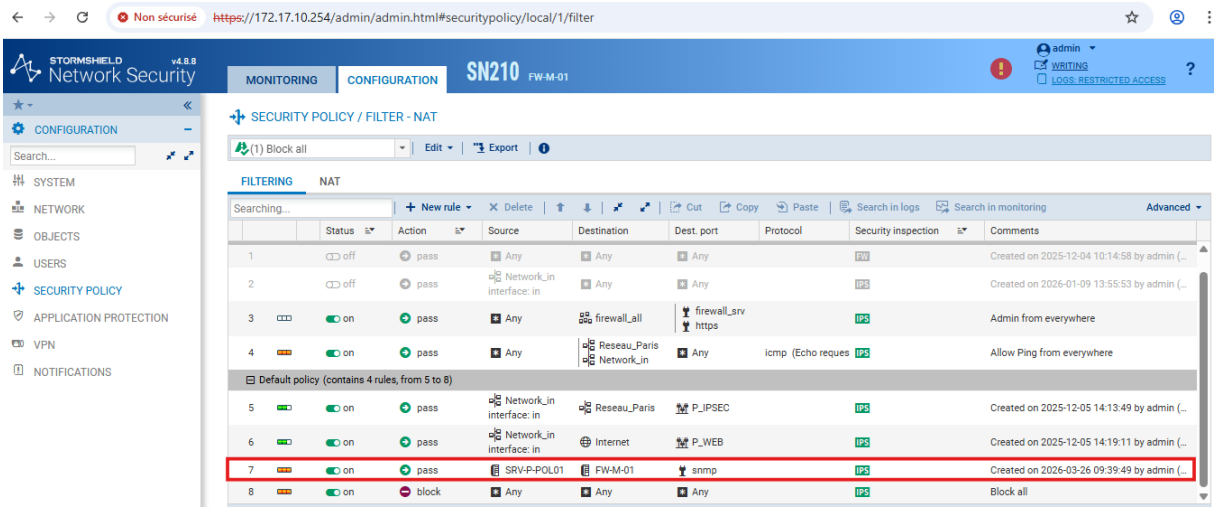


Règle 2 sur l'interface SRV : SRV net > Reseau_Oasis > P_IPSEC. Cette règle permet d'autoriser le passage des flux via le tunnel IPsec, notamment les ports SNMP (161, 162), ainsi que les ports nécessaires à la communication entre le poller et le serveur central situé à Nantes (5669, 5556, 3306, 5670).



Firewall de Marseille (Stormshield) :

Règle 1 dans SECURITY POLICY. Cette règle permet d'autoriser le passage des flux du poller vers le FW Marseille, pour le port SNMP (161).



4.7.2. Installation et configuration de Centreon sur Debian 12

Voir l'annexe 1 pour l'installation de Debian 12.

Le serveur Centreon Central est configuré avec 2 vCPU, 2 Go de mémoire vive, 40 Go de stockage et une interface réseau connectée au réseau SRV.

4.7.2.1. Mise à jour du système

Après l'installation de mon serveur Debian 12, j'ai commencé par mettre le système à jour avec la commande suivante :

```
apt update && apt upgrade
```

Explication :

apt update : Cette commande me permet de mettre à jour la liste des paquets disponibles depuis les dépôts configurés sur le système.

apt upgrade : Elle installe les dernières versions des paquets déjà présents sur le serveur.

&& : Cela signifie que la deuxième commande s'exécute uniquement si la première s'est déroulée correctement.

4.7.2.2. Installation des dépendances

Ensuite, j'installe les paquets nécessaires :

```
apt update && apt install lsb-release ca-certificates apt-transport-https software-properties-common wget gnupg2 curl
```

Installation du dépôt MariaDB

Pour installer MariaDB 10.11, j'ajoute le dépôt officiel avec :

```
curl -LsS https://r.mariadb.com/downloads/mariadb_repo_setup | sudo bash -s -- --os-type=debian --os-version=12 --mariadb-server-version="mariadb-10.11"
```

Installation du dépôt Centreon

J'ajoute ensuite le dépôt principal Centreon :

```
echo "deb https://packages.centreon.com/apt-standard/ $(lsb_release -sc)-25.10-stable main" | tee -a /etc/apt/sources.list.d/centreon-25.10-stable.list
```

J'ajoute également le dépôt des plugins :

```
echo "deb https://packages.centreon.com/apt-plugins-stable/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/centreon-plugins.list
```

Importation de la clé GPG :

```
wget -O- https://apt-key.centreon.com | gpg --dearmor | tee /etc/apt/trusted.gpg.d/centreon.gpg > /dev/null 2>&1
```

Je l'importe pour que mon système puisse vérifier que les paquets du dépôt Centreon viennent vraiment de Centreon, qu'ils n'ont pas été modifiés et qu'ils sont bien signés

Puis je mets à jour les dépôts :

```
apt update
```

4.7.2.3. Installation

J'installe le serveur central avec base locale :

```
apt update

apt install -y centreon-mariadb centreon
```

Explication :

centreon-mariadb : Installe MariaDB configurée pour fonctionner avec Centreon.

centreon : Installe le serveur central (interface web, moteur de supervision, broker, etc.).

-y : Valide automatiquement les confirmations.

Rechargement des services :

```
systemctl daemon-reload
```

Je recharge les fichiers de configuration systemd.

Puis je redémarre MariaDB :

```
systemctl restart mariadb
```

4.7.2.4. Configuration

Démarrage des services au démarrage du système :

```
systemctl enable php8.2-fpm apache2 centreon cbd centengine gorgoned centreontrapd snmpd snmptrapd

systemctl enable mariadb

systemctl restart mariadb
```

enable → J'active le démarrage automatique au boot.

restart → Je redémarre immédiatement le service.

Sécurisation de MariaDB :

```
mariadb-secure-installation
```

Cette commande me permet de :

- Définir un mot de passe root sécurisé
- Supprimer les utilisateurs anonymes
- Désactiver l'accès root distant (je réponds Non selon la procédure demandée)
- Supprimer la base de test
- Recharger les privilèges

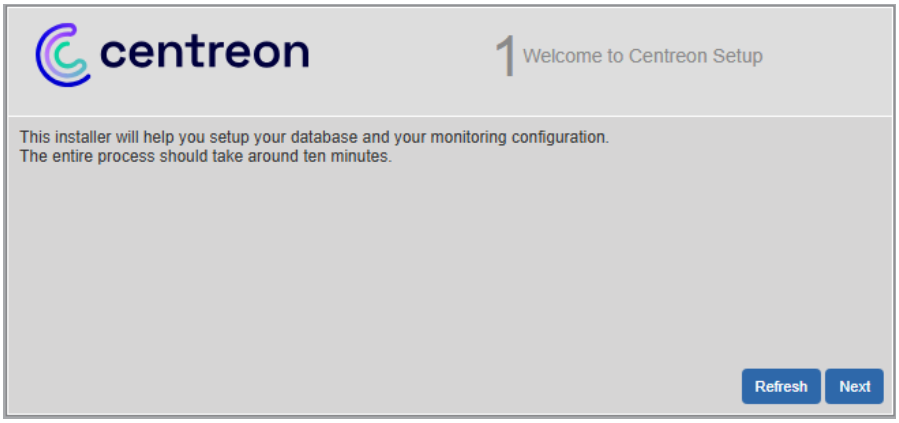
4.7.2.5. Installation Web

Je démarre Apache :

```
systemctl start apache2
```

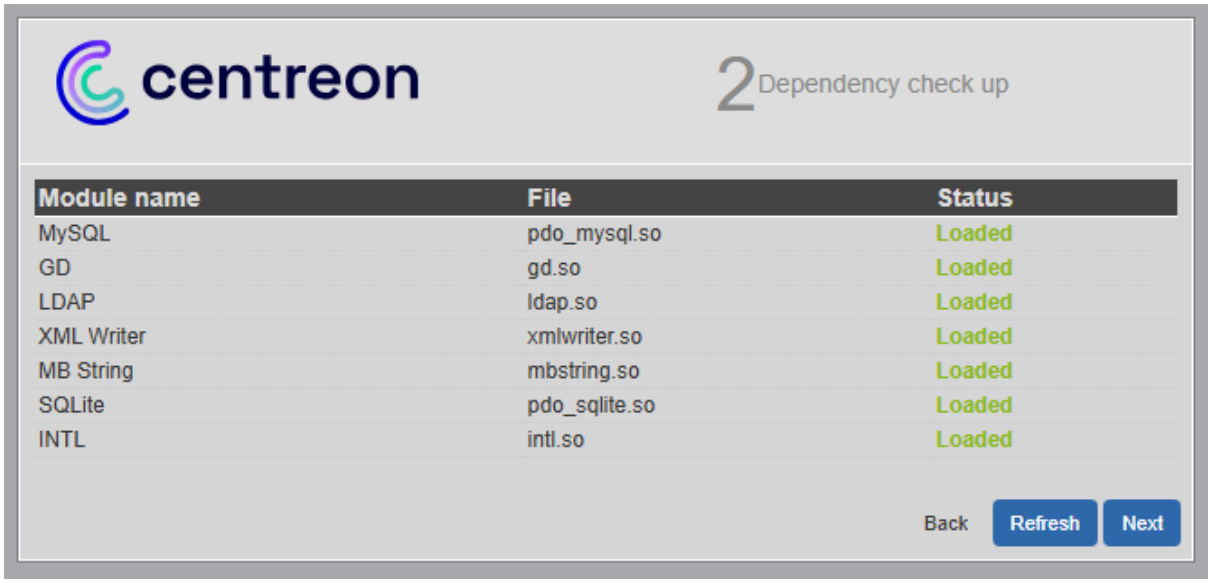
Pour terminer l'installation, je suis l'assistant d'installation sur un navigateur en tapent d'adresse IP.

Il s'agit de l'écran d'accueil de la configuration.



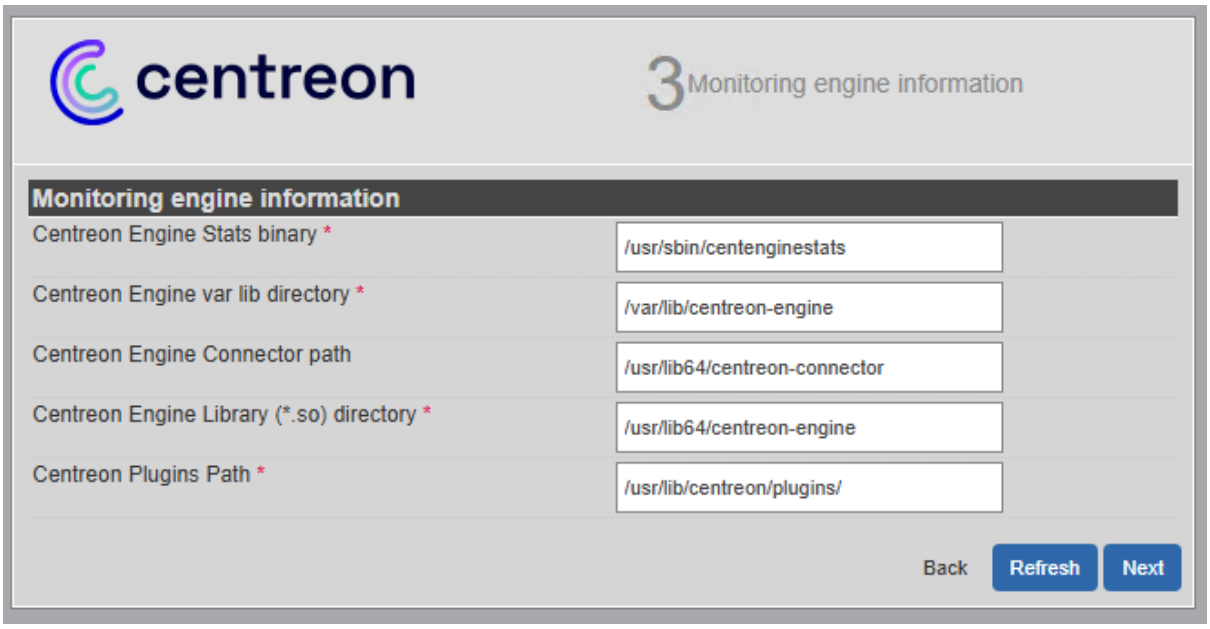
Je clique simplement sur Next pour commencer la procédure.

À cette étape, Centreon vérifie automatiquement que tous les modules et prérequis nécessaires sont bien installés sur le serveur.



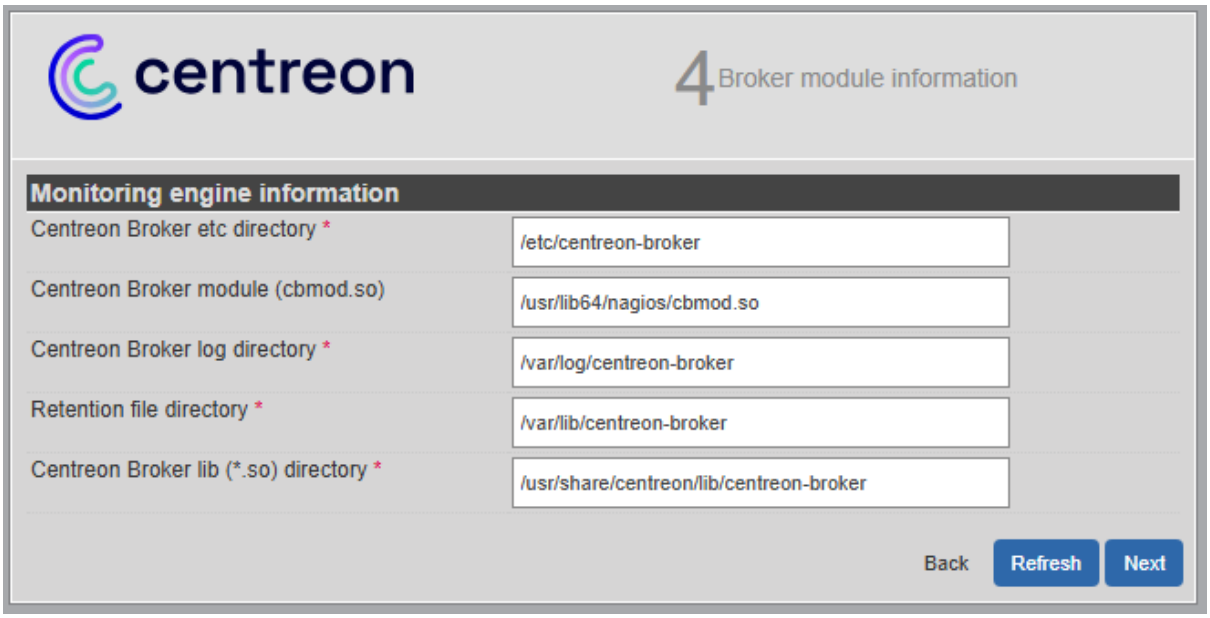
Si un prérequis n'est pas valide, je corrige le problème côté serveur, puis je clique sur Refresh pour relancer la vérification. Une fois que tout est conforme, je clique sur Next.

Ici, je dois définir les chemins utilisés par le moteur de supervision (Centreon Engine). Par défaut, les chemins proposés sont adaptés à une installation standard sur Debian 12.



Je conserve donc les valeurs par défaut recommandées, puis je clique sur Next.

Cette étape concerne le module Broker, qui sert à la transmission et au traitement des données de supervision.



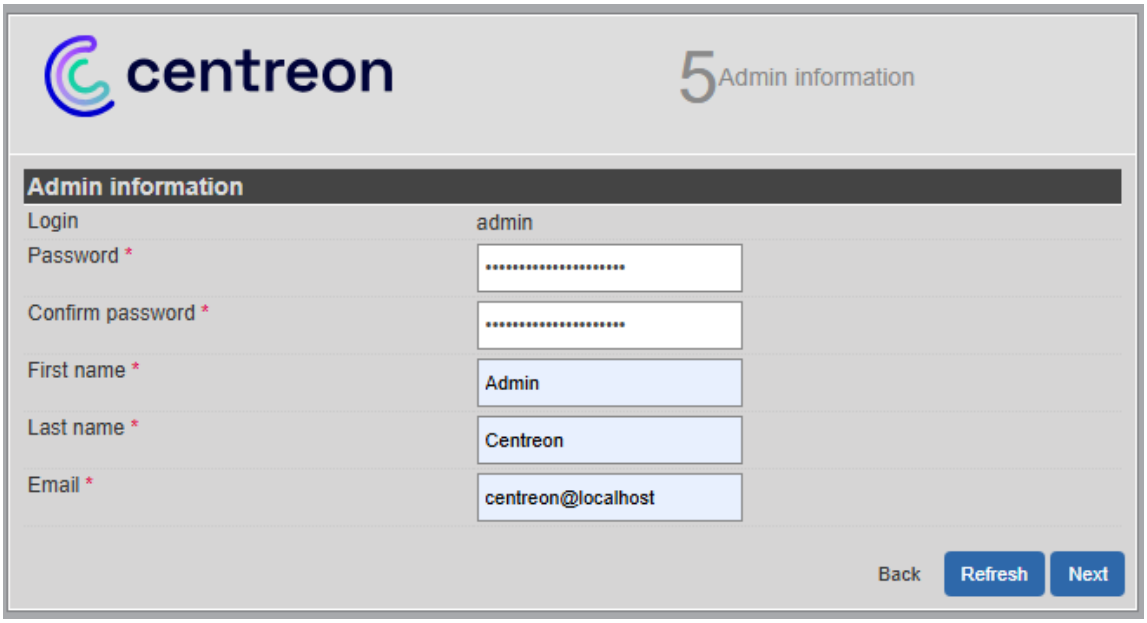
Comme pour l'étape précédente, les chemins proposés par défaut sont corrects pour mon installation. Je ne modifie rien et je clique sur Next.

À cette étape, je crée le compte administrateur par défaut.

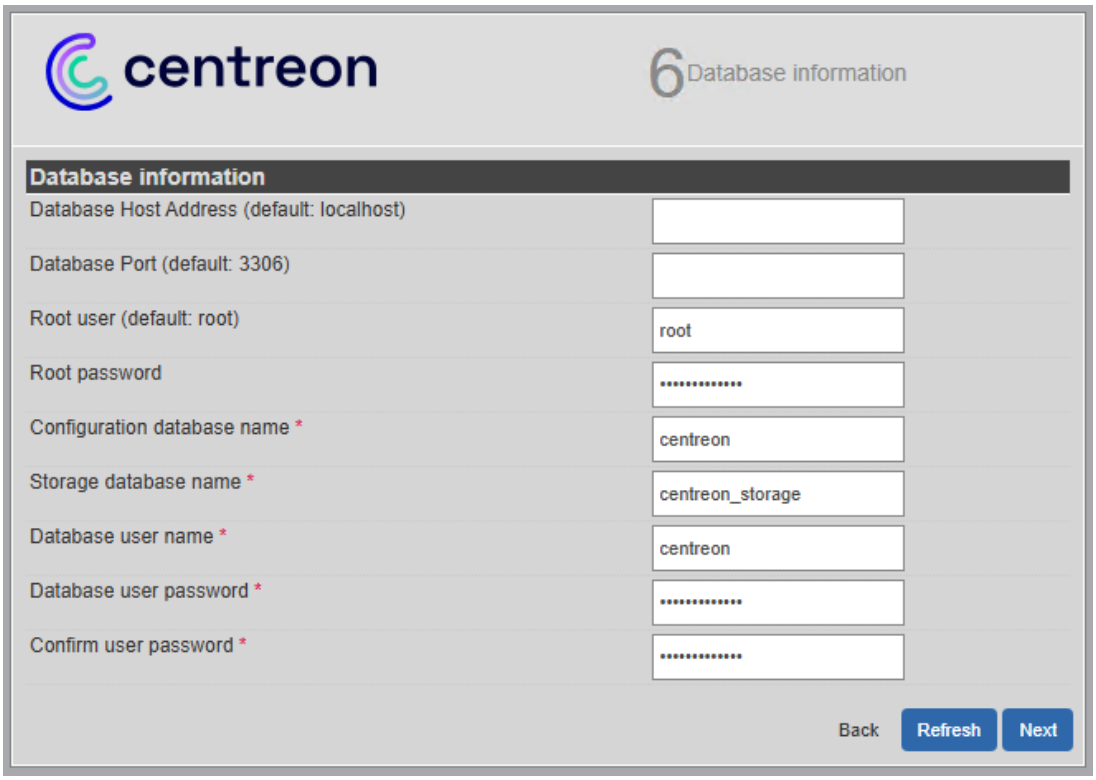
Je renseigne :

- Le nom d'utilisateur (admin par défaut)
- Le mot de passe
- L'adresse email

Ce compte me servira pour me connecter à Centreon après l'installation.



Ici, je configure la connexion à la base de données. Si j'utilise une base locale, je laisse la valeur par défaut (localhost).

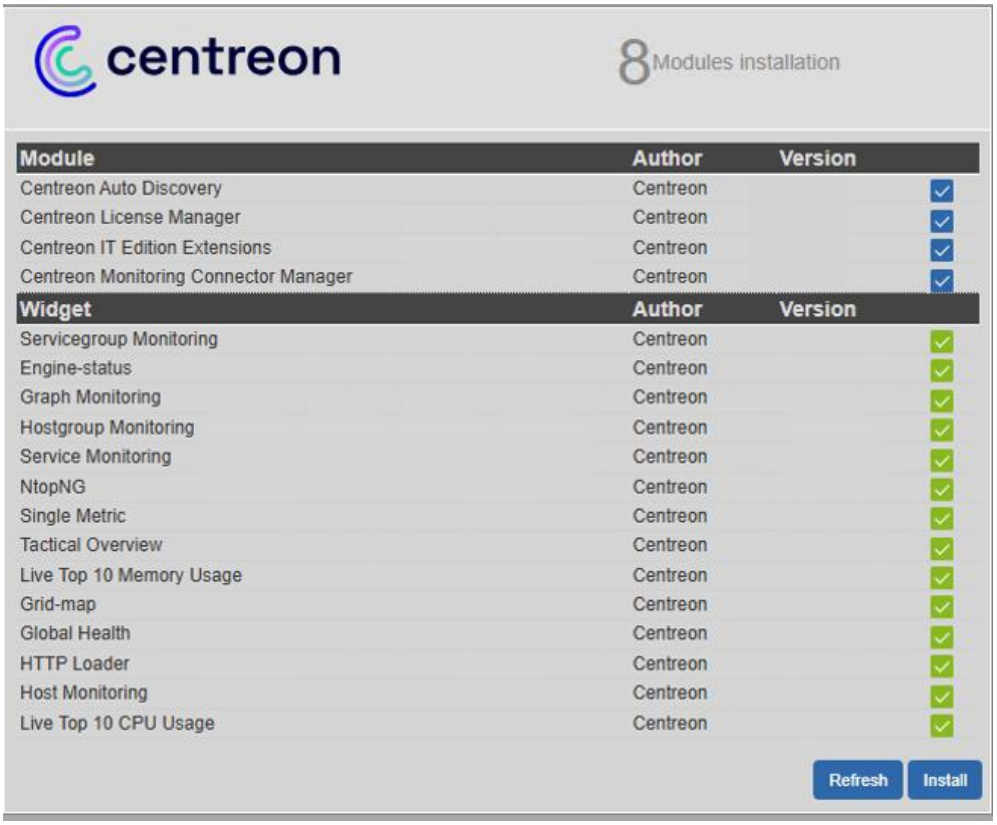


L'assistant procède maintenant à :

- La création des bases de données
- L'initialisation des tables
- La génération des fichiers de configuration

Une fois terminé, je clique sur Next.

À cette étape, je peux sélectionner les modules et widgets que je souhaite installer. Je sélectionne les modules nécessaires à mon environnement, puis je clique sur Install.



Après l'installation des modules, je clique sur Next.

Un écran final s'affiche indiquant que l'installation est terminée.

Je clique sur Finish pour terminer la configuration.

Je peux maintenant me connecter à l'interface Centreon en utilisant le compte administrateur que j'ai créé.

4.7.3. Installation et configuration d'un Poller (collecteur) Centreon sur Debian 12 :

Dans cette partie, je détaille les étapes que j'ai suivies pour installer un poller Centreon (serveur collecteur) et l'enregistrer auprès du serveur central. C'est la même procédure pour les deux Pollers. Chaque poller dispose d'1 vCPU, de 2 Go de RAM, de 20 Go de stockage et d'une interface réseau reliée au réseau SRV.

Prérequis :

Après l'installation de mon serveur Debian 12, je commence par mettre le système à jour :

```
apt update && apt upgrade
```

4.7.3.1. Pré-installation

Installation des dépendances :

Avant d'ajouter les dépôts Centreon, j'installe les dépendances nécessaires :

```
apt update && apt install lsb-release ca-certificates apt-transport-https software-properties-common wget gnupg2 curl
```

Ajout des dépôts Centreon :

Pour pouvoir installer le poller, j'ajoute les dépôts officiels Centreon.

```
echo "deb https://packages.centreon.com/apt-standard/ $(lsb_release -sc)-25.10-stable main" | tee -a /etc/apt/sources.list.d/centreon-25.10-stable.list

echo "deb https://packages.centreon.com/apt-plugins-stable/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/centreon-plugins.list
```

Ensuite, j'importe la clé GPG :

```
wget -O- https://apt-key.centreon.com | gpg --dearmor | tee /etc/apt/trusted.gpg.d/centreon.gpg > /dev/null 2>&1
```

Puis je mets à jour la liste des paquets :

```
apt update
```

4.7.3.2. Installation du Poller

Pour installer le moteur de supervision sur le serveur poller, j'exécute :

```
apt install -y --no-install-recommends centreon-poller
```

--no-install-recommends : Permet d'installer uniquement les paquets nécessaires sans composants additionnels inutiles.

Activation des services au démarrage :

Pour que les services démarrent automatiquement au boot :

```
systemctl enable centreon centengine centreontrapd snmptrapd gorgoned
```

Cela active :

- Centreon Engine (moteur de supervision)
- Les services de traps SNMP
- Gorgoned (communication avec le central)

Démarrage des services passifs, je démarre les services de supervision passive :

```
systemctl start centreontrapd snmptrapd gorgoned
```

Puis je redémarre le moteur de supervision :

```
systemctl restart centengine
```

Enregistrement du Poller auprès du Central

Pour transformer le serveur en collecteur et l'enregistrer auprès du serveur central, j'exécute la commande suivante sur le poller :

```
/usr/share/centreon/bin/registerServerTopology.sh -u admin \ -t poller -h 172.19.30.25 -n SRV-N-POL01
```

Paramètres utilisés :

-u admin : Compte administrateur Centreon utilisé pour l'API

-t poller : Type de serveur (collecteur)

-h 172.19.30.25 : Adresse IP du serveur central (vue depuis le poller)

-n SRV-N-POL01 : Nom que je donne au poller dans Centreon

Authentification :

Le script me demande :

- Le mot de passe du compte admin
- De sélectionner l'adresse IP du poller

Un résumé des informations s'affiche :

- Compte API utilisé : root
- Serveur cible : 172.19.30.12
- Nom du poller : SRV-N-POL01
- Adresse IP sélectionnée :172.19.30.25

Je confirme en répondant y.

Confirmation d'enregistrement :

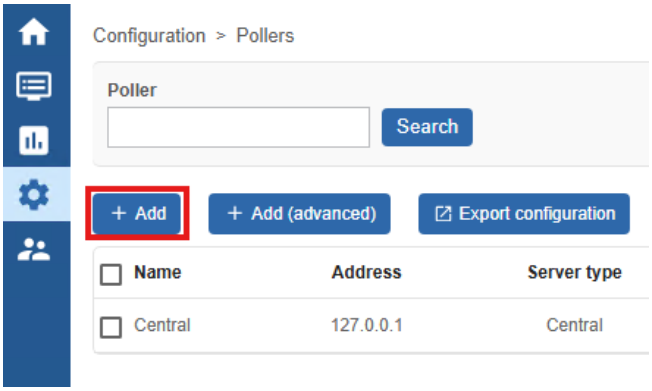
Je reçois un message indiquant que le poller a bien été lié au serveur central.

4.7.3.3. Rattachement du Poller au central

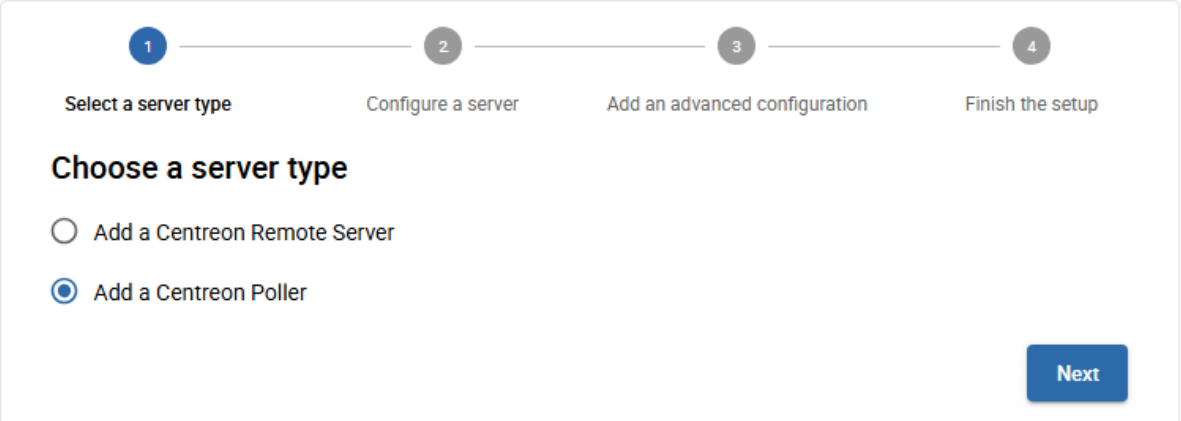
4.7.3.3.1. Configurer un nouveau collecteur

Depuis Centreon, je me rends dans : Configuration > Collecteurs > Collecteurs

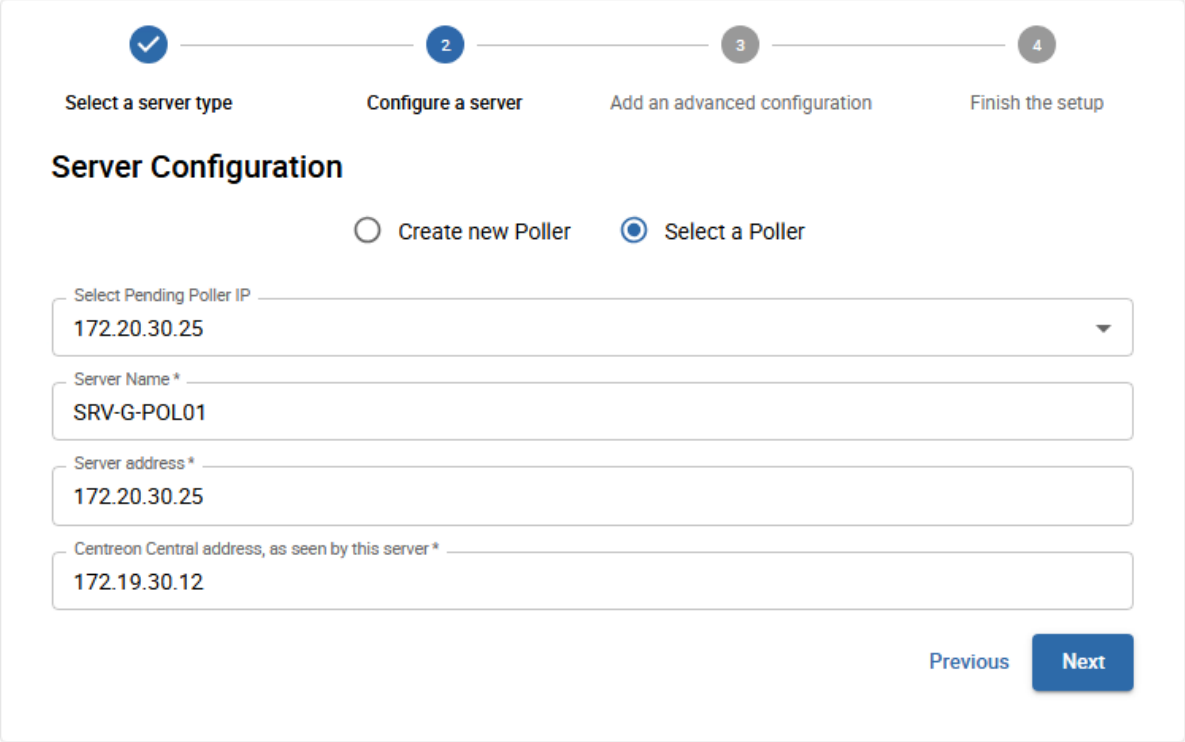
Puis je clique sur Add pour lancer l'assistant de configuration.



Je sélectionne : Ajouter un collecteur Centreon Puis je clique sur Next.

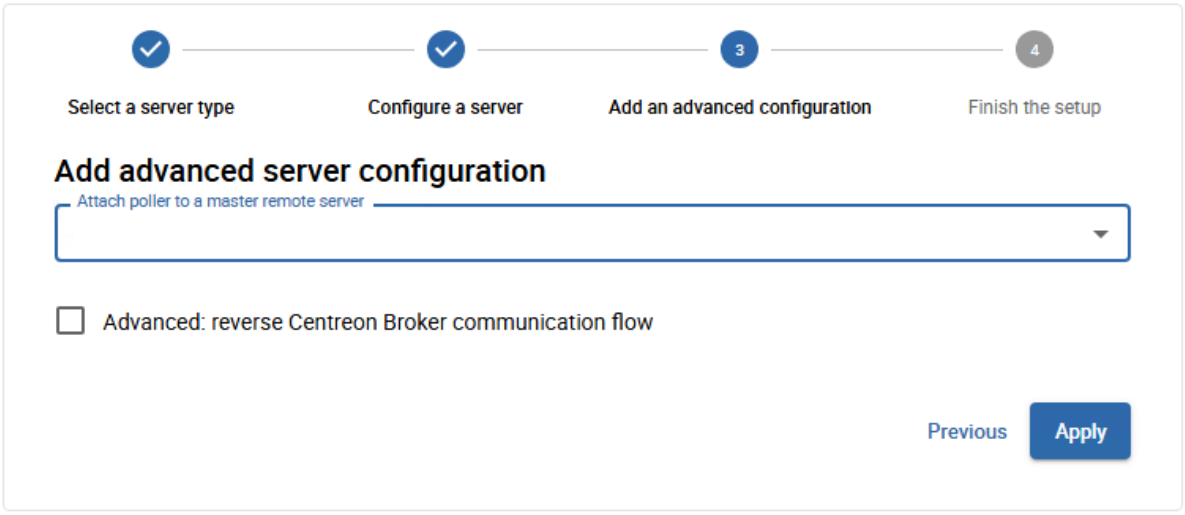


Choix du mode d'ajout :



Toutes les informations se préremplissent automatiquement.

Ensuite, je clique simplement sur Apply, car je n'ai pas de configuration particulière à effectuer.



4.7.3.3.2. Activer la communication

La communication entre le serveur Central et le Poller est assurée par Gorgone. Deux méthodes sont possibles : ZMQ (recommandé) et le SSH (méthode legacy), j'utilise ZMQ, qui est la méthode recommandée.

Récupération de la configuration Gorgone :

Depuis la liste des collecteurs, je clique sur l'icône Gorgone configuration correspondant à mon poller.

Une fenêtre pop-up s'ouvre avec une configuration à copier. Je clique sur Copy to clipboard.

Configuration côté Poller :

Sur le serveur Poller, je colle directement le contenu dans le terminal. Cela crée automatiquement le fichier de configuration Gorgone attendu.

Cette commande génère le fichier :

```
/etc/centreon-gorgone/config.d/40-gorgoned.yaml
```

Qui contient :

- L'identifiant du poller
- Le type de communication (tcp)
- Le port 5556
- La clé d'authentification
- Les modules activés (engine, action)

Redémarrage du service Gorgone :

Une fois la configuration créée, je redémarre le service sur le Poller :

```
systemctl restart gorgoned
```

Puis je vérifie son état :

```
systemctl status gorgoned
```

Le service doit apparaître en active (running). Si c'est le cas, la communication est prête côté poller.

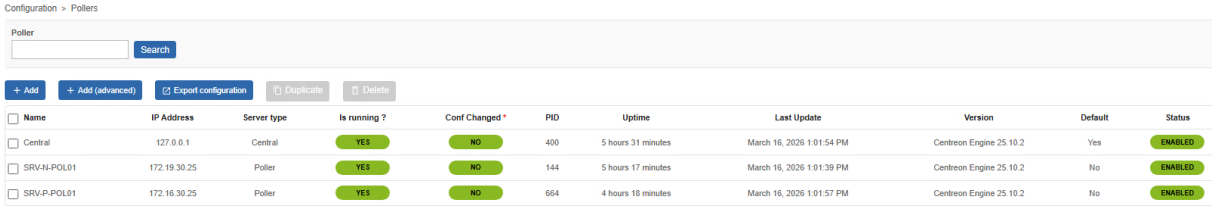
Redémarrage côté Central :

Pour forcer le Central à se reconnecter au poller, je redémarre également Gorgone sur le serveur Central :

```
systemctl restart gorgoned
```

4.7.3.3.3. Gestion des Pollers dans Centreon

Dans Centreon, la section Configuration > Poller permet de gérer les pollers utilisés pour la supervision.



Cette interface permet notamment de :

- Visualiser les Pollers configurés
- Ajouter ou modifier un Poller
- Exporter une configuration vers un ou plusieurs Poller

4.7.4. Mise en place de ma solution gratuite IT-100

Je souhaite mettre en place la solution gratuite IT-100 proposée par Centreon afin de tester toutes les fonctionnalités de Centreon IT Edition.

Cette offre me permet :

- D'installer jusqu'à 3 serveurs centraux
- De superviser jusqu'à 100 hôtes
- D'utiliser la découverte automatique des hôtes et services
- D'accéder à l'ensemble de la bibliothèque de connecteurs de supervision

4.7.4.1. Demande de la licence IT-100

Je commence par me rendre sur le site officiel de Centreon, à la page Essayez Centreon IT Edition, puis je remplis le formulaire de demande.

Après validation du formulaire, je reçois un email contenant mon jeton (token) pour activer l'offre IT-100.

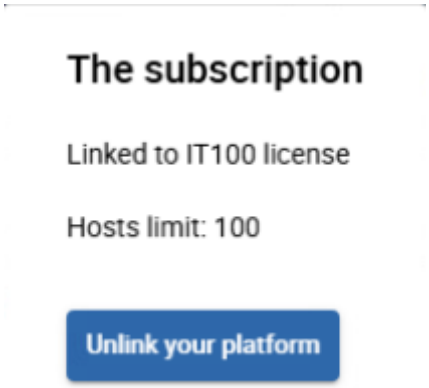
Voici le lien du site pour faire la demande : https://www.centreon.com/fr/essai-gratuit/#dployez_vous_mme_centreon

4.7.4.2. Ajout du jeton IT-100

Une fois connecté à l'interface :

Je vais dans : Administration > Extensions > Manager

Puis je clique sur le bouton Add Token, une fenêtre s'ouvre. Et je saisis le jeton reçu par email, puis je clique sur Enregistrer.



Une fois le jeton enregistré et validé, ma plateforme est prête.

4.7.4.3. Architecture et rôle des composants Centreon

Dans une architecture Centreon avec un serveur Central et un Poller, il est nécessaire d'ajouter et de connecter les composants (comme le poller) au serveur central pour assurer une supervision cohérente et centralisée.

- Base Pack : fournit des modèles et plugins prêts à l'emploi pour superviser rapidement différents équipements.
- Centreon Central : serveur principal qui gère la configuration, l'interface web et la supervision globale.
- Centreon Database : stocke toutes les données (configurations, résultats, historiques).
- Centreon Poller : exécute les contrôles sur les équipements et envoie les résultats au Central.

4.7.5. Import / Export avec le module Centreon AWIE

Pour faciliter la duplication et la sauvegarde de configuration Centreon, j'utilise le module AWIE (Centreon API Web Import/Export).

Ce module me permet d'exporter des objets depuis une plateforme source correctement configurée, puis de les importer sur une plateforme cible.

Il repose sur les commandes CLAPI, mais son avantage est que je peux tout faire directement depuis l'interface web, sans passer par la ligne de commande.

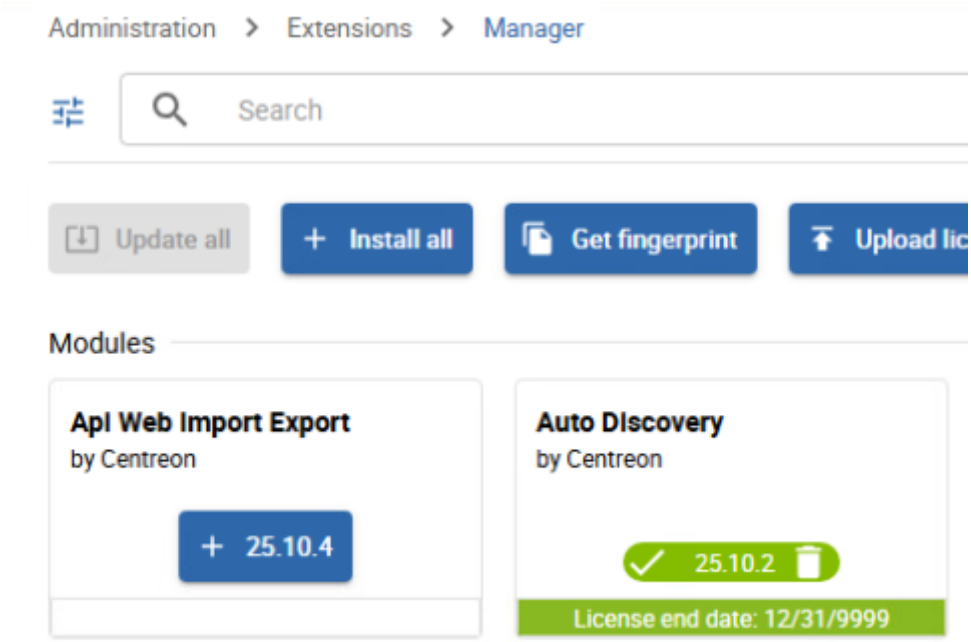
4.7.5.1. Installation du module AWIE

Sur le serveur Centreon, j'installe le module avec la commande suivante :

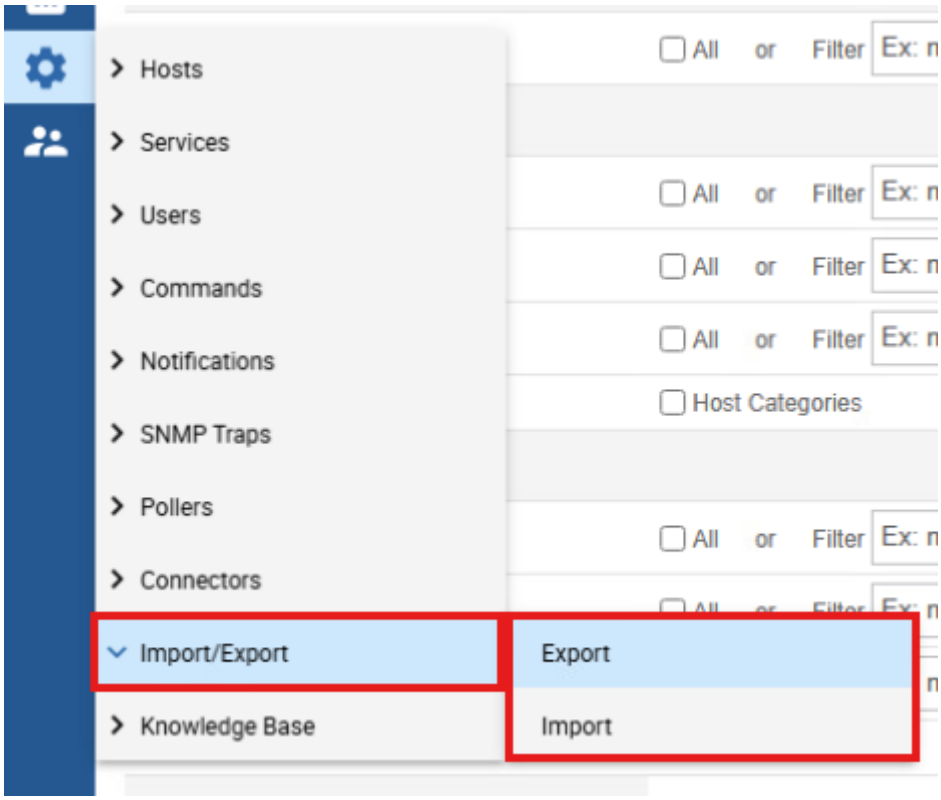
```
apt install centreon-awie
```

4.7.5.2. Mise en place du module

Ensuite, sur l'interface web de Centreon, dans Administration > Extensions > Manager, je peux ajouter le module.



Une fois ajouté, dans Configuration > Import/Export, je peux exporter la configuration pour effectuer une sauvegarde, par exemple, et aussi faire des imports si besoin.

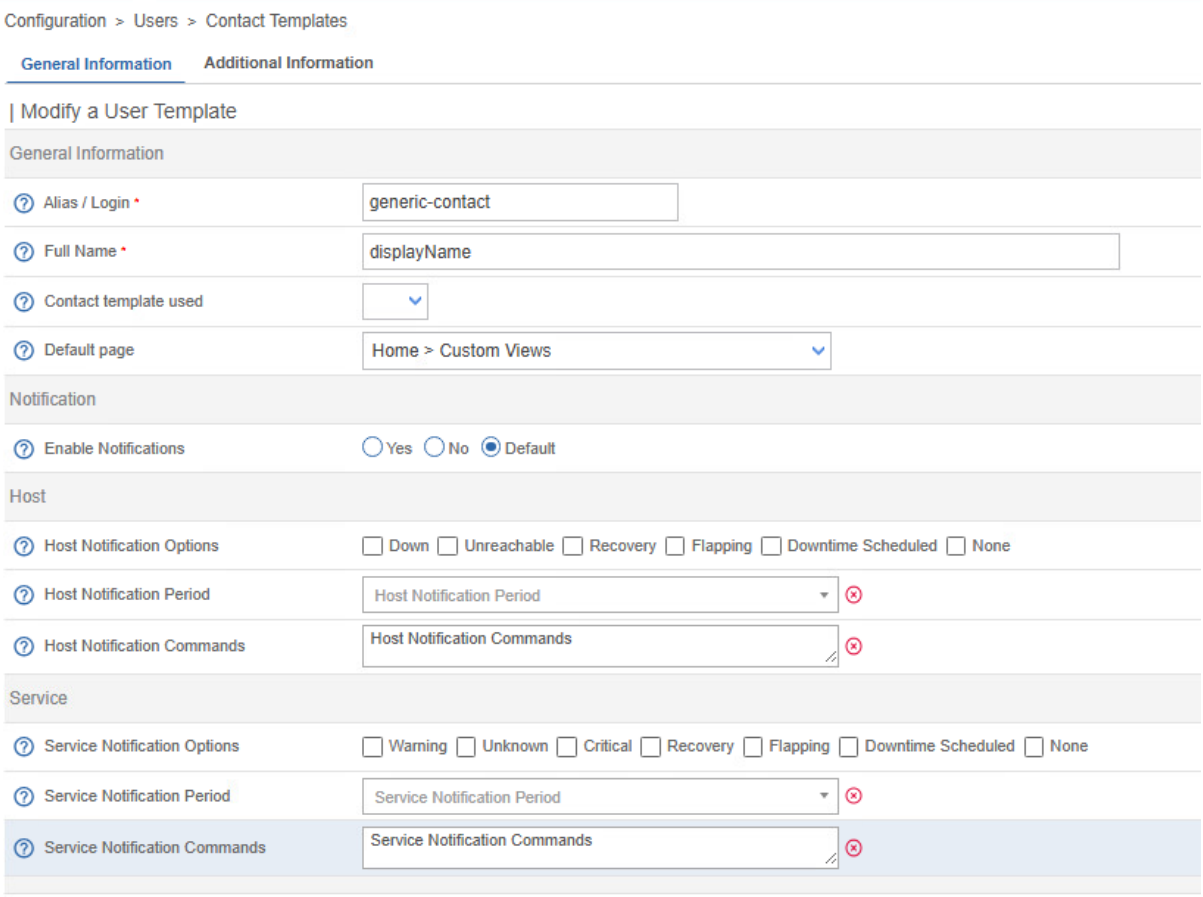


4.7.6. Connecter Centreon à un annuaire LDAP

Configuration de Centreon afin de le connecter à mon annuaire LDAP. Cela permet aux utilisateurs présents dans le LDAP de se connecter à Centreon avec leurs identifiants LDAP.

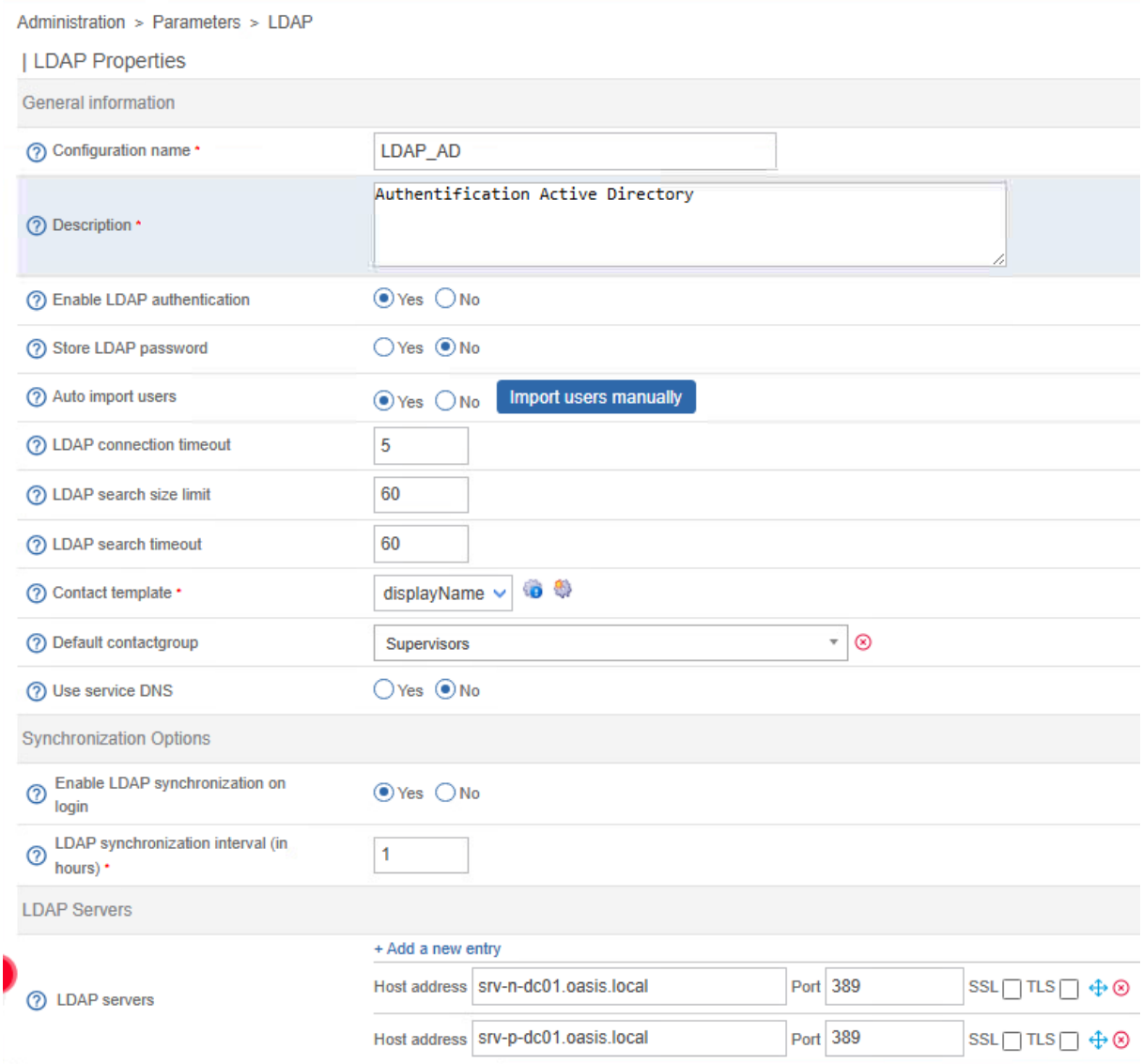
4.7.6.1. Création User Template

Dans Centreon, un User Template LDAP sert à définir une configuration par défaut pour les utilisateurs provenant de LDAP. Lorsqu'un utilisateur se connecte, son compte est créé automatiquement avec les droits, groupes et paramètres définis dans le template. Cela permet d'automatiser la gestion des accès et de gagner du temps dans l'administration.



4.7.6.2. Configuration LDAP

Voici la configuration que j'ai effectuée. La plupart des paramètres sont restés par défaut.



Informations générales :

Paramètre	Valeur	Explication
Nom de configuration	LDAP_AD	Nom de la configuration LDAP dans Centreon
Description	Authentication Active Directory	Indique que l'authentification s'appuie sur l'AD
Authentification LDAP	Activée	Centreon délègue l'authentification à l'Active Directory
Stockage mot de passe LDAP	Non	Les mots de passe ne sont pas stockés dans Centreon
Import automatique des utilisateurs	Oui	Les utilisateurs AD sont créés automatiquement lors de leur première connexion
Timeout connexion LDAP	5 secondes	Délai maximal pour établir une connexion LDAP
Limite recherche LDAP	60	Nombre maximal d'objets retournés

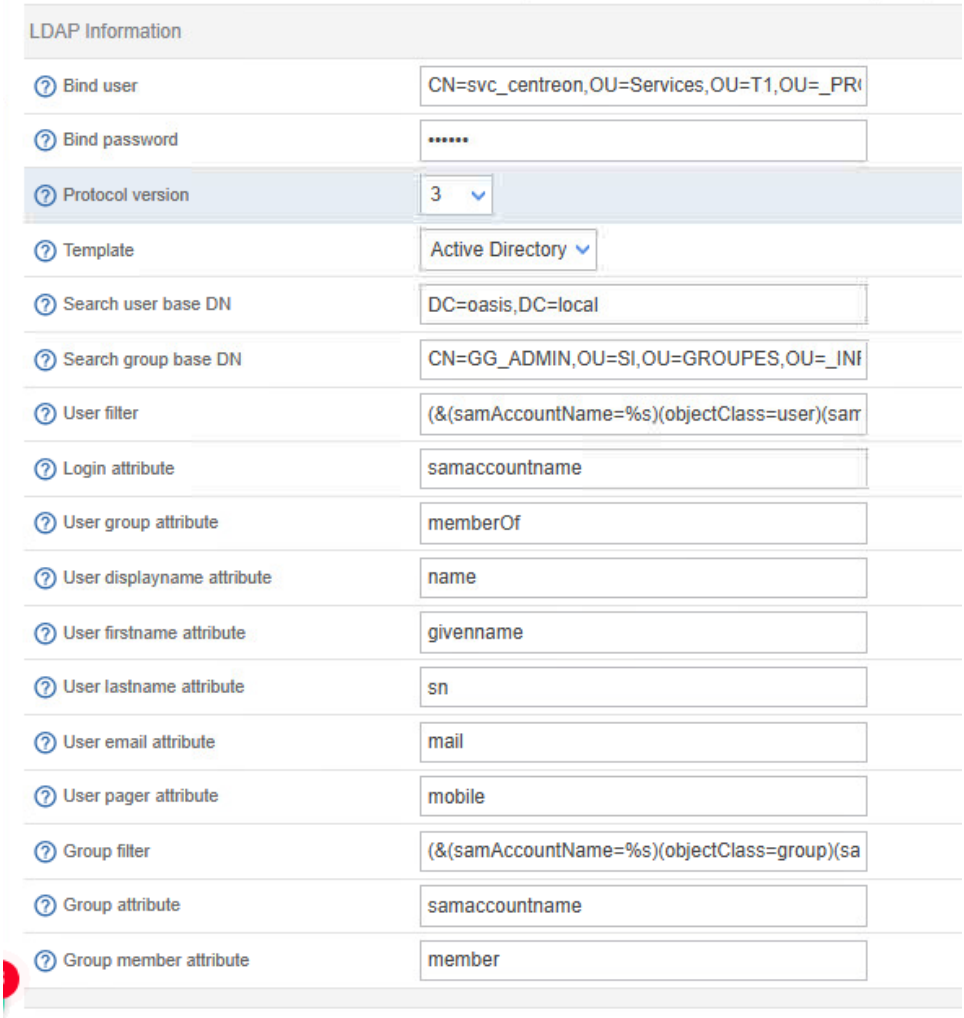
Timeout recherche LDAP	60 secondes	Durée maximale d'une requête LDAP
Groupe de contact par défaut	Supervisors	Groupe Centreon attribué par défaut aux utilisateurs importés
Synchronisation à la connexion	Activée	Mise à jour des informations utilisateur à chaque login
Intervalle de synchronisation	1 heure	Fréquence de synchronisation LDAP

Serveurs LDAP :

Deux contrôleurs de domaine sont configurés pour assurer la haute disponibilité :

- srv-n-dc01.oasis.local (port 389)
- srv-p-dc01.oasis.local (port 389)

Port 389 = LDAP standard.



Centreon utilise un compte technique pour interroger l'Active Directory :

- Bind user : CN=svc_centreon,OU=Services,OU=_PRODUCTION,DC=oasis,DC=local
- Version protocole LDAP : 3
- Template : Active Directory

Ce compte a uniquement des droits de lecture dans l'AD.

Base de recherche :

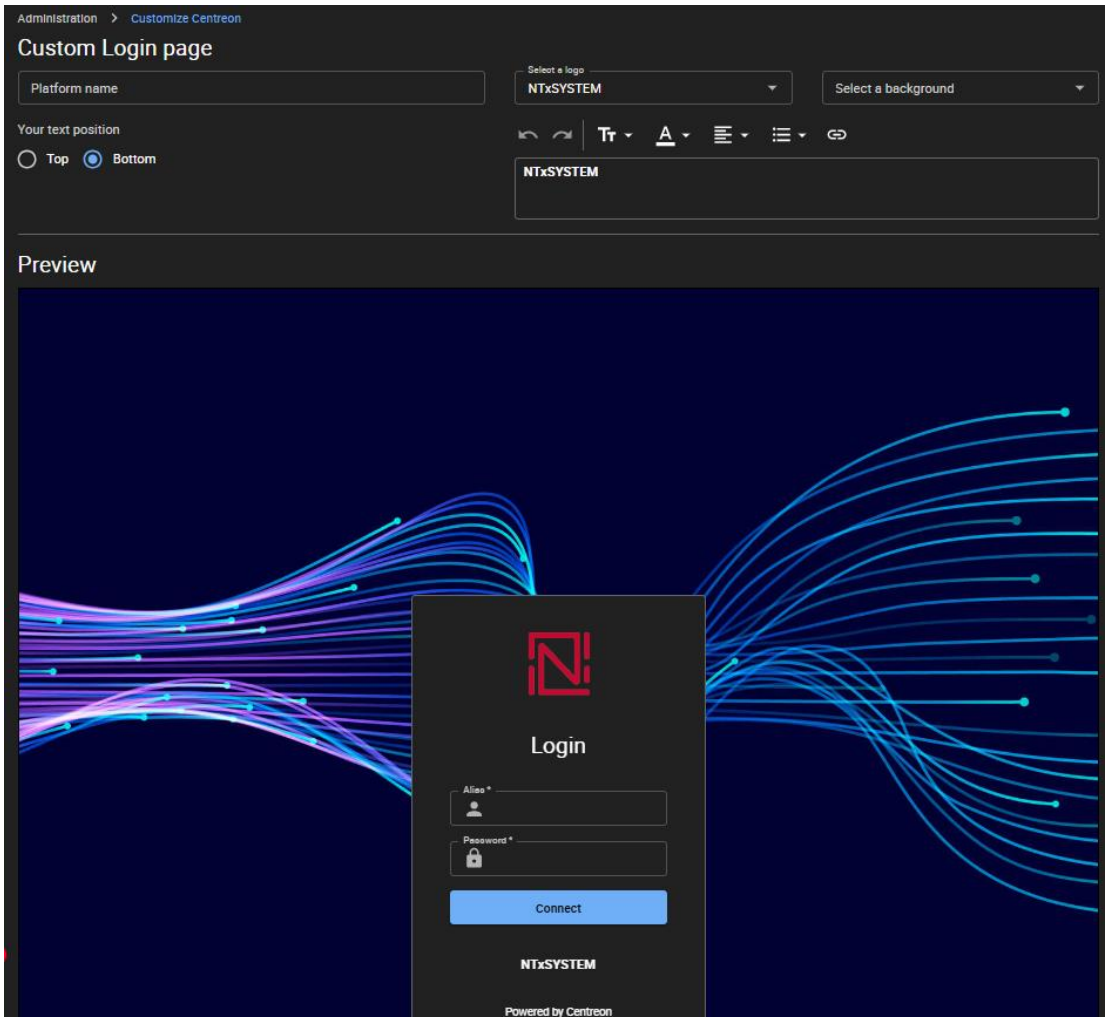
Base utilisateurs : DC=oasis,DC=local

Centreon recherche les utilisateurs dans tout le domaine oasis.local.

Base groupes : CN=GG_ADMIN,OU=SI,OU=GROUPES,OU=_INFRA,...

La recherche des groupes est limitée à une unité d'organisation spécifique.

4.7.6.3. Personnalisation page de connexion



Voici le résultat avec le logo NTxSYSTEM et le nom juste en dessous du bouton Connect.

4.7.7. Ajout des hôtes et des services

Voici toutes les machines qui seront supervisées via Centreon, avec selon le système d'exploitation différentes méthodes pour la mise en place.

Machines virtuelles Paris:

Nom	Hyperviseur	IP	Système d'exploitation
SRV-P-DC01	SRV-P-ESXI01	172.16.30.10	Microsoft Windows Server 2022
FW-P-01	SRV-P-ESXI01	172.16.50.253	Autre Linux (64 bits)
SRV-P-BCK01	SRV-P-ESXI01	172.16.30.15	Microsoft Windows Server 2022
SRV-P-GLPI01	SRV-P-ESXI01	172.16.30.14	Debian GNU/Linux 12
SRV-P-FOG01	SRV-P-ESXI01	172.16.30.11	Debian GNU/Linux 12
SRV-P-OCS01	SRV-P-ESXI01	172.16.30.13	Debian GNU/Linux 12
SRV-P-CLOUD01	SRV-P-ESXI01	172.16.30.16	Debian GNU/Linux 12
SRV-P-HaProxy	SRV-P-ESXI01	172.16.99.10	Debian GNU/Linux 12
SRV-P-NTP01	SRV-P-ESXI02	172.16.30.18	Debian GNU/Linux 12
FW-P-02	SRV-P-ESXI02	172.16.50.252	Autre Linux (64 bits)
SRV-P-DC02	SRV-P-ESXI02	172.16.30.20	Microsoft Windows Server 2022
SRV-P-DFS01	SRV-P-ESXI02	172.16.30.50	Microsoft Windows Server 2022

Machines virtuelles Nantes:

Nom	Hyperviseur	IP	Système d'exploitation
FW-N-01	Proxmox-Nantes	172.19.30.254	Autre Linux (64 bits)
SRV-N-DC01	Proxmox-Nantes	172.19.30.10	Microsoft Windows Server 2022
SRV-N-DC02	Proxmox-Nantes	172.19.30.20	Microsoft Windows Server Core 2022
SRV-N-DFS01	Proxmox-Nantes	172.19.30.50	Microsoft Windows Server 2022

Machines Marseille:

Nom	IP	Système d'exploitation
FW-M-01	172.17.10.254	Strormshield

4.7.7.1. Supervision d'un serveur Windows

Pour superviser un serveur Windows avec Centreon, il est nécessaire d'ajouter l'hôte et de configurer les services que l'on souhaite surveiller.

Dans notre infrastructure, les services critiques identifiés pour les serveurs Windows sont :

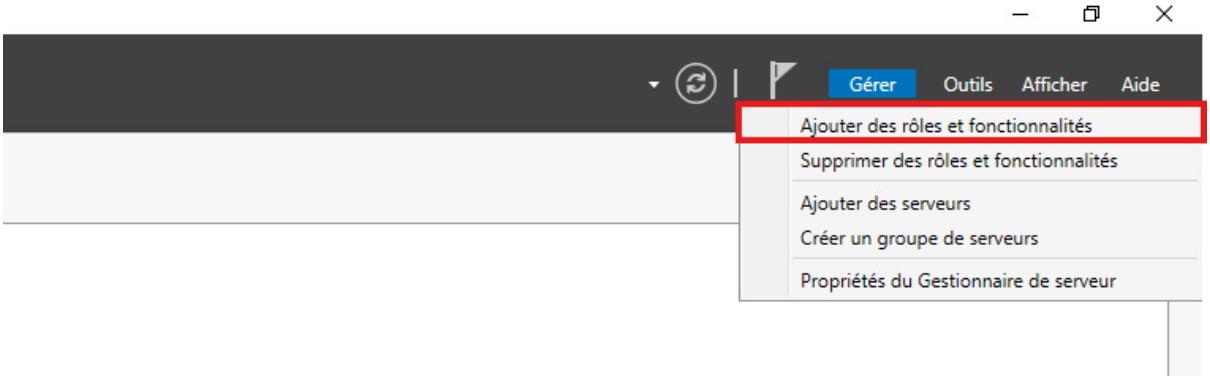
- CPU : pour vérifier l'utilisation du processeur et détecter toute surcharge pouvant ralentir les applications.
- Memory : pour surveiller l'utilisation de la mémoire vive et anticiper les risques de saturation.

- Swap : pour contrôler l'usage de la mémoire virtuelle et éviter que le serveur ne ralentisse en cas de forte charge.
- Ping : pour vérifier la connectivité réseau et détecter toute indisponibilité du serveur.

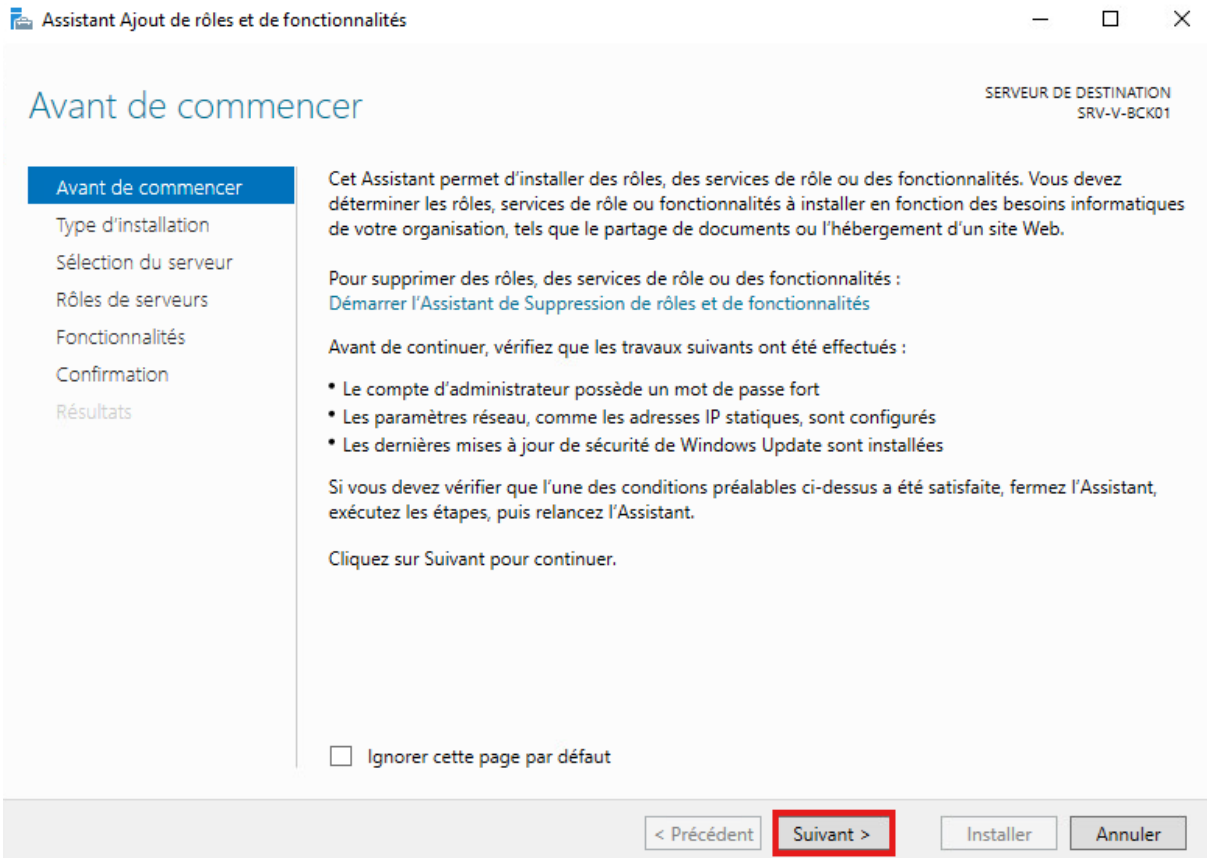
4.7.7.1.1. Configuration du serveur Windows à superviser

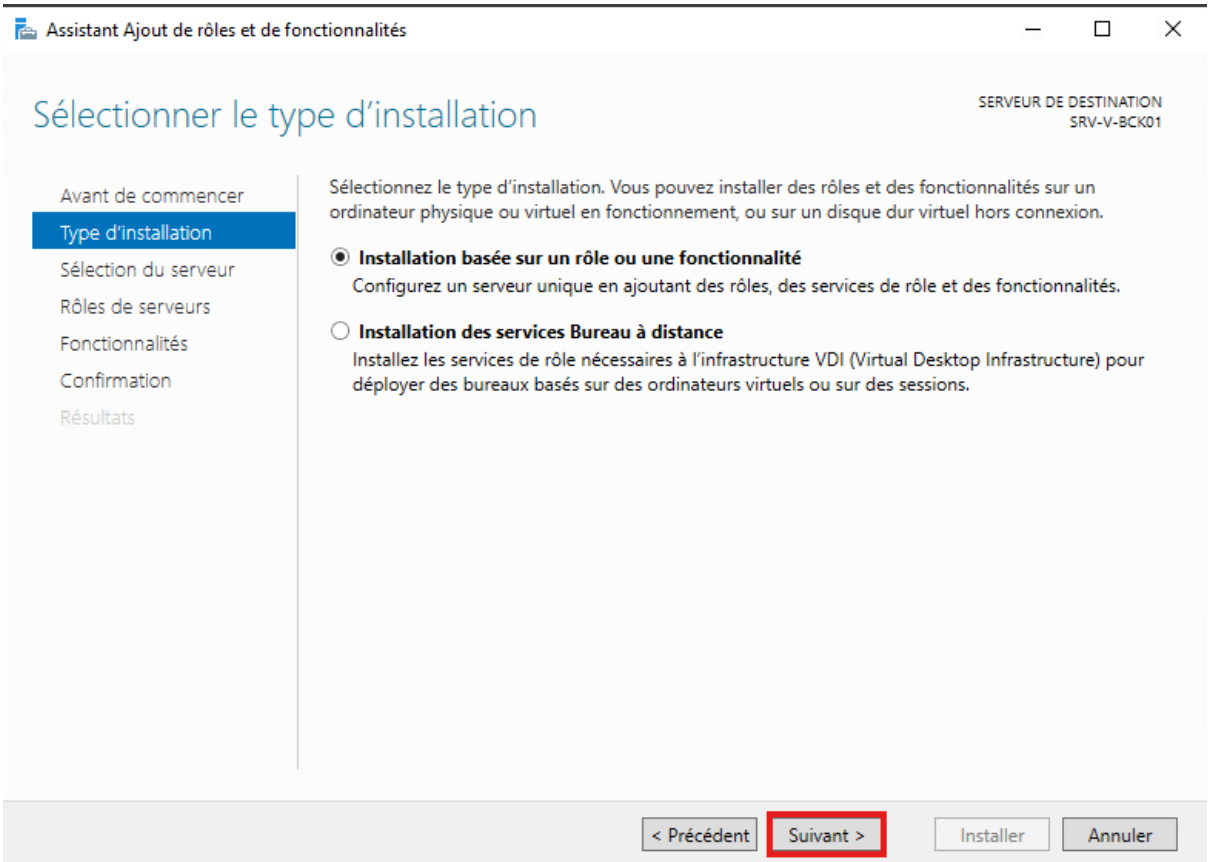
Dans un premier temps, afin de superviser un serveur Windows via Centreon, il est nécessaire d'activer et de configurer le service SNMP (Simple Network Management Protocol) sur le serveur.

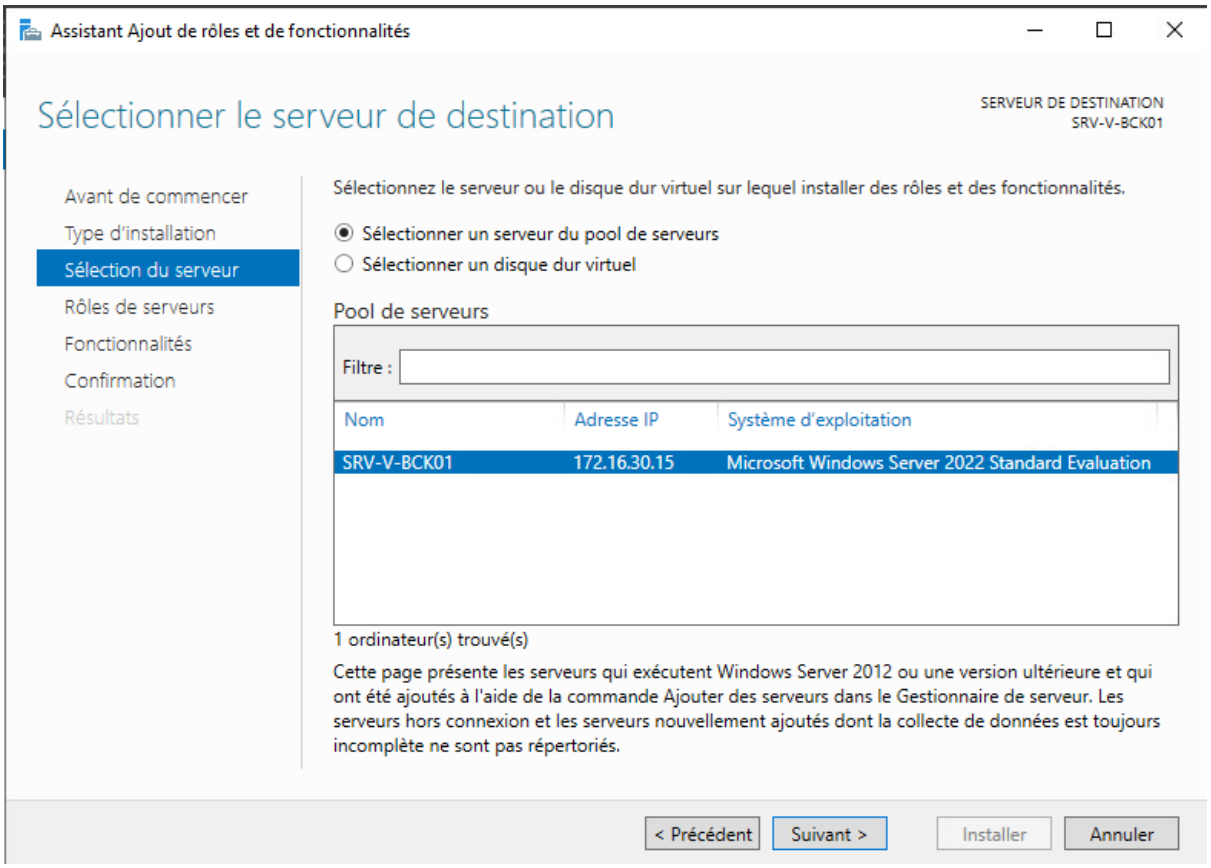
Dans le Gestionnaire de serveur, se diriger vers Gérer, puis cliquer sur Ajouter des rôles et fonctionnalités.

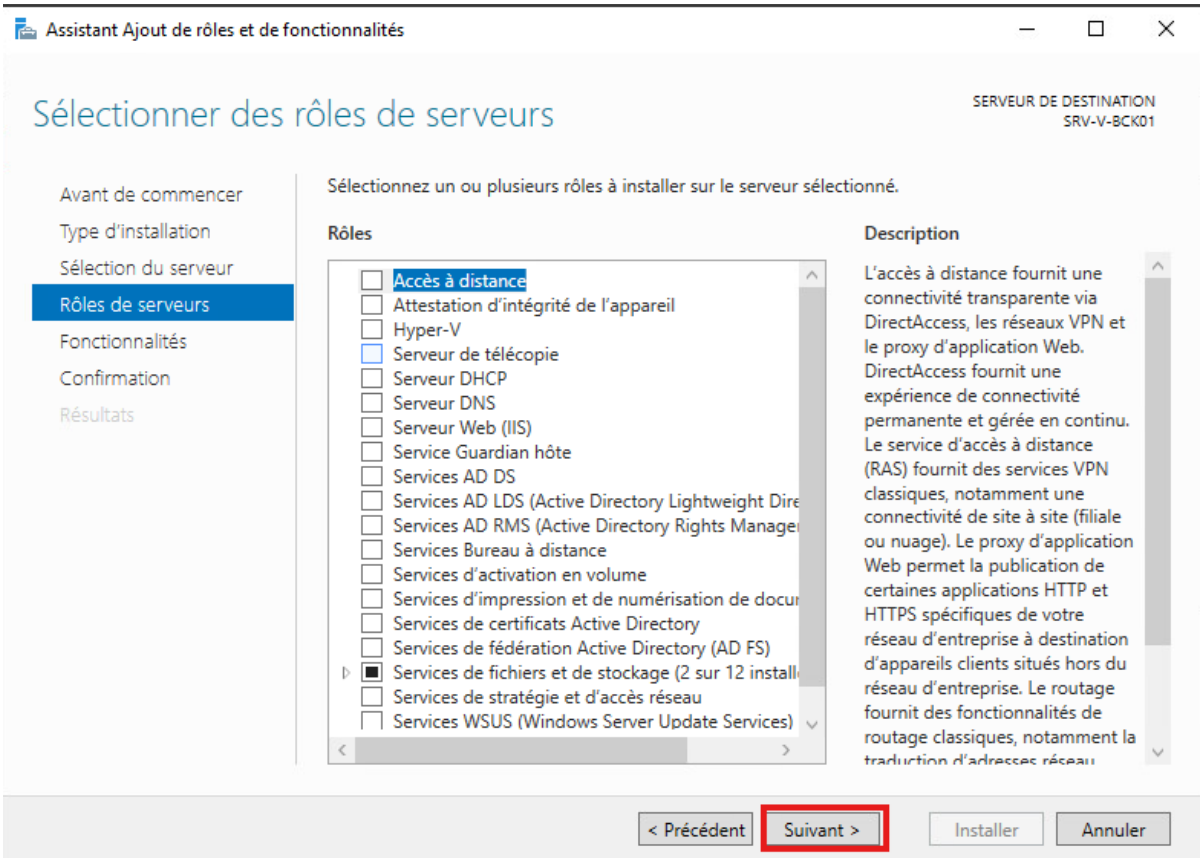


Suivre l'assistant en cliquant sur Suivant jusqu'à atteindre l'étape Sélectionner des fonctionnalités.

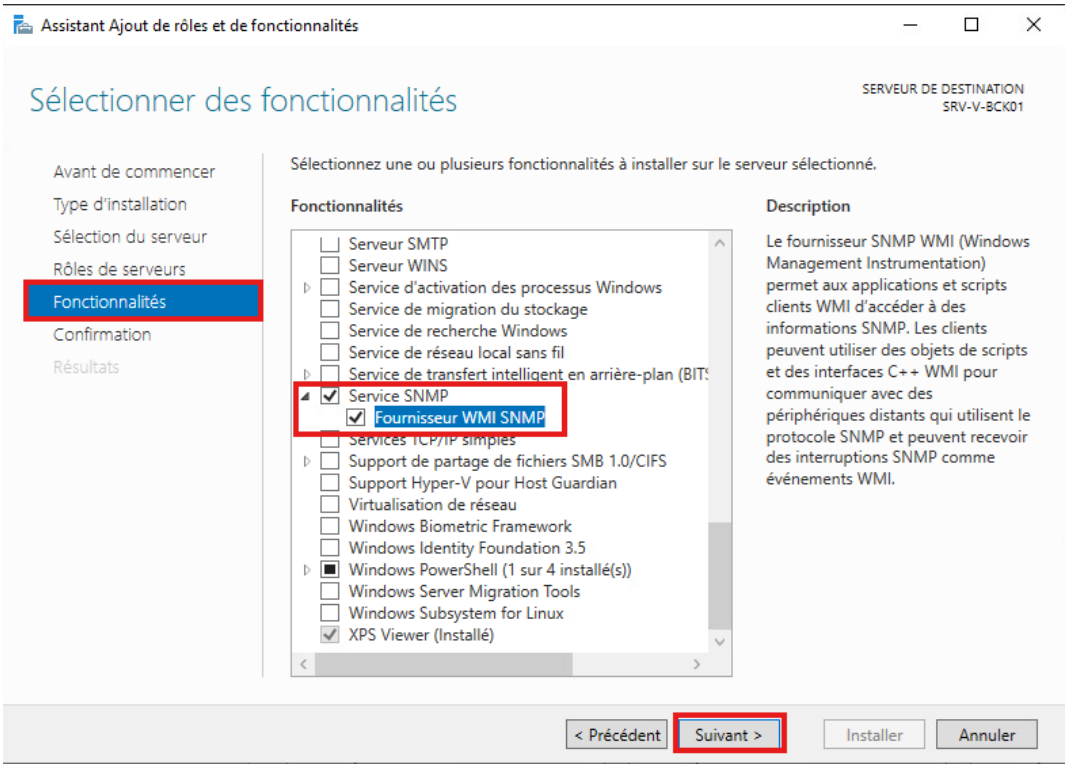

Assistant Ajout de rôles et de fonctionnalités
Avant de commencer
SERVEUR DE DESTINATION
SRV-V-BCK01
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.
Pour supprimer des rôles, des services de rôle ou des fonctionnalités :
Démarrer l'Assistant de Suppression de rôles et de fonctionnalités
Avant de continuer, vérifiez que les travaux suivants ont été effectués :
• Le compte d'administrateur possède un mot de passe fort
• Les paramètres réseau, comme les adresses IP statiques, sont configurés
• Les dernières mises à jour de sécurité de Windows Update sont installées
Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.
Cliquez sur Suivant pour continuer.
Ignorer cette page par défaut
< Précédent
Suivant >
Installer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Sélectionner le type d'installation
SERVEUR DE DESTINATION
SRV-V-BCK01
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.
Installation basée sur un rôle ou une fonctionnalité
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
Installation des services Bureau à distance
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.
< Précédent
Suivant >
Installer
Annuler

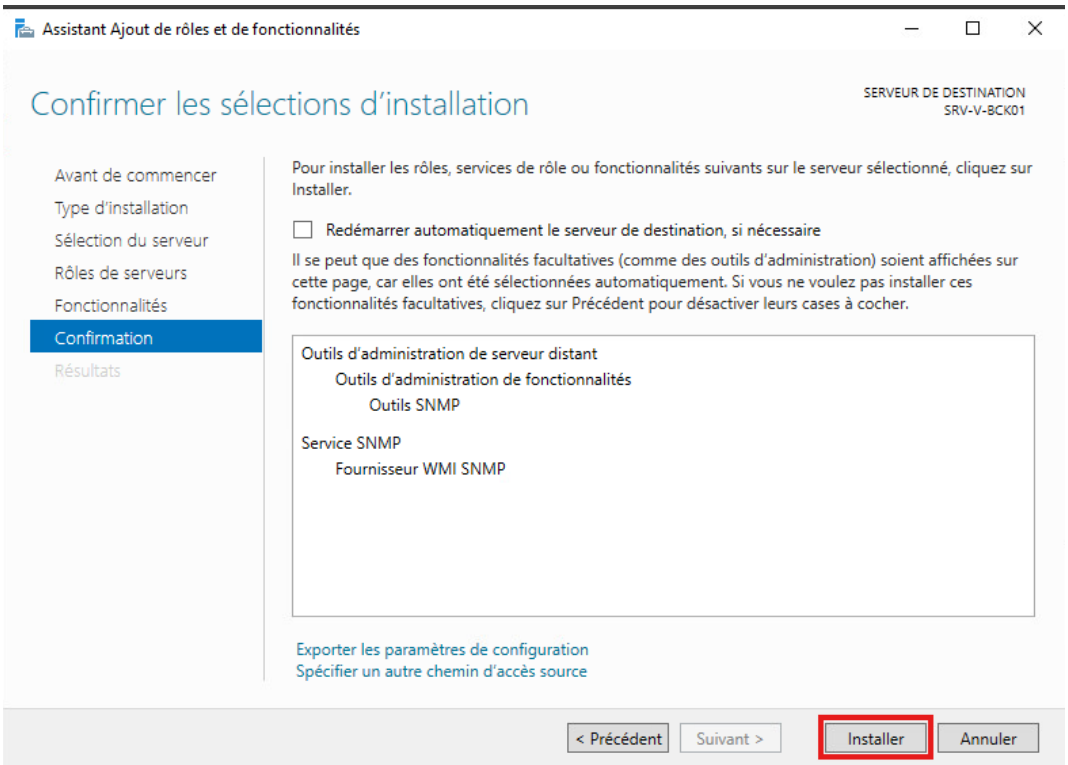

Assistant Ajout de rôles et de fonctionnalités
Sélectionner le serveur de destination
SERVEUR DE DESTINATION
SRV-V-BCK01
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.
Sélectionner un serveur du pool de serveurs
Sélectionner un disque dur virtuel
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d'exploitation
SRV-V-BCK01
172.16.30.15
Microsoft Windows Server 2022 Standard Evaluation
1 ordinateur(s) trouvé(s)
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.
< Précédent
Suivant >
Installer
Annuler

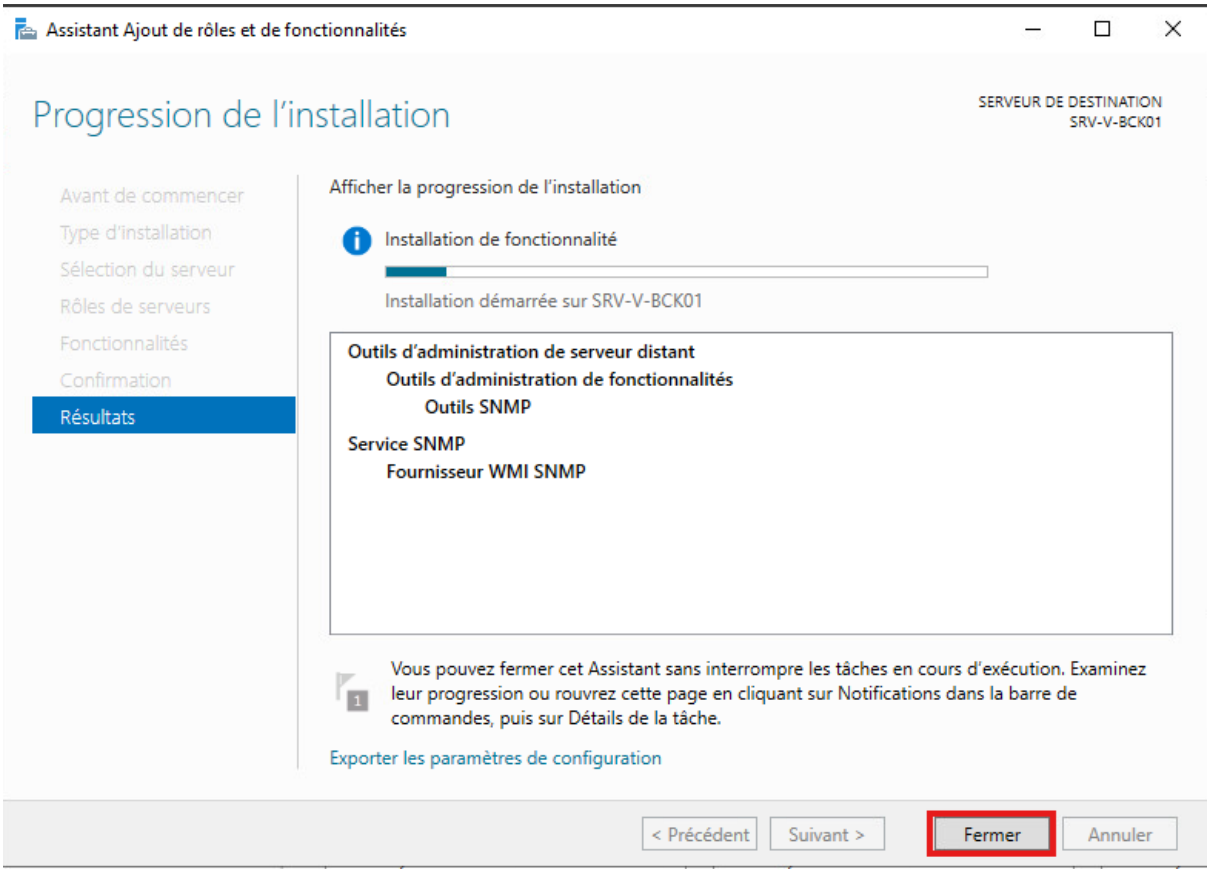

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
SRV-V-BCK01
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Description
Accès à distance
Attestation d'intégrité de l'appareil
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Service Guardian hôte
Services AD DS
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume
Services d'impression et de numérisation de docu
Services de certificats Active Directory
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (2 sur 12 install
Services de stratégie et d'accès réseau
Services WSUS (Windows Server Update Services)
L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et gérée en continu. Le service d'accès à distance (RAS) fournit des services VPN classiques, notamment une connectivité de site à site (filiale ou nuage). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la
< Précédent
Suivant >
Installer
Annuler

Une fois arrivé à l'étape Sélectionner des fonctionnalités, cocher la case Service SNMP ainsi que Fournisseur WMI SNMP. Ces composants permettent à Centreon de collecter les informations système et réseau du serveur Windows via SNMP et WMI, ce qui est essentiel pour superviser les métriques telles que CPU, mémoire, swap et connectivité réseau.

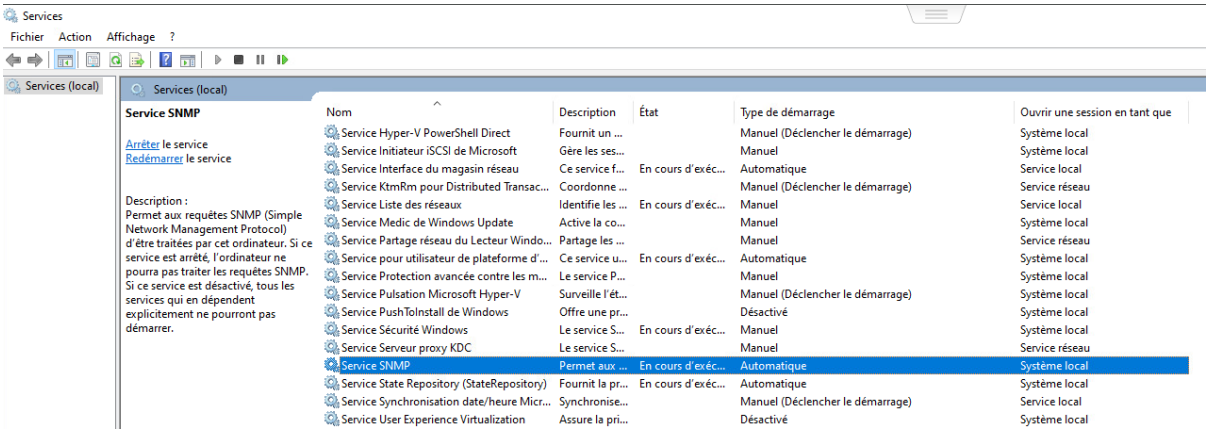


Installer les différentes fonctionnalités sélectionnées précédemment.

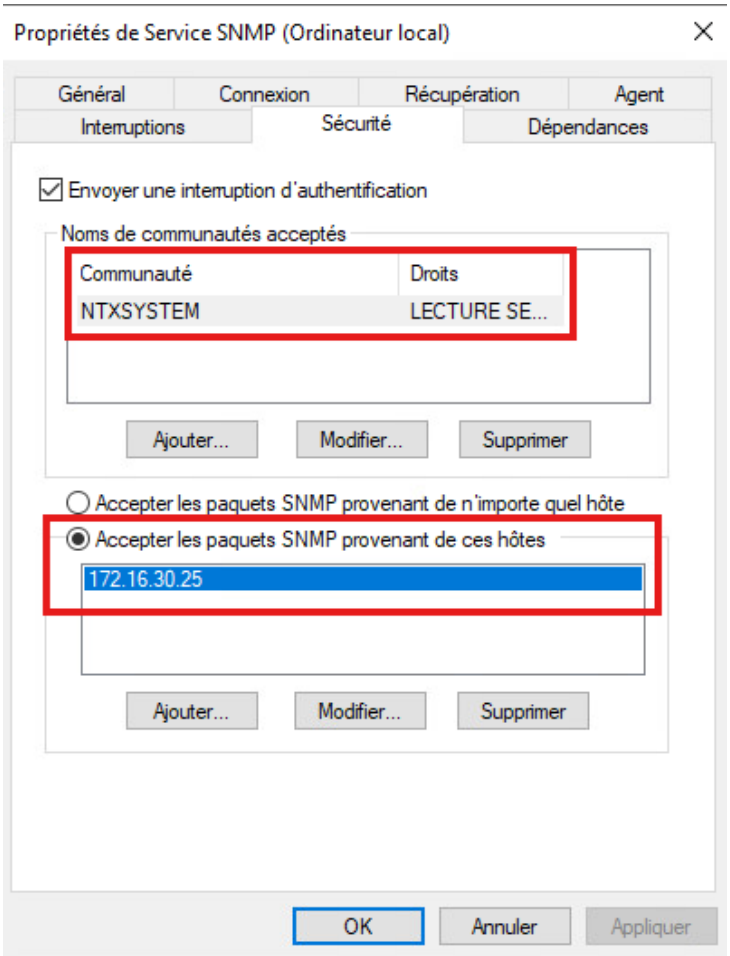




Une fois l'installation terminée, accéder à la console Services de Windows afin de configurer le service SNMP.



Dans les propriétés du service SNMP, ouvrir l'onglet Sécurité.

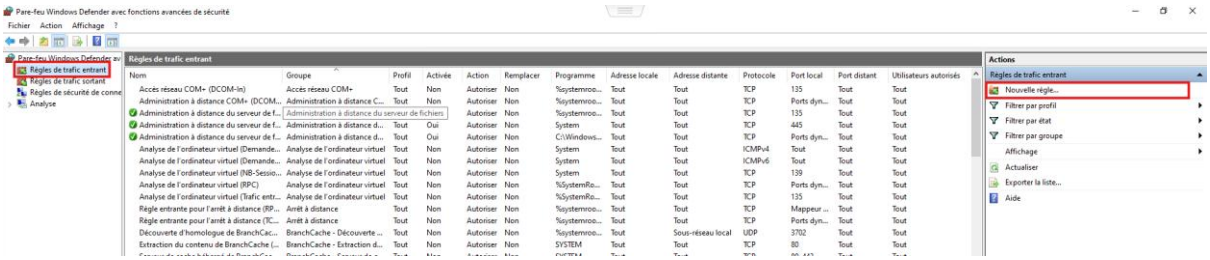


À cette étape, il est nécessaire de définir le nom de la communauté SNMP acceptée (par exemple : NTXSYSTEM). Configurer les autorisations associées à cette communauté pour nous lecture seule. Et restreindre la réception des paquets SNMP uniquement à l'adresse IP du poller Centreon auquel le serveur est rattaché.

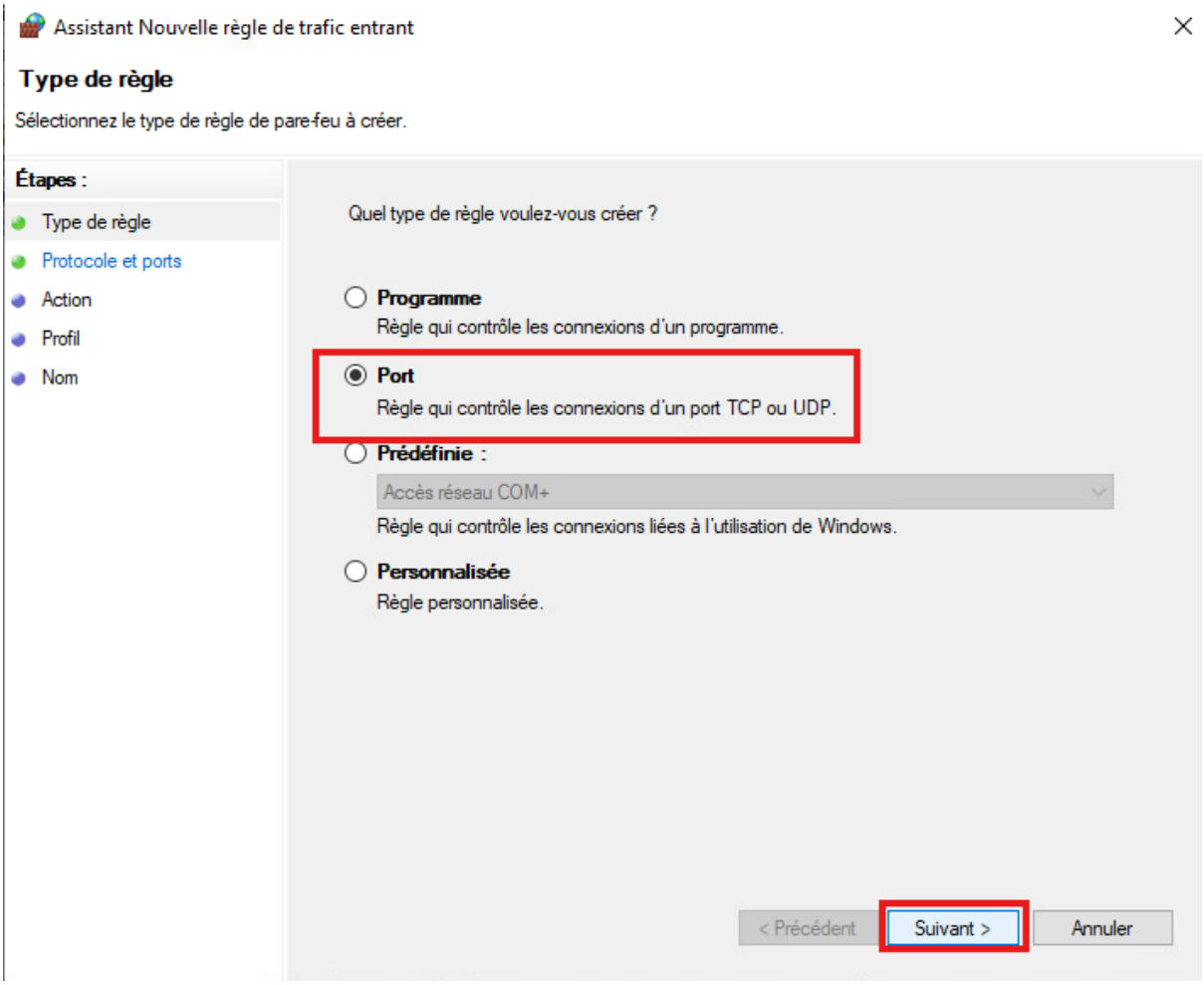
Cette configuration permet de sécuriser les échanges SNMP en limitant les requêtes aux équipements autorisés, tout en assurant la bonne communication entre le serveur Windows et le poller de supervision.

Dans un second temps, il est nécessaire de créer une règle dans le pare-feu Windows afin d'autoriser les communications SNMP.

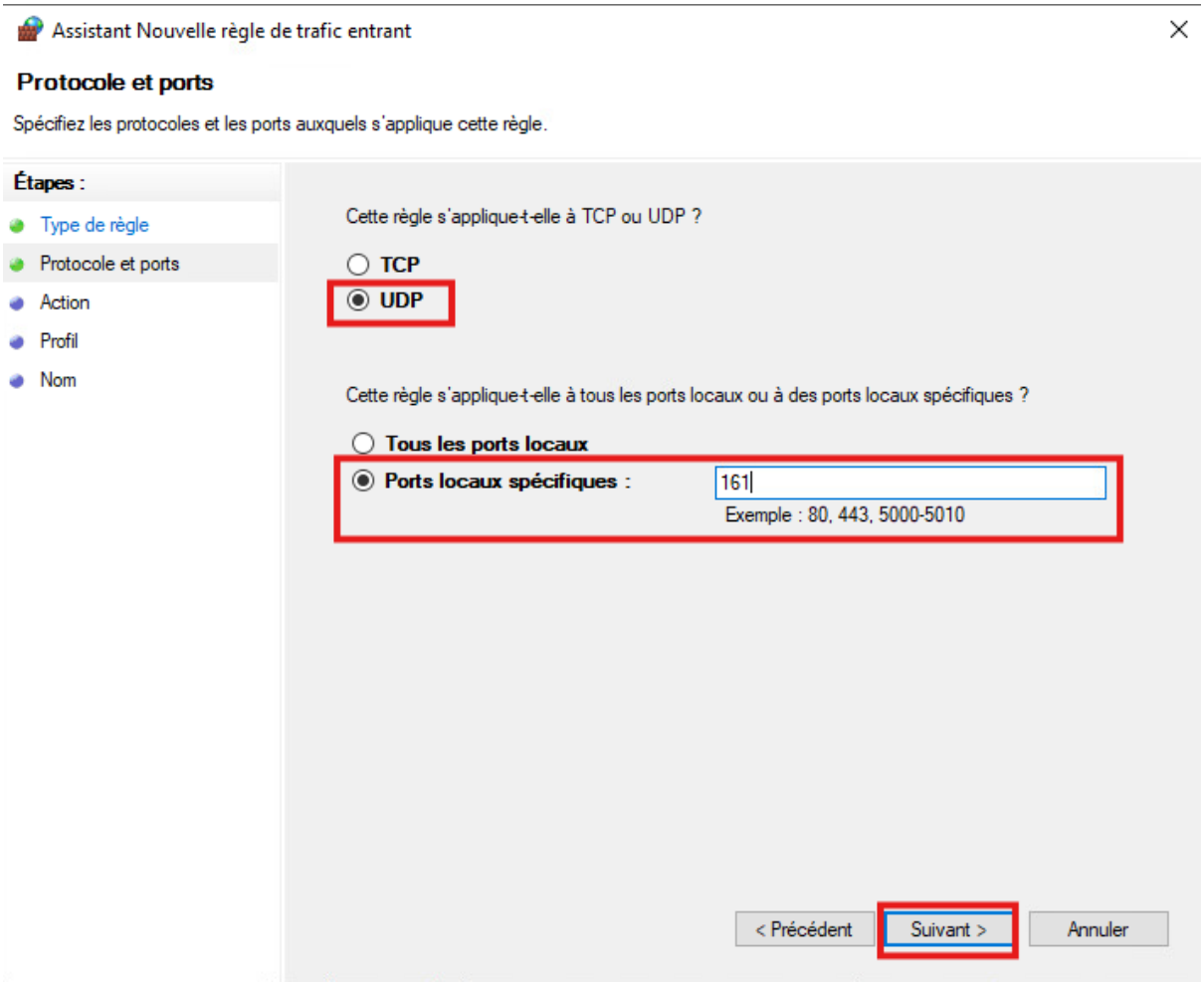
Pour cela, se rendre dans Pare-feu Windows Defender avec fonctions avancées de sécurité, puis accéder à Règles de trafic entrant et cliquer sur Nouvelle règle.



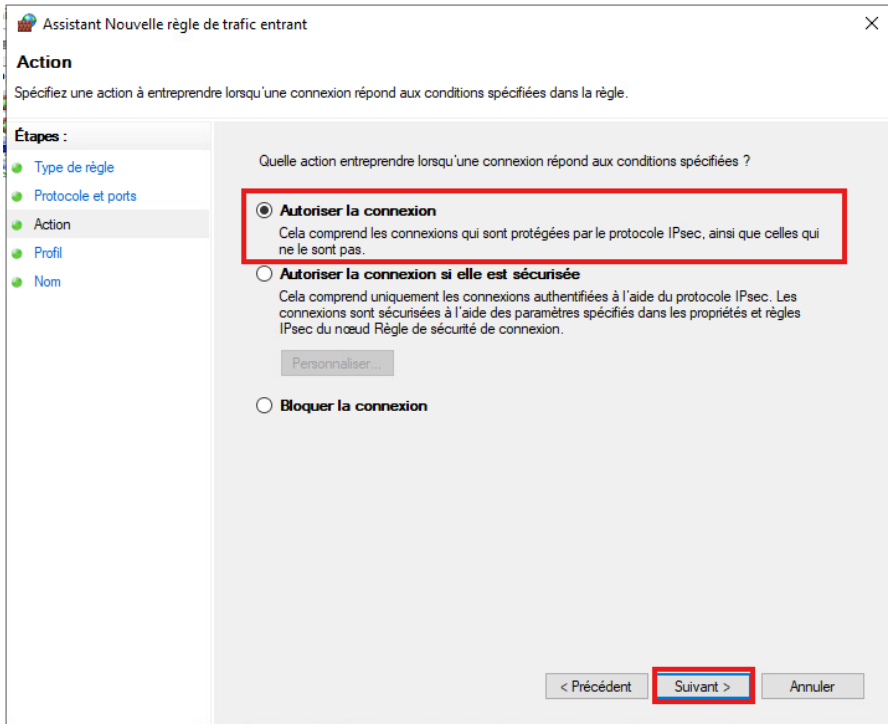
Ensuite sélectionner le type de règle Port :



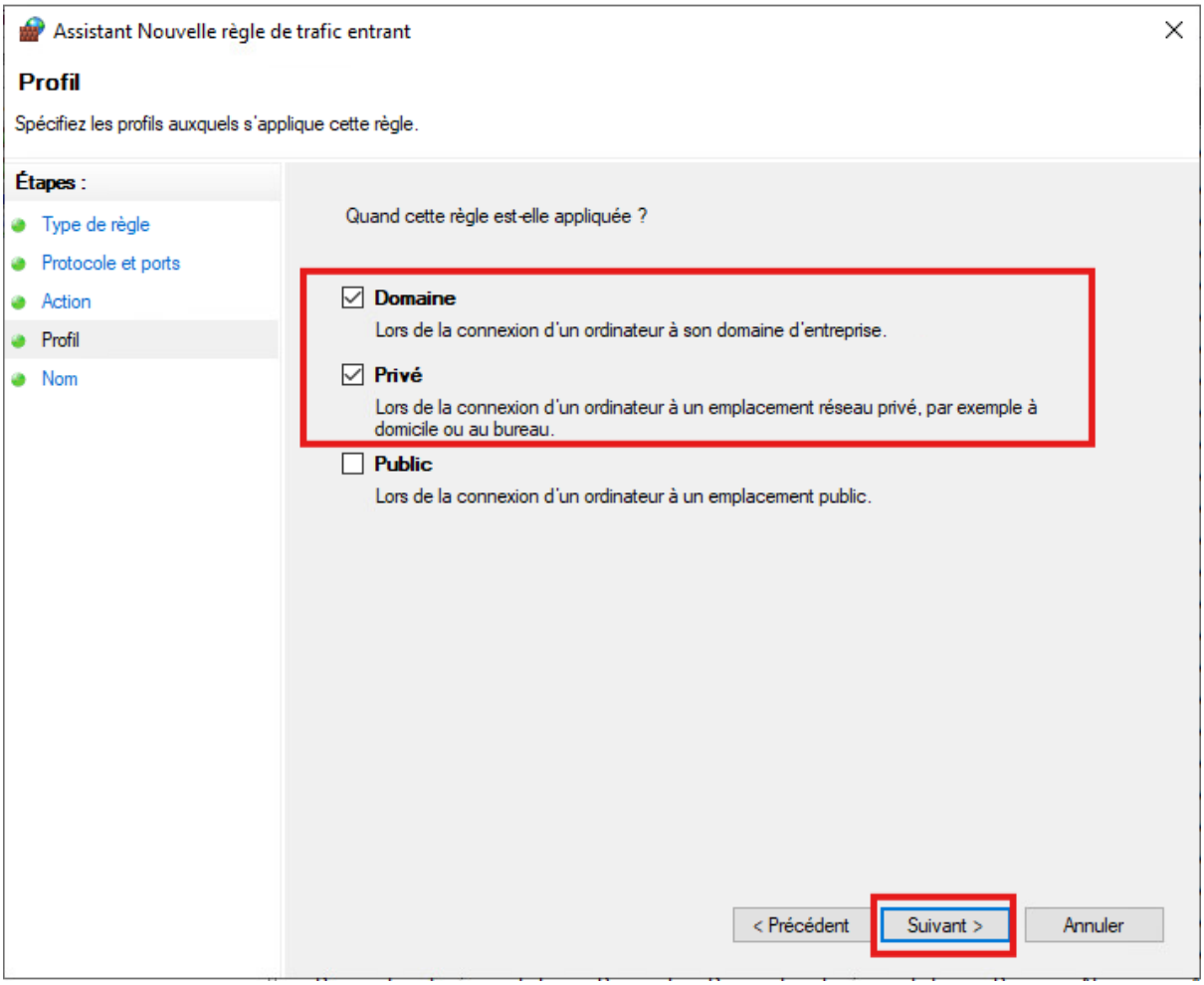
Choisir le protocole UDP (User Datagram Protocol) et spécifier le port 161, utilisé par le protocole SNMP :



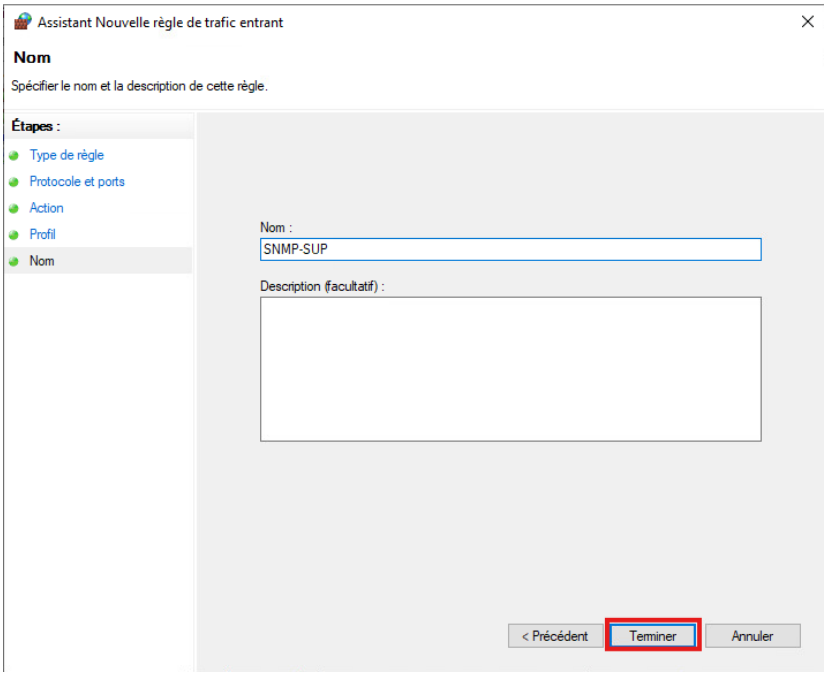
Autoriser la connexion :



Appliquer la règle aux profils Domaine et Privé :

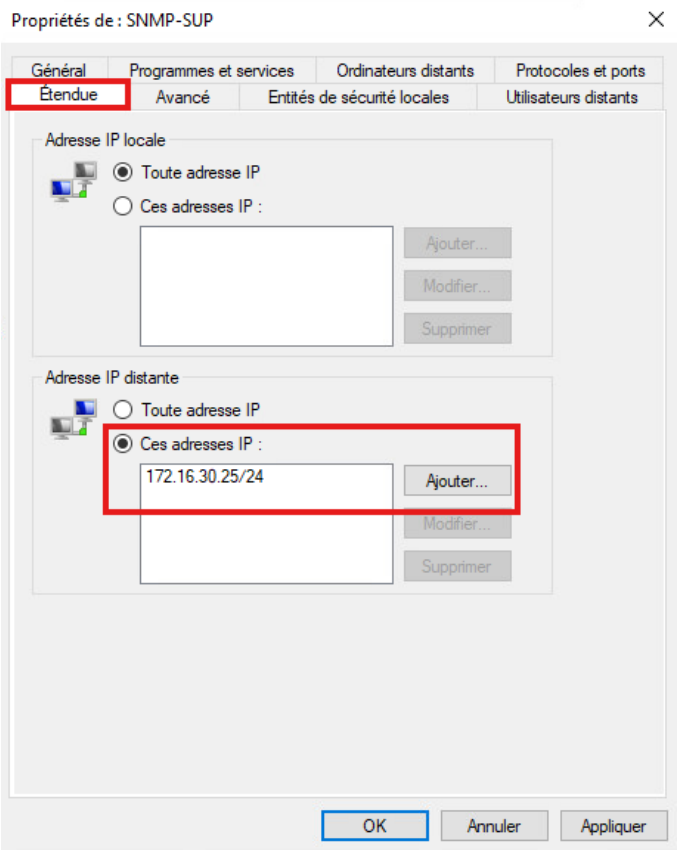


Pour terminer, attribuer un nom explicite à la règle afin de l'identifier facilement par la suite.



Une fois la règle créée, je me rends dans ses propriétés, puis dans l'onglet Étendue.

Dans la partie Adresse IP distante, j'ajoute l'adresse IP du poller Centreon auquel le serveur est rattaché.



La configuration du serveur Windows est désormais terminée.

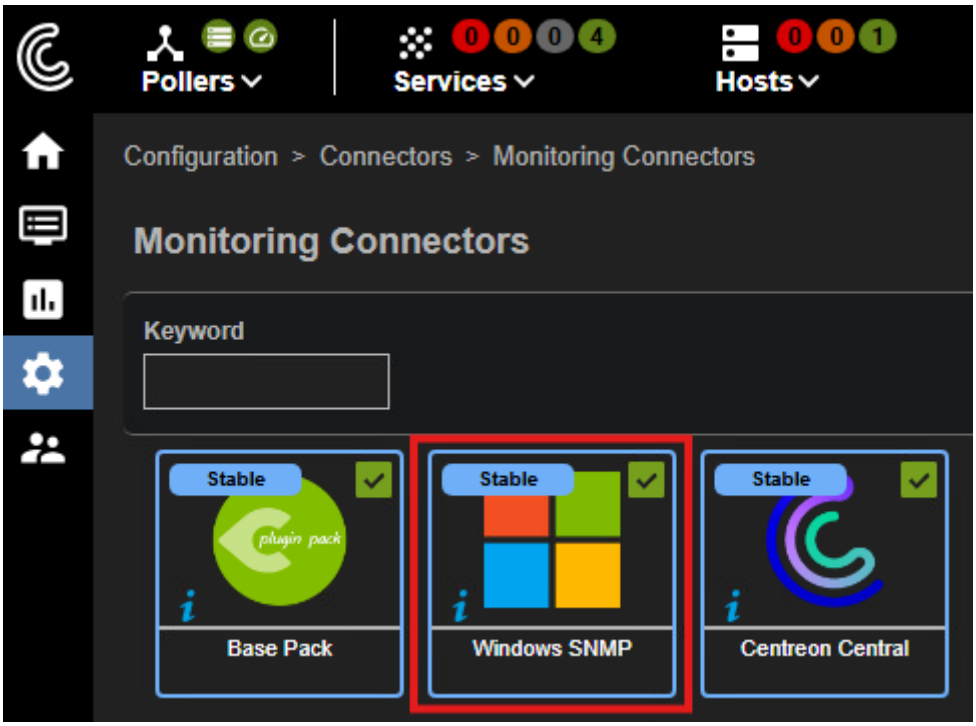
Je peux maintenant passer à l'étape suivante, qui consiste à effectuer la configuration directement dans l'interface web de Centreon afin d'ajouter le serveur en tant qu'hôte.

4.7.7.1.2. Configuration dans l'interface Centreon

Tout d'abord, je dois ajouter le connecteur de supervision nécessaire pour superviser un serveur Windows via SNMP.

Pour cela, je me rends dans l'interface web de Centreon, puis dans le menu Configuration > Connectors > Monitoring Connectors. À cette étape, je vérifie que le connecteur Windows SNMP est bien installé. Si ce n'est pas le cas, je l'ajoute.

Ce connecteur permet d'utiliser les commandes et templates prédéfinis nécessaires pour superviser les ressources système telles que le CPU, la mémoire, le swap ou encore la connectivité réseau.

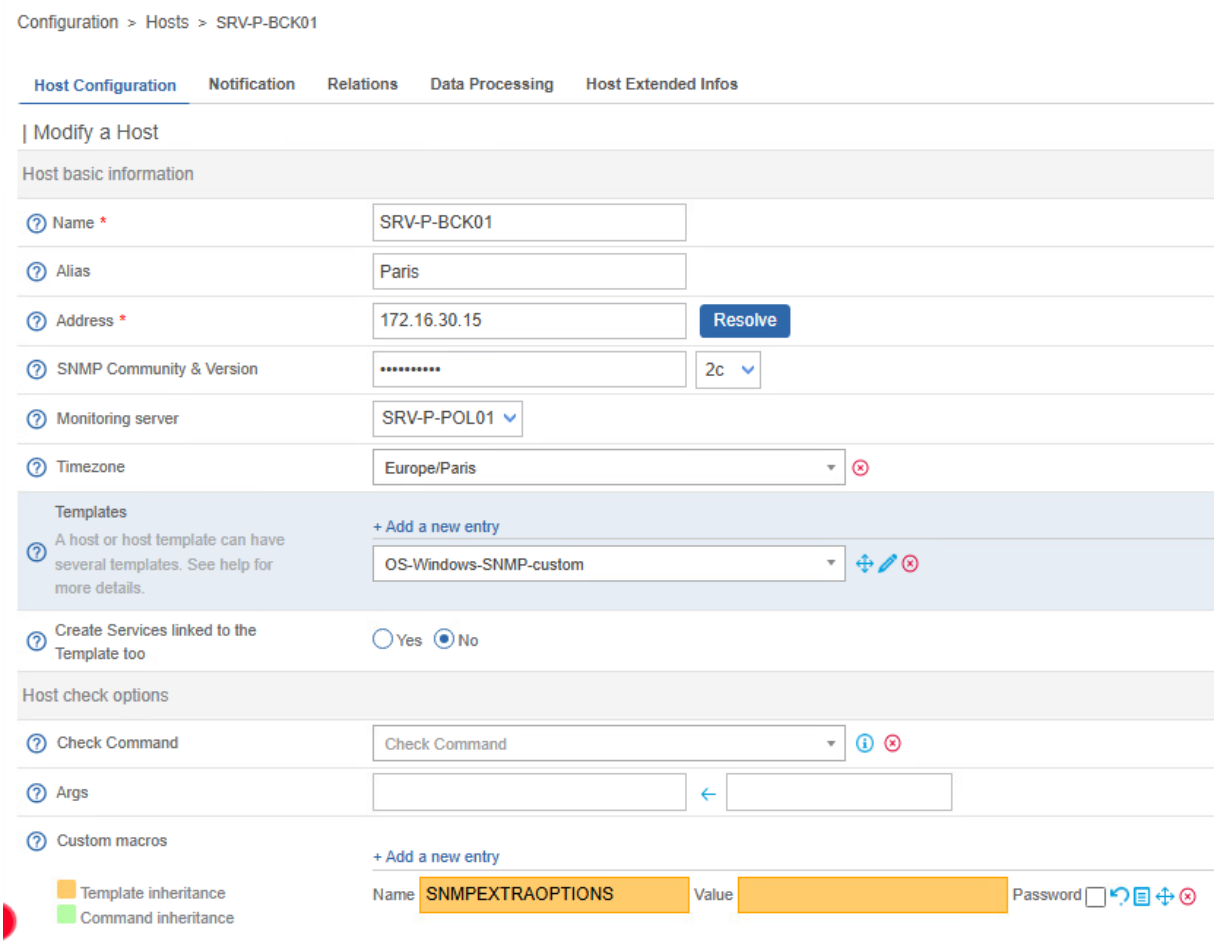


Ensuite, je me rends dans le menu Configuration > Hosts > Hosts, puis je clique sur Ajouter afin de créer un nouvel hôte.

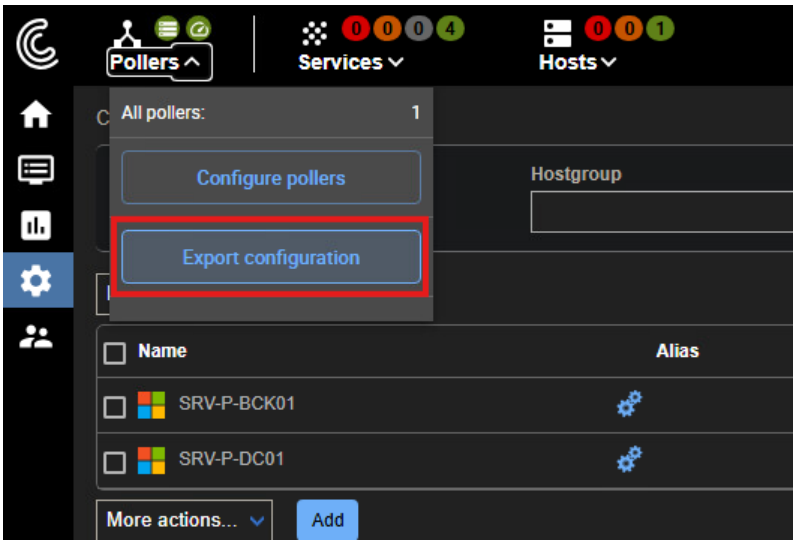
Je renseigne les différentes informations nécessaires :

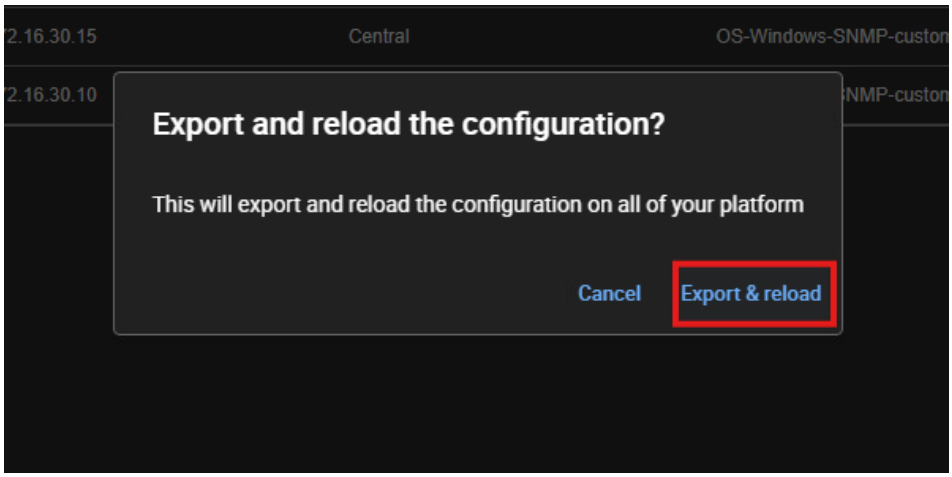
- Nom de l'hôte : nom de la machine à superviser
- Alias : nom plus explicite pour l'identifier facilement (par exemple Serveur Paris, puisqu'il est situé sur le site de Paris)
- Adresse IP : adresse IP du serveur Windows
- Communauté SNMP : identique à celle configurée précédemment sur le serveur Windows
- Monitoring server : je sélectionne le Poller de Paris, car le serveur se trouve sur ce site
- Template : j'associe le modèle OS-Windows-SNMP-custom afin de superviser automatiquement les services principaux (CPU, Memory, Swap, Ping).

L'utilisation du template permet d'appliquer automatiquement un ensemble de services et de seuils prédéfinis, ce qui facilite la configuration et garantit une supervision cohérente sur l'ensemble des serveurs Windows.



Pour terminer la configuration, je me rends dans le menu Poller > Exporter configuration. Cette opération permet à Centreon de générer automatiquement la configuration et de l'envoyer directement vers le poller concerné (ici, le poller de Paris).





Une fois l'export effectué, le poller applique la configuration et commence à superviser le serveur Windows. Après quelques minutes, les services configurés (CPU, Memory, Swap et Ping) apparaissent dans l'interface avec leur état, ce qui confirme que la supervision est opérationnelle.

Status	Resource	Parent	G	Duration	Last check	Information
OK	Swap	SRV-P-BCK01		4h 17m	2m 44s	OK: Swap Total: 13.81 GB Used: 7.16 GB (51.82%) Free: 6.65 GB (48.18%)
OK	Ping	SRV-P-BCK01		4h 21m	1m 26s	OK - 172.16.30.15: rta 0,311ms, lost 0%
OK	Cpu	SRV-P-BCK01		4h 23m	3m 20s	OK: 4 CPU(s) average usage is 4.00 %
OK	Memory	SRV-P-BCK01		4h 25m	10m 14s	OK: Ram Total: 12.00GB Used: 6.14GB (51.20%) Free: 5.86GB (48.80%)
Up	SRV-P-BCK01			4h 26m	4m 7s	OK - 172.16.30.15: rta 0,535ms, lost 0%

4.7.7.2. Supervision d'un serveur Windows Core

Pour superviser un serveur Windows Core, l'installation et la configuration se font en ligne de commande, via PowerShell, car cette version de Windows ne dispose pas d'interface graphique.

4.7.7.2.1. Configuration du serveur Windows Core à superviser

La première étape consiste à installer le service SNMP et le fournisseur WMI SNMP. Je procède de la manière suivante :

```
Install-WindowsFeature SNMP-Service, SNMP-WMI-Provider
```

Ensuite, je vérifie que le service SNMP est bien installé :

```
Get-Service SNMP
```

Puis je démarre le service et configure son démarrage automatique :

```
Start-Service SNMP

Set-Service SNMP -StartupType Automatic
```

Configuration de la communauté SNMP :

Pour que Centreon puisse récupérer les informations du serveur, je configure la communauté SNMP NTXSYSTEM en lecture seule :

```
reg add
"HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities" /v
NTXSYSTEM /t REG_DWORD /d 4 /f
```

Je restreins ensuite l'accès SNMP uniquement au poller qui supervisera ce serveur (ici, le poller de Nantes, IP : 172.19.30.25) :

```
reg add
"HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers" /v
1 /t REG_SZ /d 172.19.30.25 /f
```

Enfin, je redémarre le service pour que les modifications soient prises en compte :

```
Restart-Service SNMP
```

Configuration du pare-feu :

Il est nécessaire d'autoriser le trafic SNMP entrant sur le port UDP 161 depuis le poller. Je crée donc une règle dans le pare-feu Windows :

- Nom : SNMP-SUP
- Direction : Entrante
- Protocole : UDP
- Port : 161
- Profils : Domaine + Privé
- Adresse IP distante autorisée : 172.19.30.25/24

La commande PowerShell pour créer cette règle est la suivante :

```
New-NetFirewallRule `

-DisplayName "SNMP-SUP" `

-Direction Inbound `

-Protocol UDP `

-LocalPort 161 `

-RemoteAddress 172.19.30.25/24 `

-Profile Domain,Private `

-Action Allow
```

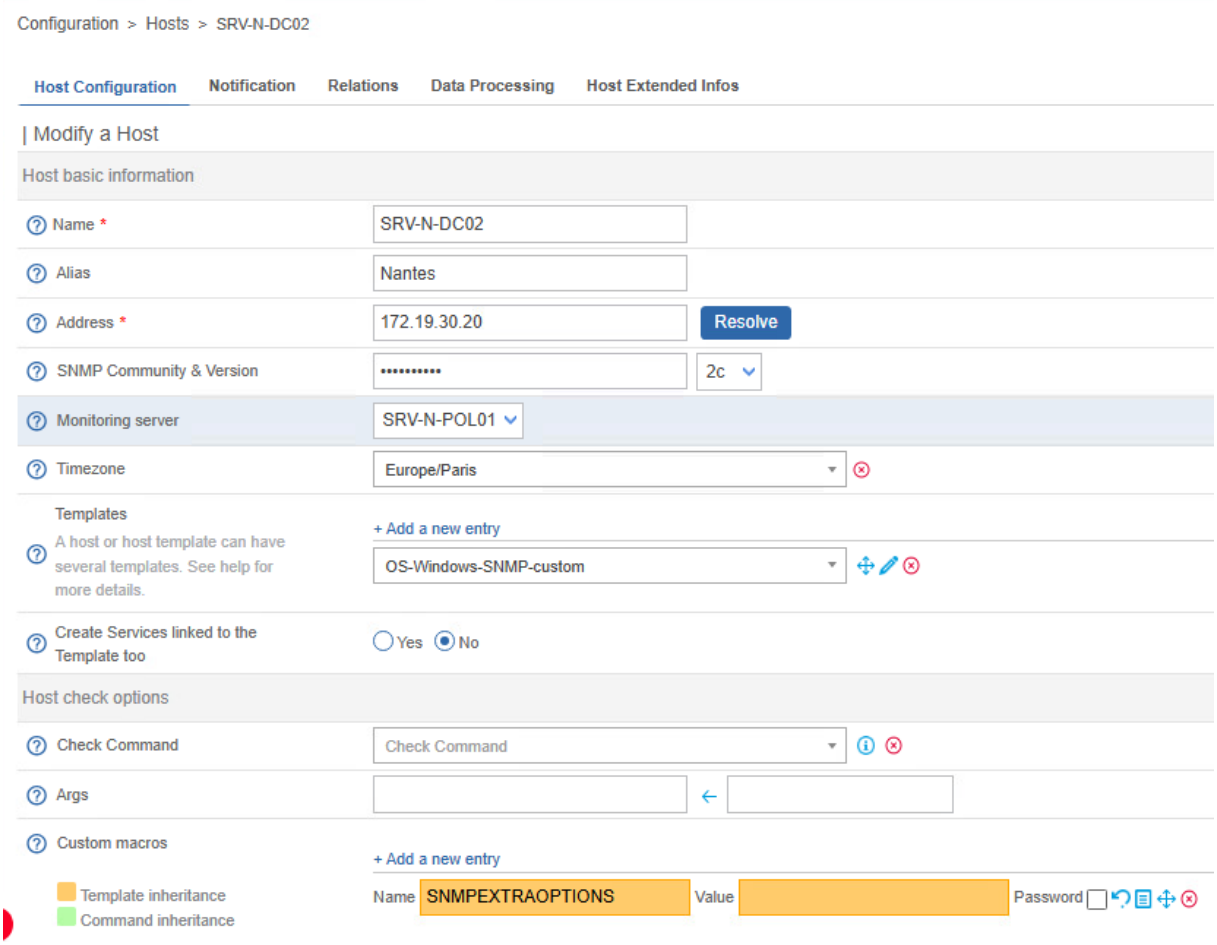
Vérification :

Pour s’assurer que la configuration est correcte je vérifie la règle du pare-feu avec la commande :

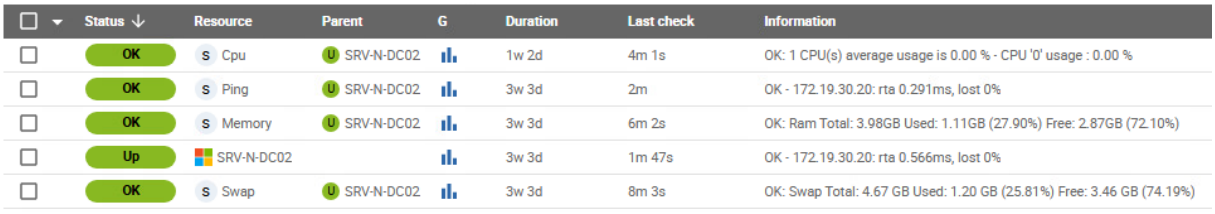
```
Get-NetFirewallRule -DisplayName "SNMP-SUP"
```

4.7.7.2.2. Configuration dans l’interface Centreon

Même configuration et fonctionnalité que pour le Windows avec interface graphique voici un exemple du SRV-N-DC02 qui est un serveur en Windows Core.



Voici la remontée des sondes :



4.7.7.3. Supervision d'un serveur Linux (Debian)

Dans le cadre de la mise en supervision des serveurs linux, j'ai mis en place le service SNMP (Simple Network Management Protocol). Ce protocole me permet de surveiller à distance l'état du serveur (charge CPU, mémoire, disque, ping, etc.) depuis notre outil de supervision Centreon.

4.7.7.3.1. Configuration du serveur Linux à superviser

Mise à jour du système :

Avant toute installation, j'ai commencé par mettre à jour les paquets du serveur afin d'éviter les problèmes de dépendances :

Commande qui permet de mettre à jour la liste des paquets disponibles dans les dépôts :

```
apt update
```

Installation du service SNMP :

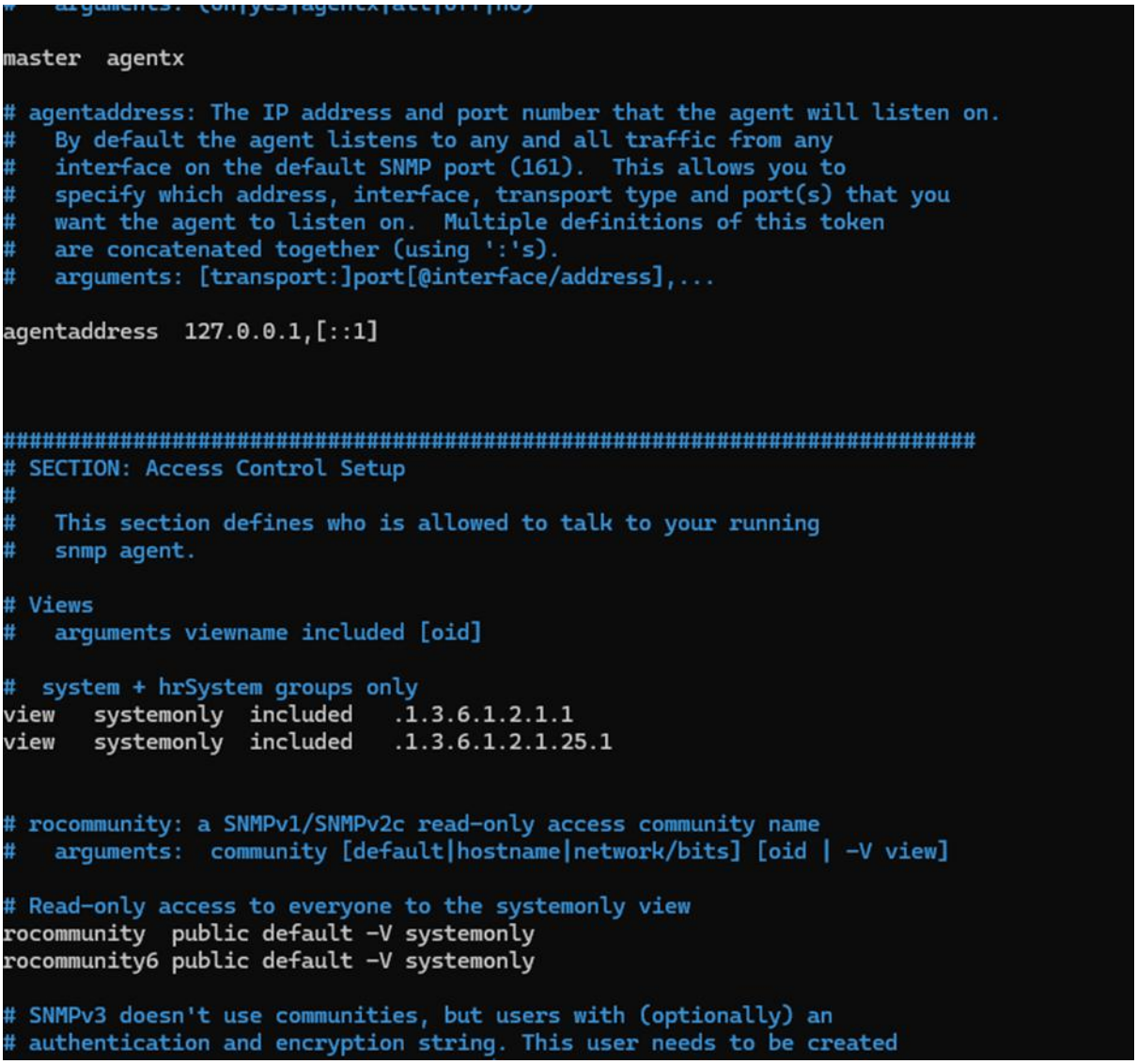
Ensuite, j'ai installé les paquets nécessaires : `apt install snmp snmpd`

- snmp : outils clients permettant de tester SNMP
- snmpd : démon SNMP (le service qui tourne sur le serveur)

Sauvegarde de la configuration d'origine :

Avant toute modification, j'ai sauvegardé le fichier de configuration original pour pouvoir revenir en arrière en cas d'erreur :

```
cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.orig
```



Cela me permet de restaurer la configuration par défaut si nécessaire.

Modification de la configuration SNMP :

J'ai ensuite modifié le fichier de configuration :

```
nano /etc/snmp/snmpd.conf
```

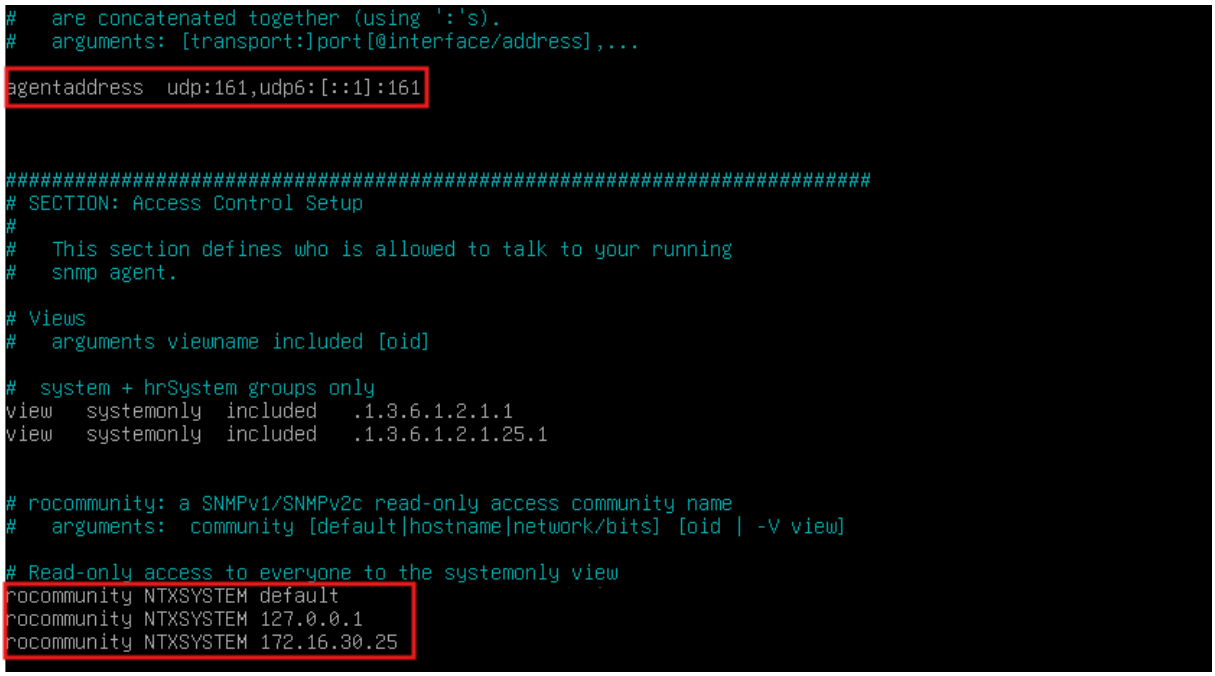
Configuration ajoutée/modifiée :

```
agentAddress udp:161,udp6:[::1]:161

rocommunity NTXSYSTEM default

rocommunity NTXSYSTEM 127.0.0.1

rocommunity NTXSYSTEM 172.16.30.25
```



Explication des paramètres :

agentAddress udp:161 : Définit le port d'écoute SNMP (port 161 en UDP). C'est le port standard utilisé par SNMP.

rocommunity NTXSYSTEM default : Définit une communauté SNMP en lecture seule (read-only). Ici, NTXSYSTEM est la chaîne d'authentification utilisée.

rocommunity NTXSYSTEM 127.0.0.1 : Autorise les requêtes SNMP depuis la machine locale.

rocommunity NTXSYSTEM 172.16.30.25 : Autorise les requêtes SNMP depuis l'adresse IP du serveur de supervision.

Redémarrage et activation du service :

Après modification, j'ai redémarré le service pour appliquer les changements :

```
systemctl restart snmpd
```

Puis j'ai activé le service pour qu'il démarre automatiquement au boot :

```
systemctl enable snmpd
```

Vérification du fonctionnement :

```
systemctl status snmpd
```

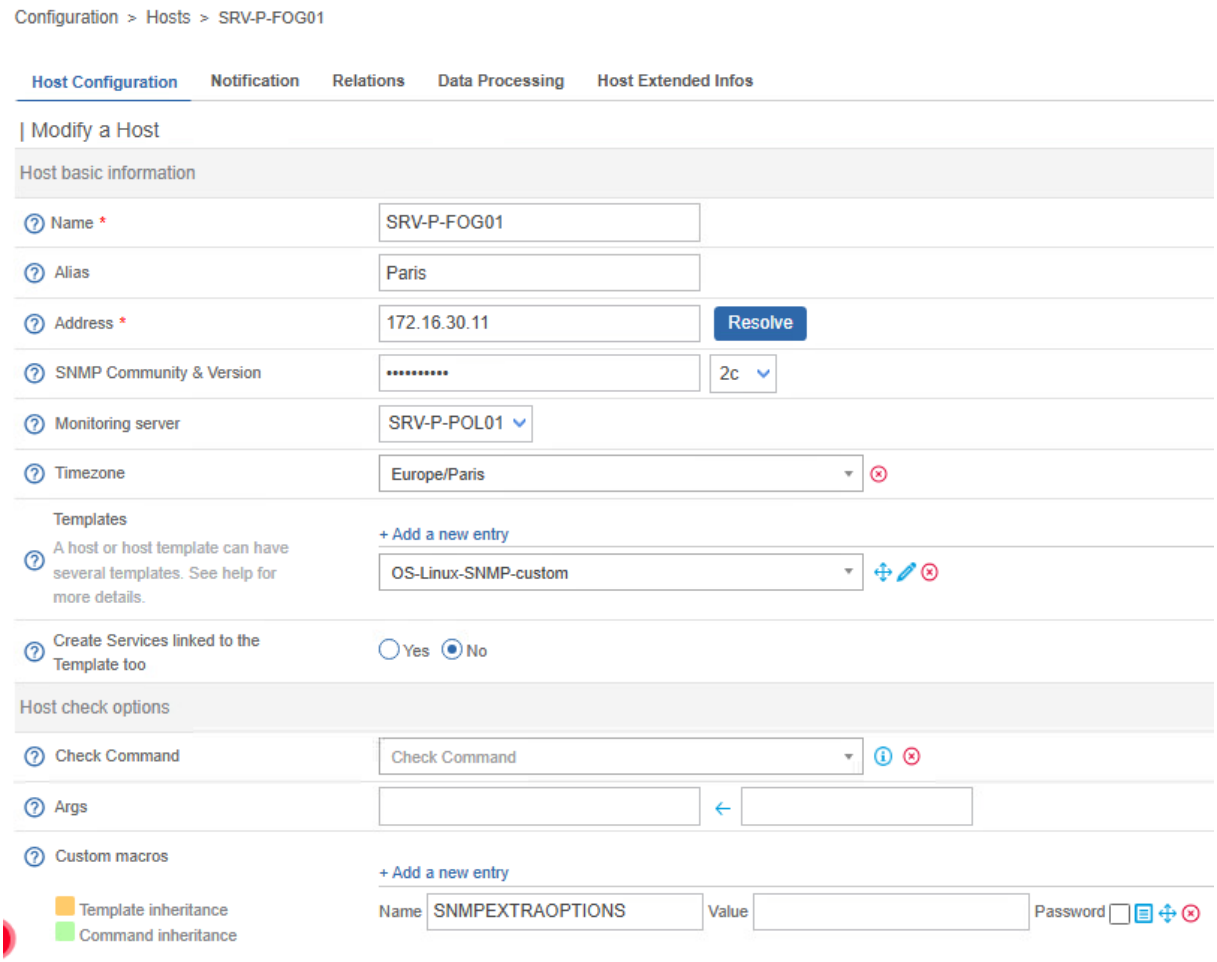
4.7.7.3.2. Configuration dans l'interface Centreon

Voici la configuration pour le serveur de FOG. Cet hôte correspond au serveur SRV-P-FOG01, localisé à Paris, avec l'adresse IP 172.16.30.11.

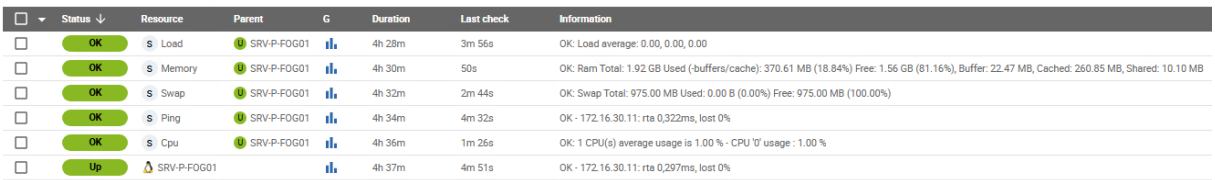
La supervision de cet équipement est réalisée via le protocole SNMP (version 2c), permettant de collecter des informations sur l'état et les performances du serveur.

Le serveur de supervision utilisé est SRV-P-POL01, qui joue le rôle de poller chargé d'exécuter les contrôles et de récupérer les données de supervision.

Un template de supervision (OS-Linux-SNMP-custom) est appliqué à cet hôte. Ce modèle permet d'hériter automatiquement des paramètres et des services de supervision nécessaires pour surveiller un serveur Linux.



Ensuite exploration de la configuration, les statues des ressources remonte un à un.



4.7.7.4. Supervision d'un Switch (HP)

La supervision de nos switches passe par le protocole SNMP. Celui-ci a été configuré sur le switch HP ProCurve Switch 2610-48 afin de permettre sa supervision depuis Centreon. Cette opération doit être effectuée sur les deux switches de l'infrastructure.

4.7.7.4.1. Configuration du switch à superviser

1 - Configuration SNMP du switch HP :

Dans un premier temps création de la communauté SNMP :

Voici la commande :

```
snmp-server community "NTXSYSTEM" Operator
```

Explication:

NTXSYSTEM : Nom de la communauté SNMP (équivalent d'un mot de passe en v2c).

Operator : Niveau d'accès attribué à la communauté.

Sur les switches HP, les niveaux sont généralement :

- Operator : accès en lecture seule (read-only)
- Manager : accès lecture/écriture (read-write)

Ici, la supervision peut consulter les informations du switch, mais ne peut pas modifier la configuration.

Dans le show snmp-server, on voit :

```
SW-P-02(config)# show snmp-server

 SNMP Communities

  Community Name   MIB View Write Access
  ---------------- -------- ------------
  NTXSYSTEM        Operator Restricted
```

La communauté est bien créée et l'accès en écriture est restreint (pas de modification possible).

2 - Configuration de l'envoi des traps SNMP

Voici la commande :

```
snmp-server host 172.16.30.25 "NTXSYSTEM"
```

Explication :

Cette commande configure le switch pour envoyer des notifications SNMP (traps) vers :

- Adresse du serveur de supervision : 172.16.30.25
- Communauté utilisée pour les traps : NTXSYSTEM

Dans le show snmp-server, on voit :

Address	Community	Events Sent	Notify Type	Retry	Timeout
172.16.30.25	NTXSYSTEM	None	trap	3	15

Détails importants :

Notify Type : trap : Le switch envoie des traps (notifications non acquittées).

Retry : 3 : Le switch tente 3 envois en cas d'échec.

Timeout : 15 : Délai d'attente entre les tentatives (en secondes).

4.7.7.4.2. Configuration dans l'interface Centreon

Pour permettre la supervision du switch HP, il est nécessaire d'ajouter le connecteur de supervision HP Procurve SNMP.

Chemin dans l'interface : Configuration > Connectors > Monitoring Connectors.

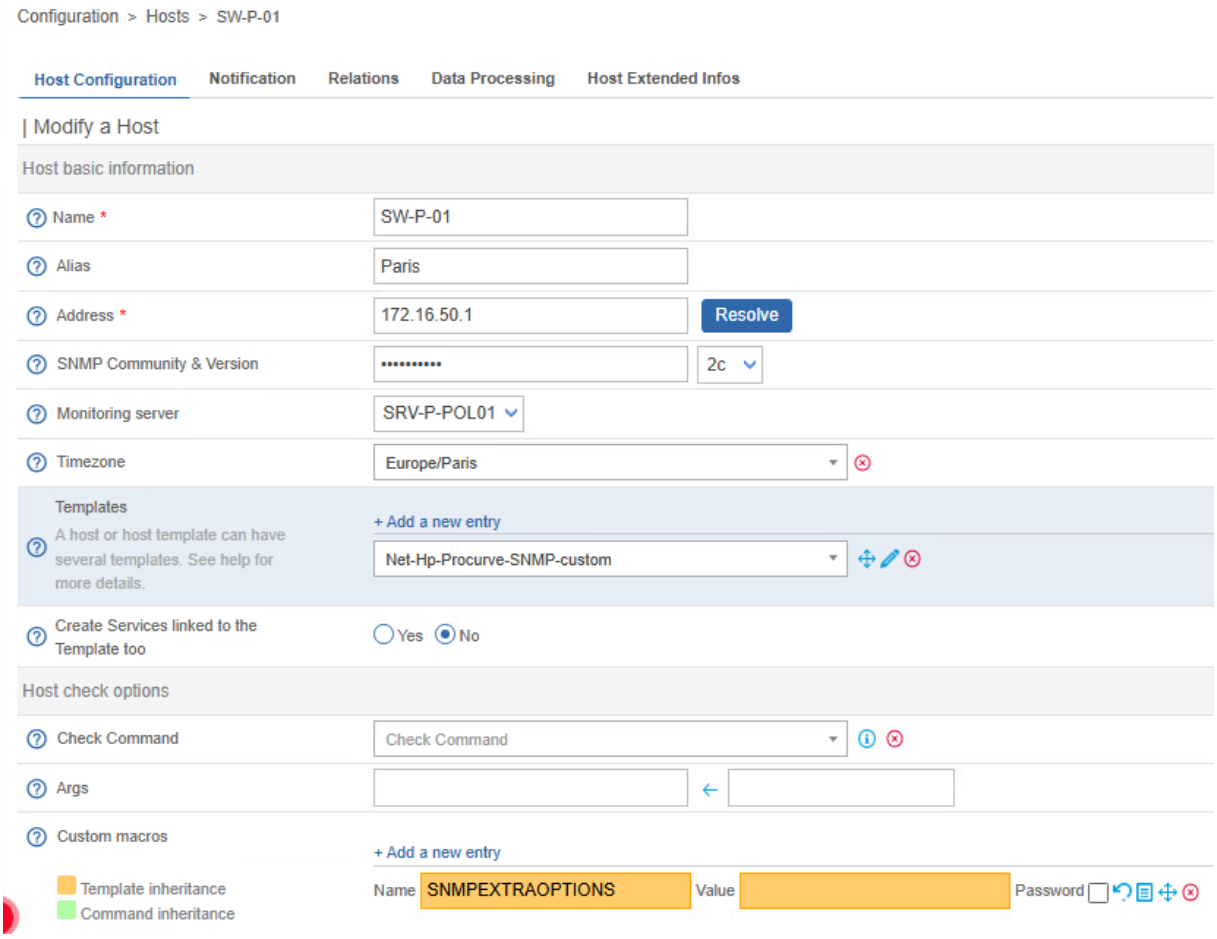
Il faut ajouter le connecteur :

Ce connecteur permet à Centreon de communiquer avec le switch via le protocole SNMP et d'interroger ses différents indicateurs de fonctionnement.

Services supervisés via le connecteur HP Procurve SNMP :

Service supervisé	Description	Objectif de la supervision	Intérêt pour l'exploitation
Uptime	Temps de fonctionnement du switch depuis le dernier redémarrage	Vérifier la stabilité de l'équipement	Permet de détecter un redémarrage intempestif ou une coupure d'alimentation
Memory	Utilisation de la mémoire RAM du switch	Surveiller la charge mémoire	Détecter une surcharge pouvant entraîner des ralentissements ou un dysfonctionnement
Environment	État matériel : température, alimentation, ventilateurs	Surveiller l'environnement physique du switch	Anticiper une panne matérielle (surchauffe, alimentation défaillante)
CPU	Taux d'utilisation du processeur	Mesurer la charge du switch	Identifier une surcharge réseau ou un problème de configuration
Ping	Test de connectivité réseau (ICMP)	Vérifier que le switch est joignable	Détecter immédiatement une perte de communication

Ensuite je vais dans Configuration > Hosts > Hosts > Add pour ajouter la configuration :



Avec le nom, l'IP, le templates (connecteur), etc.

Une fois ceci sauvegardé, et la configuration exportée, voici la remontée des sondes de supervision sous Centreon.

Status	Resource	Parent	G	Duration	Last check	Information
OK	Ping	SW-P-01		3h 11m	1m 8s	OK - 172.16.50.1: rta 1,158ms, lost 0%
OK	Cpu	SW-P-01		4h 29m	4m 38s	OK: CPU Usage: 3.00%
Up	SW-P-01			4h 38m	3m 51s	OK - 172.16.50.1: rta 1,419ms, lost 0%
OK	Environment	SW-P-01		3w 2d	1m 32s	OK: All 4 components are ok [4/4 sensors].
OK	Uptime	SW-P-01		3w 2d	5m 20s	OK: System uptime is: 5h 57m 41s
OK	Memory	SW-P-01		3w 2d	3m 26s	OK: All memories are ok.

4.7.7.5. Supervision d'OPNsense

OPNsense est une distribution open source basée sur FreeBSD, utilisée comme pare-feu et routeur. Elle permet d'assurer la sécurité, le filtrage et le routage du réseau. Afin d'intégrer OPNsense dans l'outil de supervision Centreon, il est nécessaire d'activer le protocole SNMP sur l'équipement.

4.7.7.5.1. Configuration du firewall OPNsense à superviser

Installation du plugin SNMP :

Par défaut, le service SNMP n'est pas activé sur OPNsense. Il est donc nécessaire d'installer le plugin dédié.

Étapes :

- Se connecter à l'interface web d'OPNsense avec un compte administrateur.
- Naviguer dans le menu : System > Firmware > Plugins
- Dans la liste des plugins disponibles, rechercher et installer le plugin : os-net-snmp

Ce plugin permet d'activer et de configurer le service SNMP sur OPNsense.

Activation du service SNMP :

Une fois le plugin installé, se rendre dans le menu : Services → SNMP

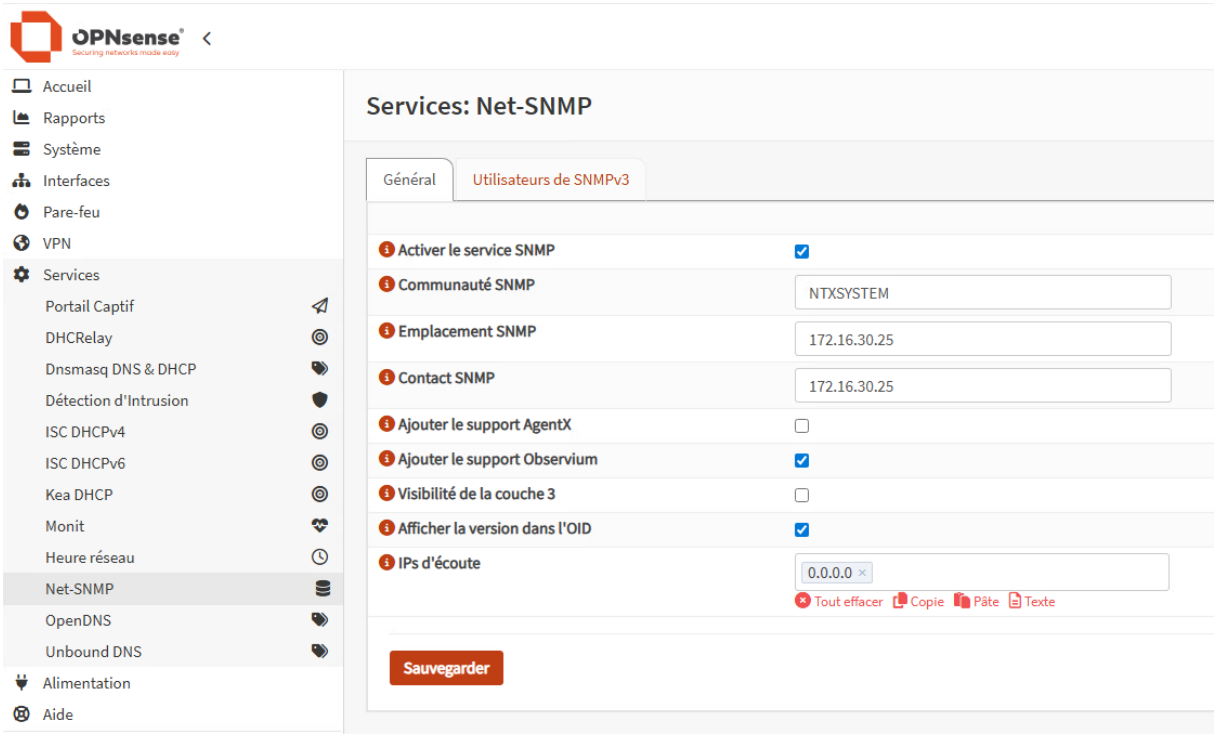
Cocher la case Enable afin d'activer le service SNMP.

Configuration des paramètres SNMP :

Pour permettre la supervision depuis Centreon, les paramètres suivants doivent être configurés :

- Community : NTXSYSTEM
- Adresse autorisée (ou localisation du serveur de supervision) : 172.16.30.25

Cette configuration autorise le serveur Centreon à interroger OPNsense via SNMP afin de superviser son état (charge CPU, mémoire, etc.).



4.7.7.5.2. Configuration dans l'interface Centreon

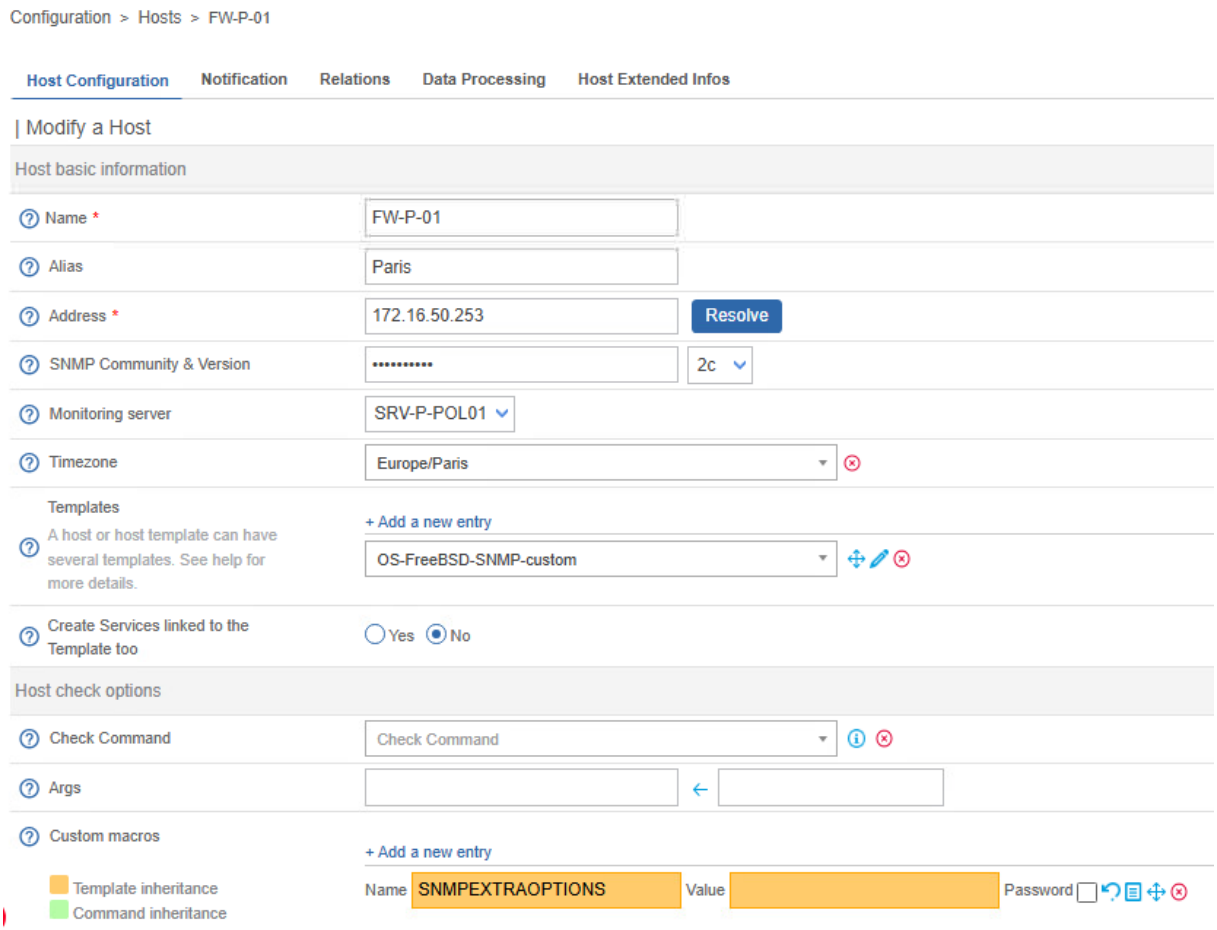
Dans Centreon, le connecteur FreeBSD est utilisé pour superviser les machines fonctionnant avec le système d'exploitation FreeBSD. Il s'agit d'un ensemble de modèles et de commandes qui permettent de récupérer automatiquement différentes informations du système via le protocole SNMP.

Grâce à ce connecteur, je peux surveiller plusieurs indicateurs importants du FW.

Dans cette étape, j'ajoute et je configure un nouvel hôte dans Centreon afin de superviser le pare-feu OPNsense. Je renseigne le nom de l'hôte (FW-P-01), son alias et son adresse IP (172.16.50.254). La supervision se fait via le protocole SNMP en version 2c, avec la communauté correspondante.

J'associe ensuite le modèle OSFreeBSD-SNMP-custom, qui permet d'appliquer automatiquement des paramètres et des contrôles adaptés au système. Enfin, le serveur

de supervision utilisé est le poller de Paris et le fuseau horaire est configuré sur Europe/Paris.



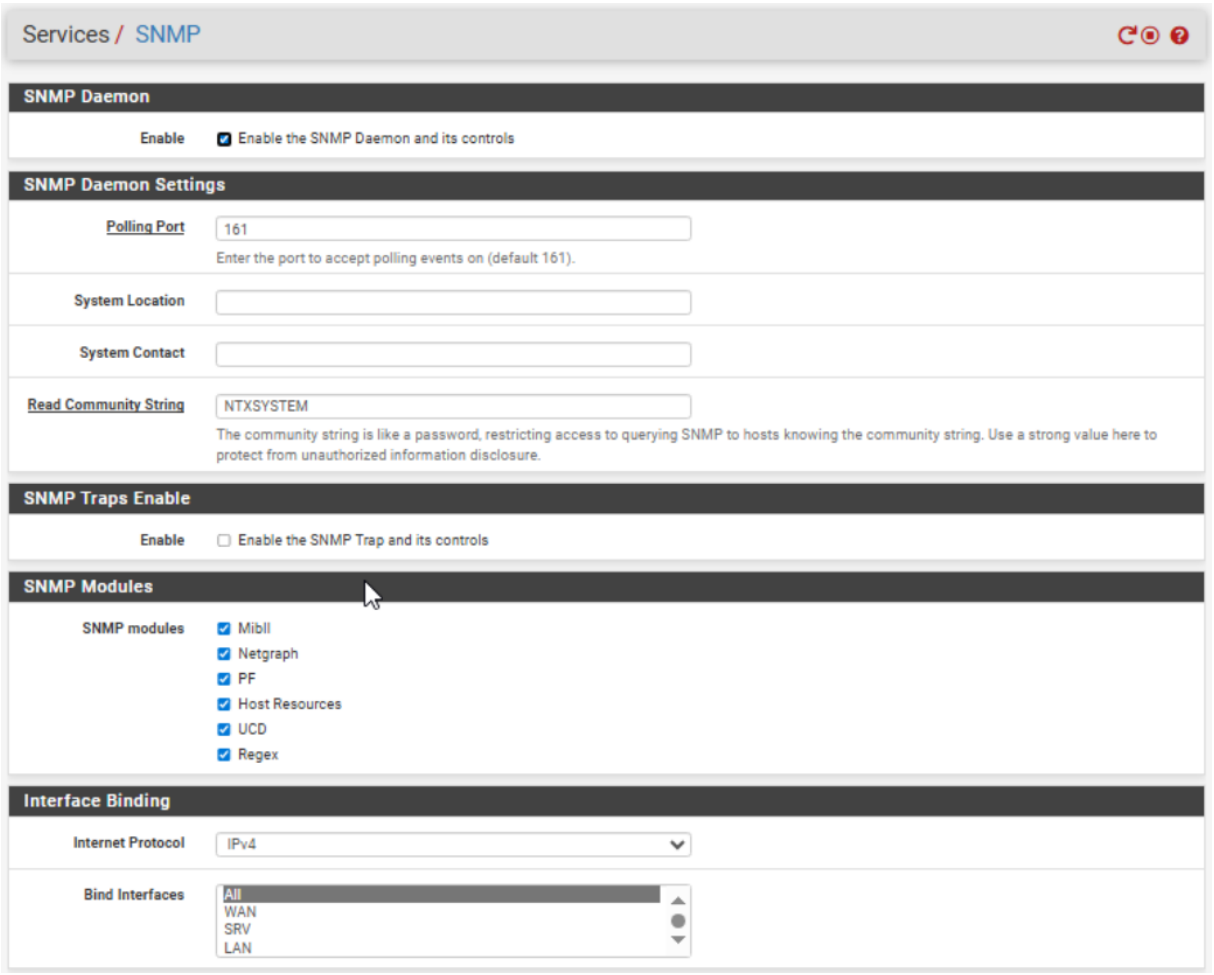
Une fois ceci sauvegardé, et la configuration exportée, voici la remontée des sondes de supervision sous Centreon.

4.7.7.6. Supervision de Pfsense

J'ai mis en place la collecte d'informations via le protocole SNMP afin de permettre à l'outil de supervision de récupérer les métriques du pare-feu. Cette supervision permet de suivre l'état du firewall, l'utilisation de ses ressources système ainsi que certaines statistiques réseau. La configuration s'effectue en deux étapes principales : d'une part la configuration du firewall à superviser, et d'autre part son intégration dans la plateforme de supervision Centreon.

4.7.7.6.1. Configuration du firewall PFsense à superviser

La première étape a consisté à configurer le firewall afin qu'il puisse être interrogé par le serveur de supervision.



Les paramètres principaux configurés sont les suivants :

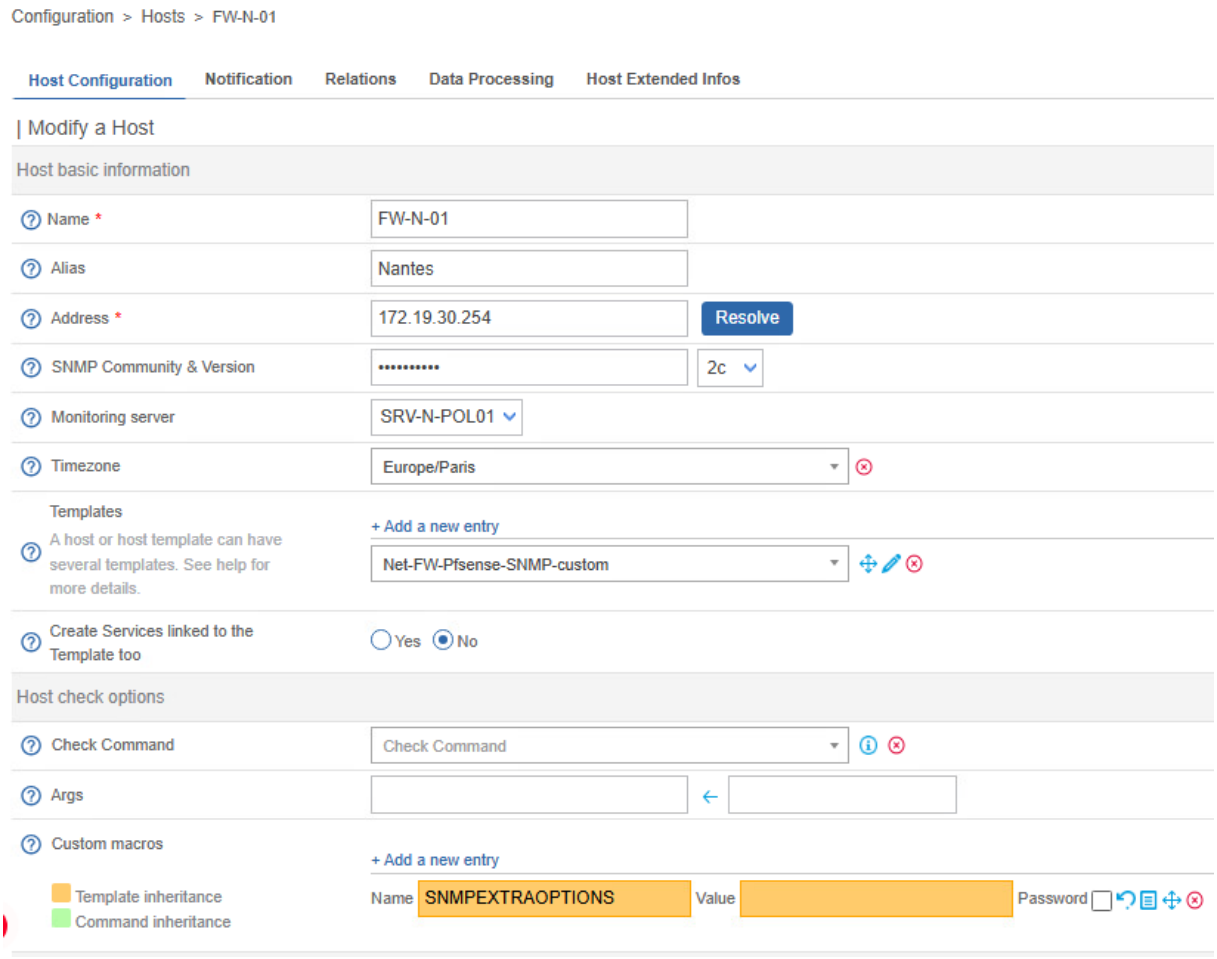
- Activation du service SNMP pour permettre la supervision à distance
- Port SNMP : 161, qui correspond au port standard utilisé pour les requêtes SNMP
- Community String configurée pour sécuriser l'accès aux informations SNMP. Cette chaîne agit comme un mot de passe permettant uniquement aux systèmes autorisés d'interroger le firewall
- Activation des modules SNMP, permettant de récupérer différentes informations système telles que :
    - L'utilisation du processeur
    - L'utilisation de la mémoire
    - Les statistiques réseau
    - L'état des interfaces
- Configuration des interfaces d'écoute, afin de définir sur quelles interfaces le service SNMP accepte les requêtes

Cette configuration permet au serveur de supervision d'accéder aux informations nécessaires au suivi du fonctionnement du firewall.

4.7.7.6.2. Configuration dans l'interface Centreon

Une fois le service SNMP activé sur le firewall, j'ai ajouté l'équipement dans la plateforme de supervision Centreon.

Dans le menu de configuration des hôtes, j'ai créé un nouvel équipement correspondant au firewall de Nantes.



J'ai renseigné les paramètres suivants :

- Nom de l'hôte : FW-N-01
- Alias : Nantes
- Adresse IP : 172.19.30.254
- Version SNMP et la Community : SNMP v2c et NTXSYSTEM
- Serveur de supervision : SRV-N-POL01
- Fuseau horaire : Europe/Paris

J’ai ensuite associé un template de supervision nommé Net-FW-Pfsense-SNMP-custom. Ce template permet d’automatiser la création des services de supervision liés à ce type d’équipement. Pour utiliser ce template, il faut ajouter le connecteur correspondant : pfSense SNMP.

Grâce à ce template, plusieurs contrôles ont été mis en place automatiquement, notamment :

- La charge du processeur (CPU)
- L’utilisation de la mémoire
- Le temps de fonctionnement du système (Uptime)
- La charge du système (Load Average)
- Les statistiques de paquets réseau
- La vérification de la disponibilité du firewall via Ping

Une fois la configuration terminée et les services générés, Centreon interroge régulièrement le firewall via SNMP afin de récupérer les informations de supervision.

Les résultats sont ensuite affichés dans l’interface de supervision sous forme de services avec différents états (OK, Warning ou Critical). Cela permet de détecter rapidement d’éventuels dysfonctionnements et d’assurer un suivi efficace de l’état du firewall.

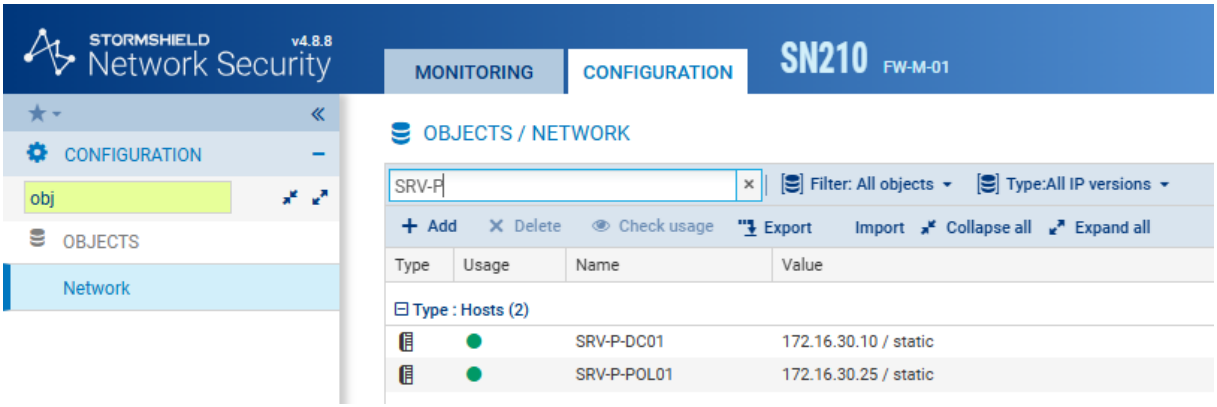
Status	Resource	Parent	G	Duration	Last check	Information
Unknown	S Blocked-Packets-Per-Interface	U FW-N-01		1w 3h	3m 41s	UNKNOWN: Need to specify OIDs
OK	S Bad-Offset-Packets	U FW-N-01		3m 46s	3m 41s	OK: Bad Offset Packets : 0.00/s
OK	S Uptime	U FW-N-01		3m 47s	3m 41s	OK: System uptime is: 6h 10m 45s
OK	S Swap	U FW-N-01		3m 47s	3m 41s	OK: Swap Total: 1023.88 MB Used: 0.00 B (0.00%) Free: 1023.88 MB (100.00%)
OK	S Short-Packets	U FW-N-01		3m 47s	3m 41s	OK: Short Packets : 0.00/s
OK	S Runtime	U FW-N-01		3m 47s	3m 41s	OK: PfSense running since : 6h 10m 20s
OK	S Normalize-Packets	U FW-N-01		3m 47s	3m 41s	OK: Normalized Packets : 0.00/s
OK	S Memory	U FW-N-01		3m 47s	3m 41s	OK: Ram Total: 1.94 GB, Used (-cache): 365.19 MB (18.40%), Cached: 146.64 MB
OK	S Memory-Dropped-Packets	U FW-N-01		3m 47s	3m 41s	OK: Dropped Packets Due To Memory : 0.00/s
OK	S Match-Packets	U FW-N-01		3m 47s	3m 41s	OK: Packets Matched Filter Rule : 3.00/s
OK	S Load	U FW-N-01		3m 47s	3m 41s	OK: Load average: 0.38, 0.46, 0.46
OK	S Fragment-Packets	U FW-N-01		3m 47s	3m 41s	OK: Fragmented Packets : 0.00/s
OK	S Cpu	U FW-N-01		3m 47s	3m 41s	OK: 1 CPU(s) average usage is 0.00 % - CPU '0' usage : 0.00 %
Up	FW-N-01			5h 3m	4m 22s	OK - 172.19.30.254: rta 1,039ms, lost 0%
OK	S Ping	U FW-N-01		5h 4m	4m	OK - 172.19.30.254: rta 0,978ms, lost 0%

4.7.7.7. Supervision de Stormshield

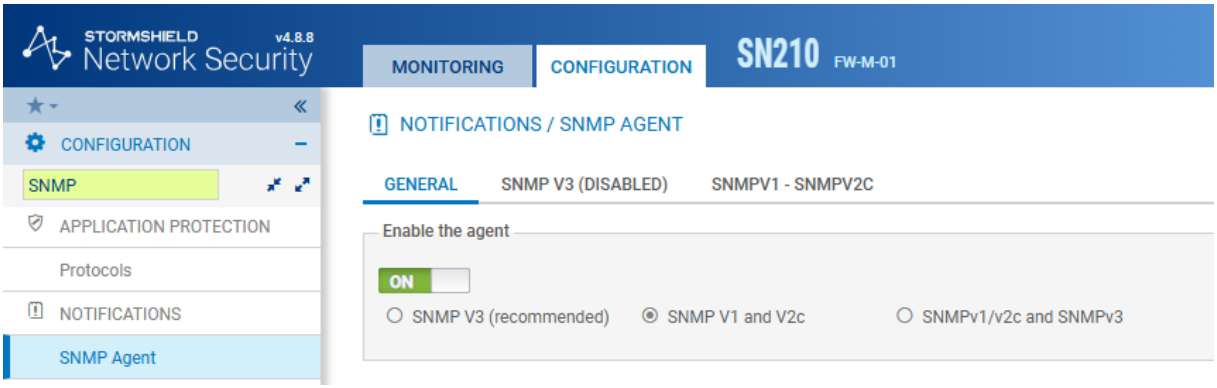
Notre site de Marseille est équipé d'un firewall Stormshield SN210.

4.7.7.7.1. Configuration du firewall Stormshield à superviser

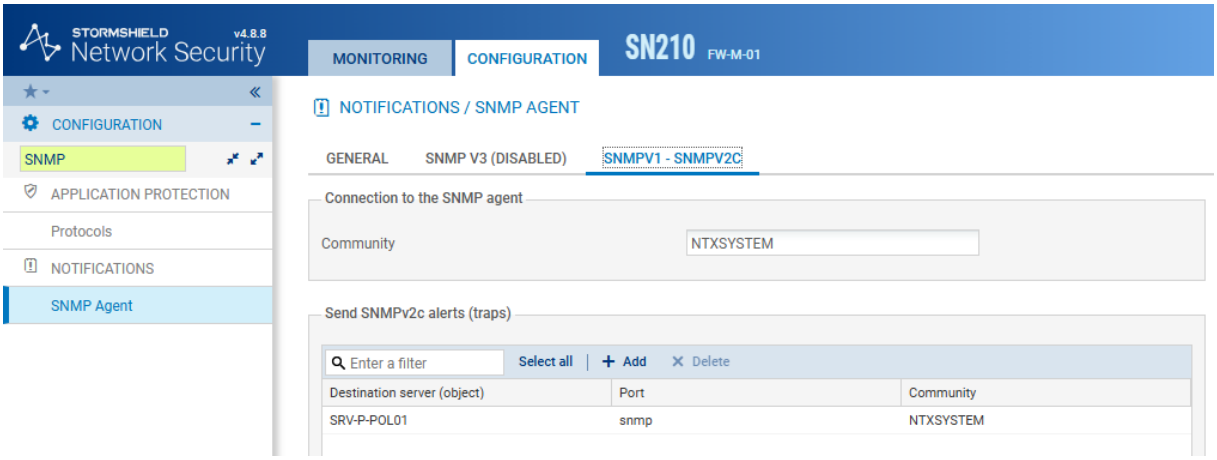
Dans un premier temps, je crée un alias pour le poller de Paris afin de rendre la configuration plus simple et plus compréhensible par la suite.



Ensuite, j'active le service SNMP sur le firewall.



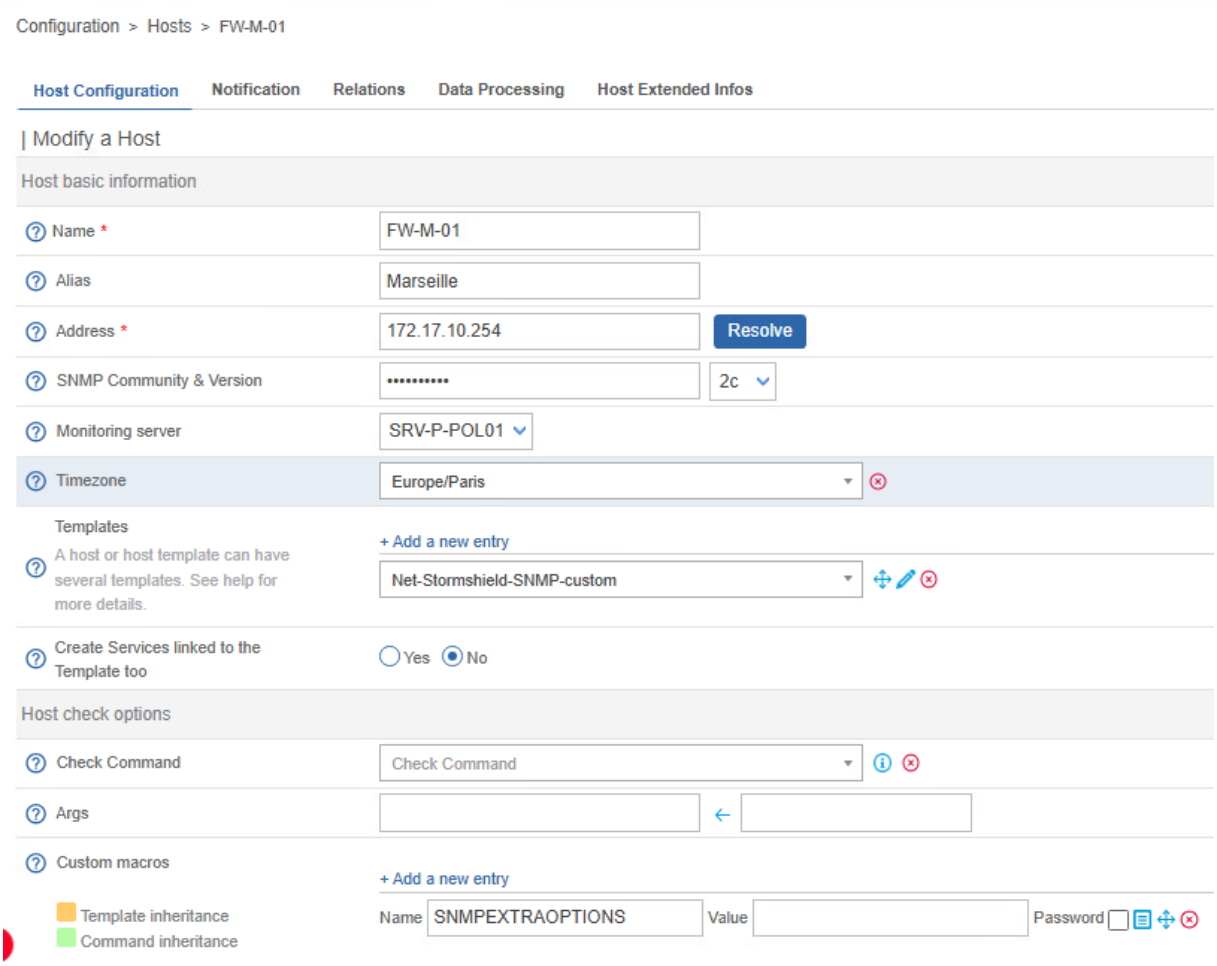
Puis, dans la rubrique SNMP v2c, je configure la communauté « NTXSYSTEM ». J'ajoute ensuite le poller comme destination, en utilisant le port SNMP (161) et en sélectionnant la communauté configurée précédemment.



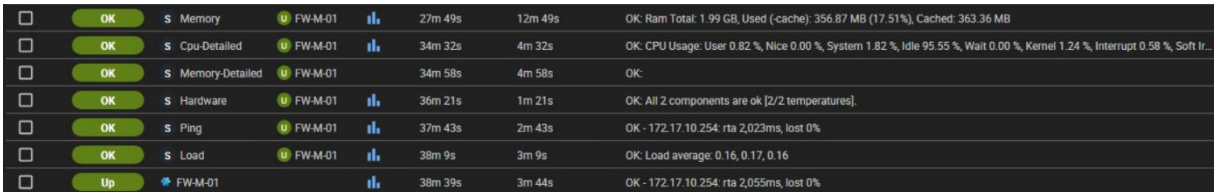
4.7.7.7.2. Configuration dans l'interface Centreon

Ajout du connecteur de supervision « Stormshield SNMP » dans le menu : « Configuration > Gestionnaire de connecteurs de supervision ».

Ajout du firewall dans Centreon avec une configuration basique, en veillant à bien choisir le template « Net-Stormshield-SNMP-custom » afin de superviser les différents services.



Une fois cela sauvegardé et la configuration exportée, la remontée des sondes doit ensuite s'effectuer.



4.7.7.8. Borne Wifi

Sur le site de Paris, une borne wifi Cisco modèle C9105AXI-E est installé. Il faut donc la superviser.

4.7.7.8.1. Configuration de la borne wifi à superviser

Il faut se connecter à la borne via le port COM à l'aide d'un câble série.

Ensuite, appliquer la configuration suivante par ligne de commande :

```
conf t
```

Permet d'entrer en mode de configuration globale de l'équipement. C'est dans ce mode que l'on peut modifier les paramètres du système.

```
snmp-server community NTXSYSTEM RO
```

Définit une communauté SNMP nommée NTXSYSTEM avec des droits RO (Read Only). Cela signifie que le serveur de supervision pourra lire les informations de l'équipement, mais pas les modifier.

```
snmp-server host 172.16.30.25 version 2c monitoring
```

Déclare un serveur SNMP (ici l'adresse IP 172.16.30.25, correspondant au poller Centreon). L'équipement enverra ses informations (traps) à cette adresse en utilisant le protocole SNMP version 2c et la communauté monitoring.

```
snmp-server enable traps
```

Active l'envoi de traps SNMP. Les traps sont des notifications envoyées automatiquement au serveur de supervision en cas d'événement (panne, redémarrage, alerte, etc.).

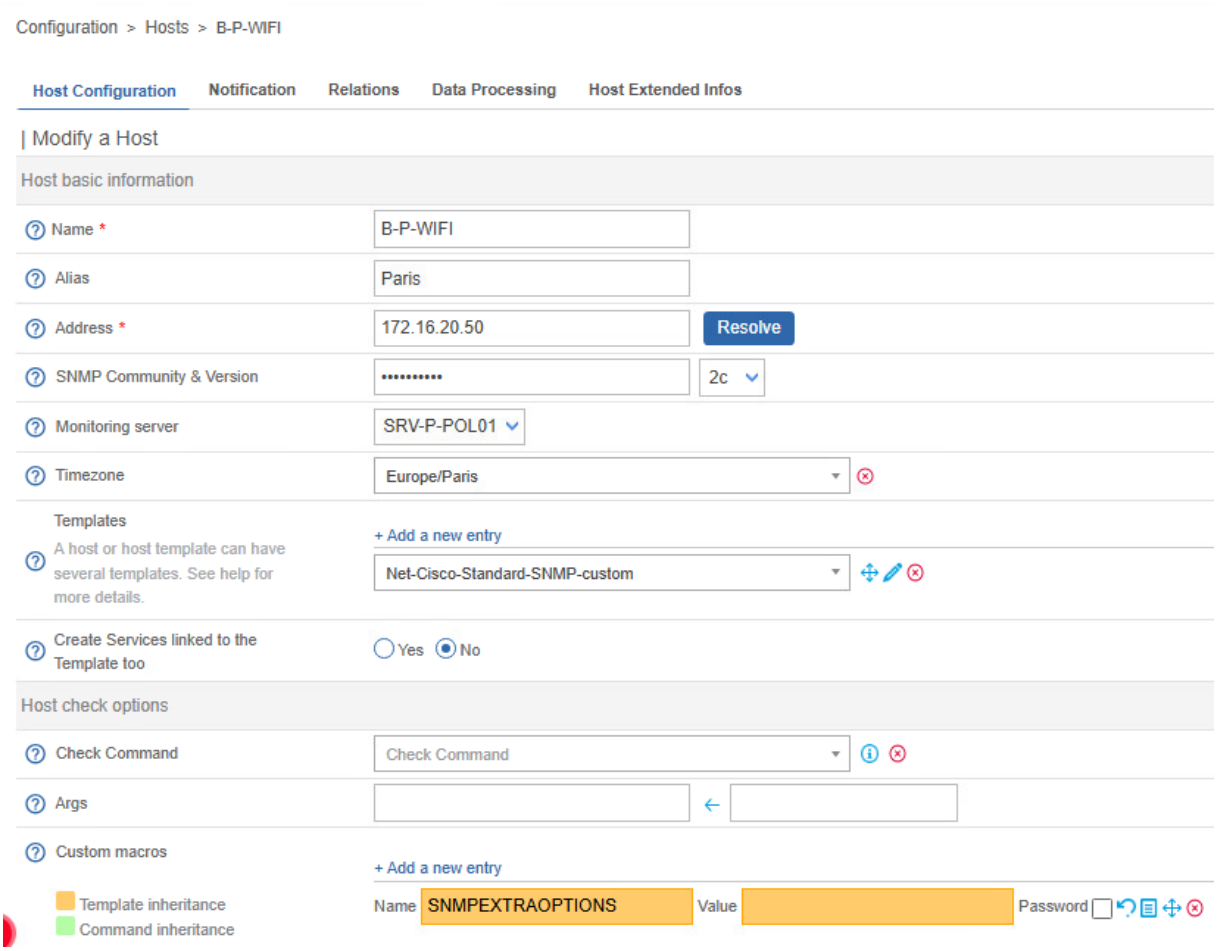
```
end
```

Permet de quitter le mode de configuration et de revenir au mode privilégié.

4.7.7.8.2. Configuration dans l'interface Centreon

Ajout du connecteur de supervision « Cisco Standard SNMP » dans le menu : « Configuration > Gestionnaire de connecteurs de supervision ».

Ajout de la borne wifi dans Centreon avec une configuration basique, en veillant à bien choisir le Template « Net-Cisco-Standard-SNMP-custom » afin de superviser les différents services.



Une fois cela sauvegardé et la configuration exportée, la remontée des sondes doit ensuite s'effectuer.

4.7.8. Alertes et seuils de tolérance

Dans Centreon, la supervision repose sur des checks réguliers associés à des seuils de tolérance qui permettent de détecter les anomalies avant qu'elles ne deviennent critiques. La configuration est identique sur tous les hôtes et se fait automatiquement grâce aux connecteurs. Je peux bien sûr modifier les seuils si nécessaire.

Définition des seuils :

Chaque service surveillé (CPU, mémoire, ping, disque...) utilise des seuils :

- WARNING : niveau d'alerte préventif
- CRITICAL : niveau critique nécessitant une action immédiate

Exemple :

- CPU > 80% → WARNING
- CPU > 90% → CRITICAL

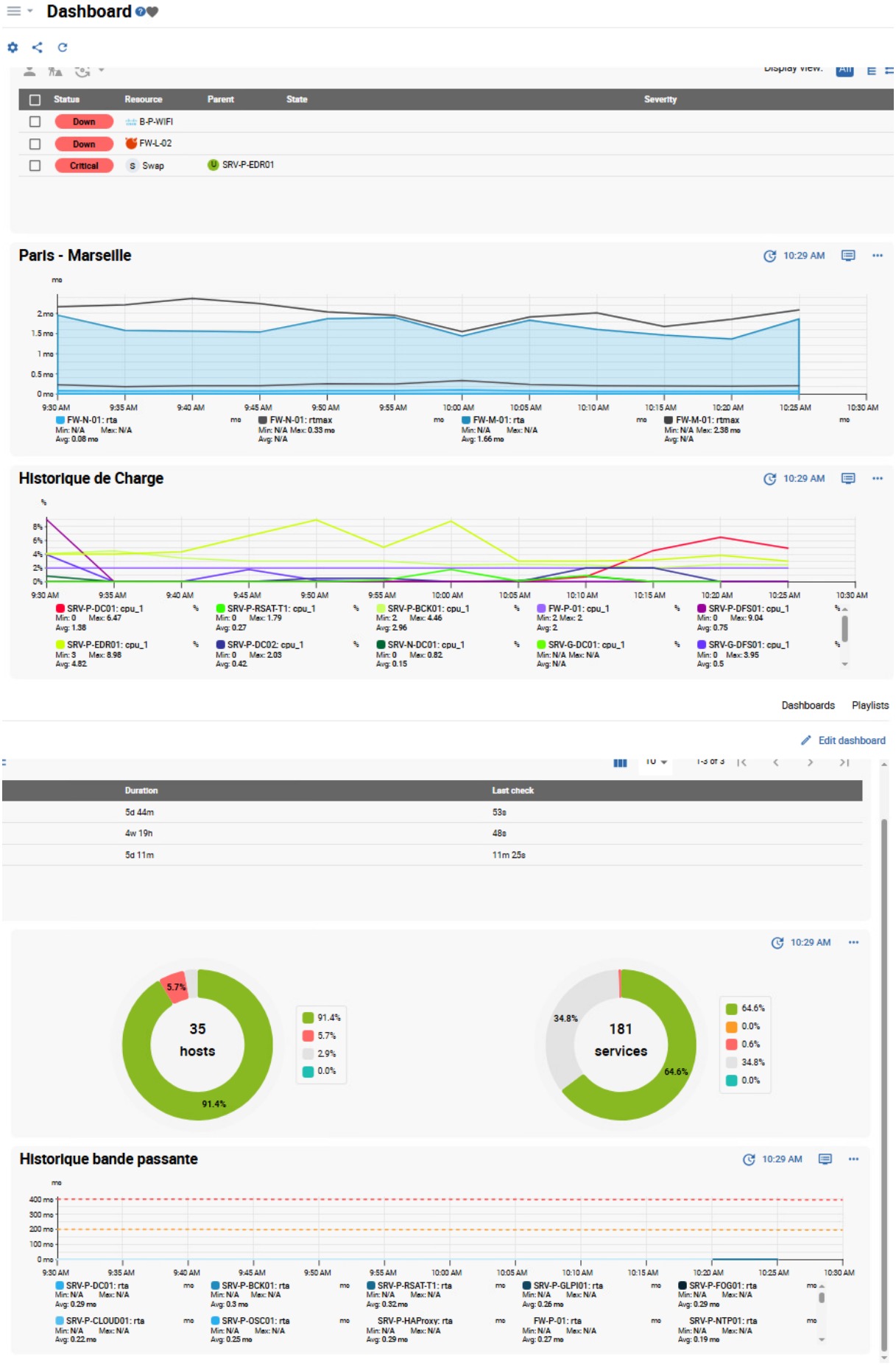
Fréquence des vérifications :

Les contrôles sont exécutés selon deux intervalles :

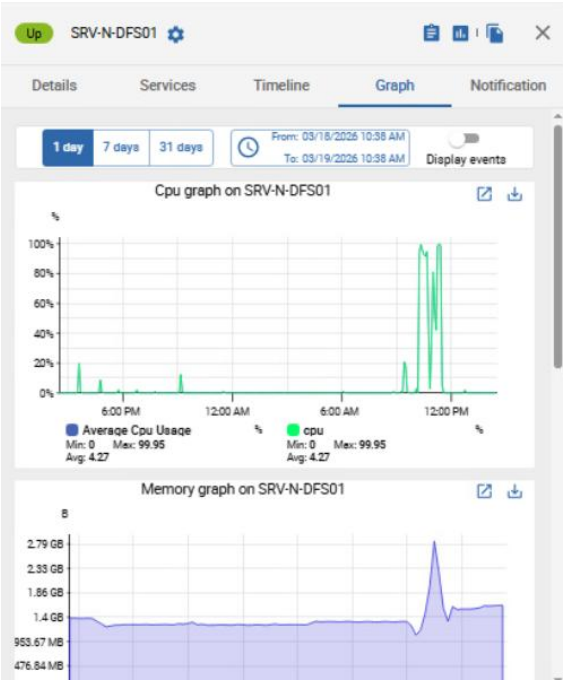
- Intervalle normal (ex : 5 minutes) → surveillance standard
- Intervalle de retry (ex : 1 minute) → vérifications rapprochées en cas de problème

4.7.9. Mise en place de Dashboard

Ci-dessous, un exemple de dashboard créé dans l'interface (La capture est coupée en deux pour une meilleure visibilité.). On peut y identifier rapidement les serveurs et des services en état WARNING, DOWN ou CRITICAL. Un petit graphique la disponibilité réseau des sites Paris - Marseille. Deux diagrammes circulaires présentent l'état des machines et des services : la majorité des machines est en bon état, mais certaines rencontrent des problèmes. Pour les services, beaucoup sont OK, une partie est en état inconnu et quelques-uns présentent des erreurs. Il y a aussi des graphes pour l'évolution de historique de charge des serveurs et la bande passante.


Dashboard
Status
Resource
Parent
State
Severity
Down
B-P-WIFI
Down
FW-L-02
Critical
Swap
SRV-P-EDR01
Paris - Marseille
10:29 AM
FW-N-01: rta
FW-N-01: rtmax
FW-M-01: rta
FW-M-01: rtmax
Historique de Charge
10:29 AM
SRV-P-DC01: cpu_1
SRV-P-RSAT-T1: cpu_1
SRV-P-BCK01: cpu_1
FW-P-01: cpu_1
SRV-P-DFS01: cpu_1
SRV-P-EDR01: cpu_1
SRV-P-DC02: cpu_1
SRV-N-DC01: cpu_1
SRV-G-DC01: cpu_1
SRV-G-DFS01: cpu_1
Dashboards
Playlists
Edit dashboard
Duration
Last check
5d 44m
53s
4w 19h
48s
5d 11m
11m 25s
10:29 AM
35
hosts
5.7%
91.4%
91.4%
5.7%
2.9%
0.0%
181
services
34.8%
64.6%
64.6%
0.0%
0.6%
34.8%
0.0%
Historique bande passante
10:29 AM
SRV-P-DC01: rta
SRV-P-BCK01: rta
SRV-P-RSAT-T1: rta
SRV-P-GLPI01: rta
SRV-P-FOG01: rta
SRV-P-CLOUD01: rta
SRV-P-OSC01: rta
SRV-P-HAProxy: rta
FW-P-01: rta
SRV-P-NTP01: rta

On peut également afficher un petit graphique pour chaque machine en cliquant directement dessus.



4.7.10. Phase de test

La phase de test s'est déroulée sur plusieurs jours afin de vérifier que tout fonctionnait correctement. Sur la capture ci-dessous, on peut constater que tous les hôtes sont bien remontés.

Status	Resource	Parent	G	Duration	Last check	Information
Up	FW-L-01			4h 12m	2m 46s	OK - 172.18.30.253: rta 1.317ms, lost 0%
Up	SRV-P-HAProxy			4h 13m	3m 49s	OK - 172.16.99.10: rta 0,410ms, lost 0%
Up	SRV-P-NTP01			4h 13m	3m 49s	OK - 172.16.30.18: rta 0,397ms, lost 0%
Up	SRV-P-NETBOX01			4h 13m	3m 49s	OK - 172.16.30.22: rta 0,330ms, lost 0%
Up	SW-P-02			4h 13m	3m 49s	OK - 172.16.50.2: rta 1,348ms, lost 0%
Up	FW-P-01			4h 13m	3m 54s	OK - 172.16.50.253: rta 0,594ms, lost 0%
Up	SW-P-01			4h 13m	3m 54s	OK - 172.16.50.1: rta 1,254ms, lost 0%
Up	SRV-P-CLOUD01			4h 14m	3m 49s	OK - 172.16.30.16: rta 0,260ms, lost 0%
Up	SRV-P-FOG01			4h 14m	3m 49s	OK - 172.16.30.11: rta 0,294ms, lost 0%
Up	SRV-P-GLPI01			4h 14m	3m 49s	OK - 172.16.30.14: rta 0,398ms, lost 0%
Up	SRV-P-BCK01			4h 15m	3m 49s	OK - 172.16.30.15: rta 0,359ms, lost 0%
Up	SRV-N-DC01			5d 18h	3m 46s	OK - 172.19.30.10: rta 2.309ms, lost 0%
Up	SRV-P-DC01			1w 6d	3m 49s	OK - 172.16.30.10: rta 0,354ms, lost 0%
Up	SRV-N-DFS01			3w 2d	3m 46s	OK - 172.19.30.50: rta 0.370ms, lost 0%
Up	SRV-G-DC02			3w 2d	3m 46s	OK - 172.20.30.20: rta 0.923ms, lost 0%
Up	FW-N-01			3w 3d	3m 46s	OK - 172.19.30.254: rta 0.246ms, lost 0%
Up	FW-G-01			3w 3d	3m 46s	OK - 172.20.30.254: rta 0.375ms, lost 0%
Up	SRV-G-DFS01			3w 3d	3m 46s	OK - 172.20.30.50: rta 0.904ms, lost 0%
Up	SRV-G-DC01			3w 3d	3m 6s	OK - 172.20.30.10: rta 0.923ms, lost 0%

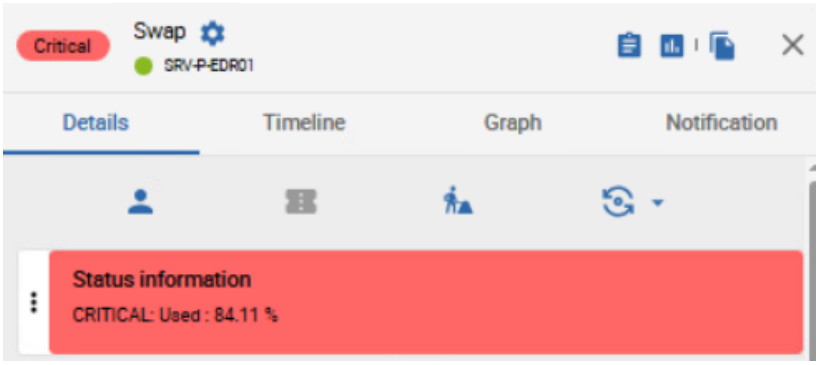
Il en va de même pour les services (CPU, RAM, disque, trafic).

Status	Resource	Parent	G	Duration	Last check	Information
OK	Ping	SW-P-01		4h 33m	3m 16s	OK - 172.16.50.1: rta 1,194ms, lost 0%
OK	Swap	SRV-P-RSAT-T1		5h 36m	6m 33s	OK: Swap Total: 10.75 GB Used: 1.71 GB (15.94%) Free: 9.04 GB (84.06%)
OK	Memory	SRV-P-RSAT-T1		5h 36m	6m 33s	OK: Ram Total: 8.00GB Used: 1.84GB (22.97%) Free: 6.16GB (77.03%)
OK	Cpu	SRV-P-RSAT-T1		5h 36m	1m 33s	OK: 2 CPU(s) average usage is 0.00 %
OK	Ping	SRV-P-RSAT-T1		5h 36m	1m 33s	OK - 172.16.30.31: rta 0,397ms, lost 0%
OK	Cpu	SW-P-02		5h 51m	1m 40s	OK: CPU Usage: 4.00%
OK	Cpu	SW-P-01		5h 51m	1m 46s	OK: CPU Usage: 3.00%
OK	Cpu	SRV-P-NETBOX01		5h 51m	1m 57s	OK: 1 CPU(s) average usage is 2.00 % - CPU '0' usage : 2.00 %
OK	Load	FW-P-01		5h 52m	2m 26s	OK: Load average: 0.21, 0.18, 0.17
OK	Load	SRV-P-HAProxy		5h 52m	2m 32s	OK: Load average: 0.00, 0.00, 0.00
OK	Load	SRV-P-CLOUD01		5h 52m	2m 43s	OK: Load average: 0.00, 0.00, 0.00
OK	Load	SRV-P-FOG01		5h 52m	2m 49s	OK: Load average: 0.00, 0.00, 0.00
OK	Load	SRV-P-GLPI01		5h 52m	2m 54s	OK: Load average: 0.00, 0.00, 0.00
OK	Swap	SRV-P-BCK01		5h 53m	8m 6s	OK: Swap Total: 13.81 GB Used: 7.09 GB (51.34%) Free: 6.72 GB (48.66%)
OK	Load	SRV-P-NETBOX01		5h 53m	3m 51s	OK: Load average: 0.00, 0.00, 0.00
OK	Memory	SRV-P-FOG01		5h 54m	9m 43s	OK: Ram Total: 1.92 GB Used (-buffers/cache): 370.55 MB (18.84%) Free: 1.56 GB (81.16%), Buffer: 23.65 MB, Cached: 260.93 MB, Shared: 10.10 MB
OK	Memory	SRV-P-GLPI01		5h 54m	9m 48s	OK: Ram Total: 1.92 GB Used (-buffers/cache): 288.27 MB (14.65%) Free: 1.64 GB (85.35%), Buffer: 53.34 MB, Cached: 345.40 MB, Shared: 37.80 MB
OK	Memory	SRV-P-NETBOX01		5h 55m	10m 45s	OK: Ram Total: 3.82 GB Used (-buffers/cache): 966.74 MB (24.69%) Free: 2.88 GB (75.31%), Buffer: 95.66 MB, Cached: 688.64 MB, Shared: 17.56 MB
OK	Swap	SRV-P-FOG01		5h 56m	11m 37s	OK: Swap Total: 975.00 MB Used: 0.00 B (0.00%) Free: 975.00 MB (100.00%)

Pour le test, j'ai coupé la borne Wi-Fi et une alerte a immédiatement été remontée, ce qui a confirmé le bon fonctionnement du système. Et en la remettant en ligne, elle est directement remontée dans la supervision.

	Down	B-P-WIFI		4d 5h	2m 31s	CRITICAL - 172.16.20.50: rta nan, lost 100%

De plus, le swap sur cette machine est également passé en alerte, et après vérification directement sur la machine, cela correspondait bien à la réalité.



Test des alertes sur un serveur Windows. Dans un premier temps, on peut bien voir que tout est OK dans la supervision depuis plusieurs jours sur cette machine :

Status	Resource	Parent	G	Duration	Last check	Information
OK	Ping	SRV-P-DFS01		1d 1h	3m 48s	OK - 172.16.30.50: rta 0,323ms, lost 0%
Up	SRV-P-DFS01			1d 1h	3m 44s	OK - 172.16.30.50: rta 0,536ms, lost 0%
OK	Cpu	SRV-P-DFS01		4w 1d	1m 39s	OK: 2 CPU(s) average usage is 0.00 %
OK	Memory	SRV-P-DFS01		4w 1d	3m 33s	OK: Ram Total: 8.00GB Used: 1.91GB (23.86%) Free: 6.09GB (76.14%)
OK	Swap	SRV-P-DFS01		4w 1d	5m 26s	OK: Swap Total: 9.25 GB Used: 1.56 GB (16.82%) Free: 7.69 GB (83.18%)

Je vais maintenant couper la carte réseau de ce serveur pour voir si l'information remonte bien. Et l'on peut voir que cela est directement remonté.

Status	Resource	Parent	G	Duration	Last check	Information
Down	SRV-P-DFS01			7s	19s	CRITICAL - 172.16.30.50: rta nan, lost 100%
Critical	Ping	SRV-P-DFS01		19s	19s	CRITICAL - 172.16.30.50: rta nan, lost 100%
Unknown	Swap	SRV-P-DFS01		19s	19s	UNKNOWN: SNMP Table Request: Timeout
Unknown	Memory	SRV-P-DFS01		19s	19s	UNKNOWN: SNMP Table Request: Timeout
Unknown	Cpu	SRV-P-DFS01		19s	19s	UNKNOWN: SNMP Table Request: Timeout

Je réactive la carte réseau, mais je coupe le service SNMP. Je devrais normalement voir que le ping est OK.

Status	Resource	Parent	G	Duration	Last check	Information
Unknown	Swap	SRV-P-DFS01		4m 35s	41s	host SRV-P-DFS01 is down
Unknown	Memory	SRV-P-DFS01		4m 35s	41s	host SRV-P-DFS01 is down
Unknown	Cpu	SRV-P-DFS01		4m 35s	41s	host SRV-P-DFS01 is down
OK	Ping	SRV-P-DFS01		11s	11s	OK - 172.16.30.50: rta 0,237ms, lost 0%
Up	SRV-P-DFS01			38s	11s	OK - 172.16.30.50: rta 0,486ms, lost 0%

Et maintenant, je réactive le service SNMP et tout devrait remonter directement.

Status	Resource	Parent	G	Duration	Last check	Information
OK	Swap	SRV-P-DFS01		10s	10s	OK: Swap Total: 9.25 GB Used: 2.23 GB (24.13%) Free: 7.02 GB (75.87%)
OK	Memory	SRV-P-DFS01		10s	10s	OK: Ram Total: 8.00GB Used: 2.51GB (31.36%) Free: 5.49GB (68.64%)
OK	Cpu	SRV-P-DFS01		10s	10s	OK: 2 CPU(s) average usage is 49.50 %
OK	Ping	SRV-P-DFS01		1m 41s	10s	OK - 172.16.30.50: rta 0,290ms, lost 0%
Up	SRV-P-DFS01			2m 8s	10s	OK - 172.16.30.50: rta 0,396ms, lost 0%

Simulation d'une coupure réseau entre Paris et Marseille : je vais couper le réseau du site de Marseille pour vérifier que les alertes fonctionnent bien. Ici, on peut voir que tout est bien UP.

	Up	FW-M-01		4d 21h	5s	OK - 172.17.10.254: rta 1,829ms, lost 0%

Et une fois la coupure effectuée, une alerte apparaît directement dans Centreon.

	Down	FW-M-01		8s	20s

Une fois la mise en réseau rétablie, la remontée dans Centreon se fait automatiquement.

	Up	FW-M-01		1m 39s	1m 36s	OK - 172.17.10.254: rta 2,035ms, lost 0%

4.8. Axe amélioration

Plusieurs axes d'amélioration peuvent être envisagés pour faire évoluer le projet.

Tout d'abord, le passage au protocole SNMPv3 permettrait de renforcer la sécurité de la supervision. Contrairement au SNMPv2c, il intègre un système d'authentification

(login/mot de passe) ainsi que du chiffrement des échanges, garantissant une meilleure protection des données transmises entre les équipements et le serveur de supervision.

Ensuite, pour les serveurs Windows, la mise en place d'une supervision via un client NRPE pourrait être envisagée. Cette solution permettrait d'obtenir des informations plus détaillées et plus précises sur l'état des machines (services, ressources système, processus), tout en offrant une meilleure flexibilité dans la configuration des contrôles.

Par ailleurs, il serait pertinent de :

- Mettre en place des seuils d'alerte plus fins afin d'anticiper les incidents avant qu'ils n'impactent les utilisateurs
- Configurer des notifications avancées (mail, SMS) pour améliorer la réactivité des équipes techniques même s'il y a déjà des tableaux de bord avec les alertes

Ces améliorations permettraient de rendre la solution de supervision plus sécurisée, plus performante et mieux adaptée aux besoins futurs de l'entreprise OASIS.

4.9. Conclusion

En conclusion, ce projet m'a permis d'acquérir de nombreuses compétences dans le domaine de la supervision et de la gestion d'infrastructure. J'ai pu réaliser des tâches concrètes, comme la configuration de Centreon pour superviser différents équipements réseau et serveurs, ce qui m'a permis de mieux comprendre le fonctionnement d'une infrastructure multi-sites et la remontée d'alertes en temps réel.

Malgré certaines difficultés rencontrées, notamment la supervision des hôtes ESXi en version 8, pour laquelle les connecteurs disponibles sont uniquement compatibles avec des versions ultérieures ou nécessitent l'utilisation de vCenter, ainsi que l'absence de notifications par e-mail en raison du manque de serveur de messagerie et d'adresse e-mail dédiée pour notre entreprise fictive.

La solution de supervision Centreon, est capable de surveiller l'état des équipements critiques, d'alerter les équipes en cas d'incident et d'assurer une visibilité globale sur l'infrastructure. Cette expérience m'a permis de renforcer mes connaissances techniques tout en développant ma capacité à résoudre des problèmes concrets dans un environnement professionnel.

Pour terminer, ce projet m'a permis de valider plusieurs compétences du référentiel BTS SIO Option SISR :

- Gérer le patrimoine informatique
- Répondre aux incidents et aux demandes d'assistance et d'évolution
- Travailler en mode projet
- Mettre à disposition des utilisateurs un service informatique

5. Annexe

5.1. Annexe 1 : Documentation Installation Debian 12

5.1.1. Objet

Cette instruction décrit la manière de procéder pour installer une machine virtuelle Debian 12.

5.1.2. Domaine D'application

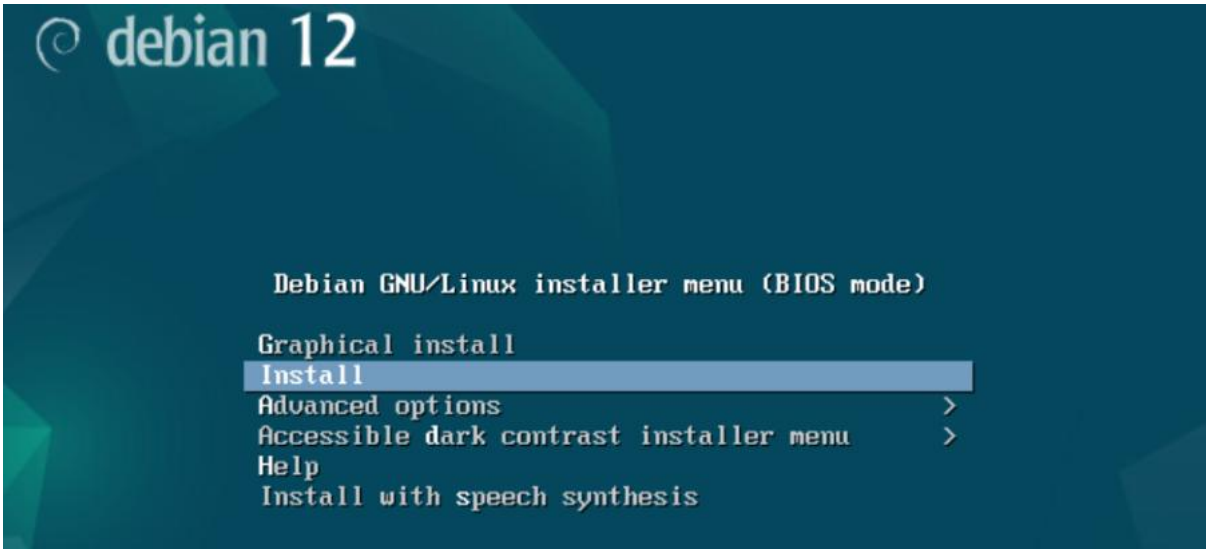
Le contenu de cette instruction concerne toutes les personnes de NTxSystem qui sont voués à installer des machines linux (Debian).

5.1.3. Définition et abréviations

Debian est une distribution Linux libre et open-source.

5.1.4. Installation Debian

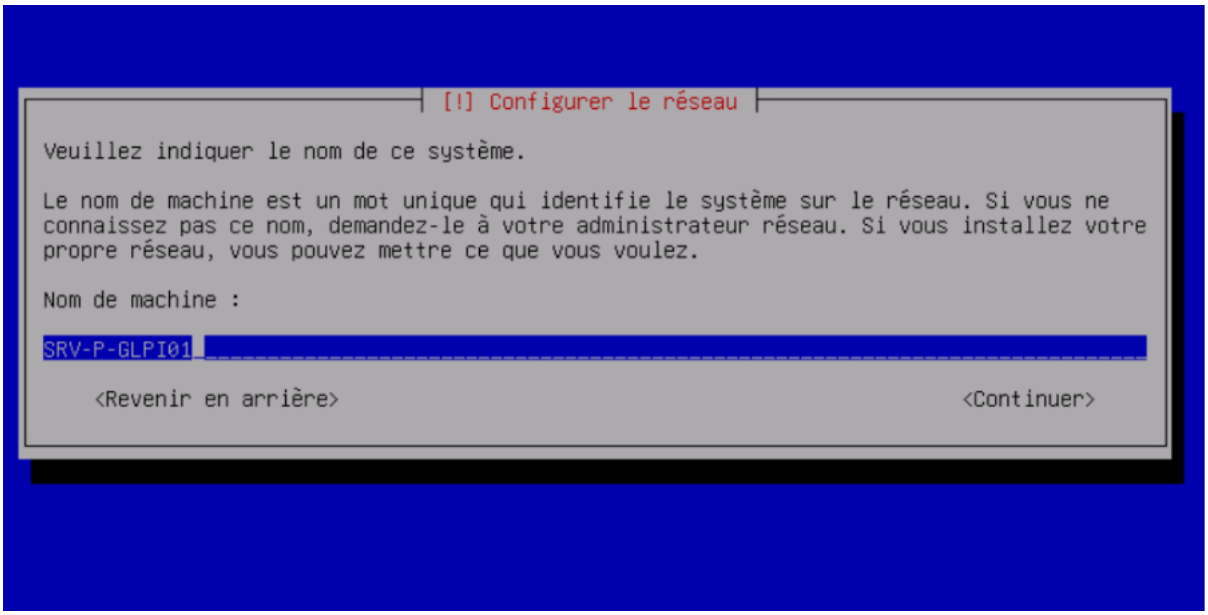
Après avoir connecter un iso Debian, boot sur l'iso.
Pour installer une Debian sans interface graphique, choisir "Install"



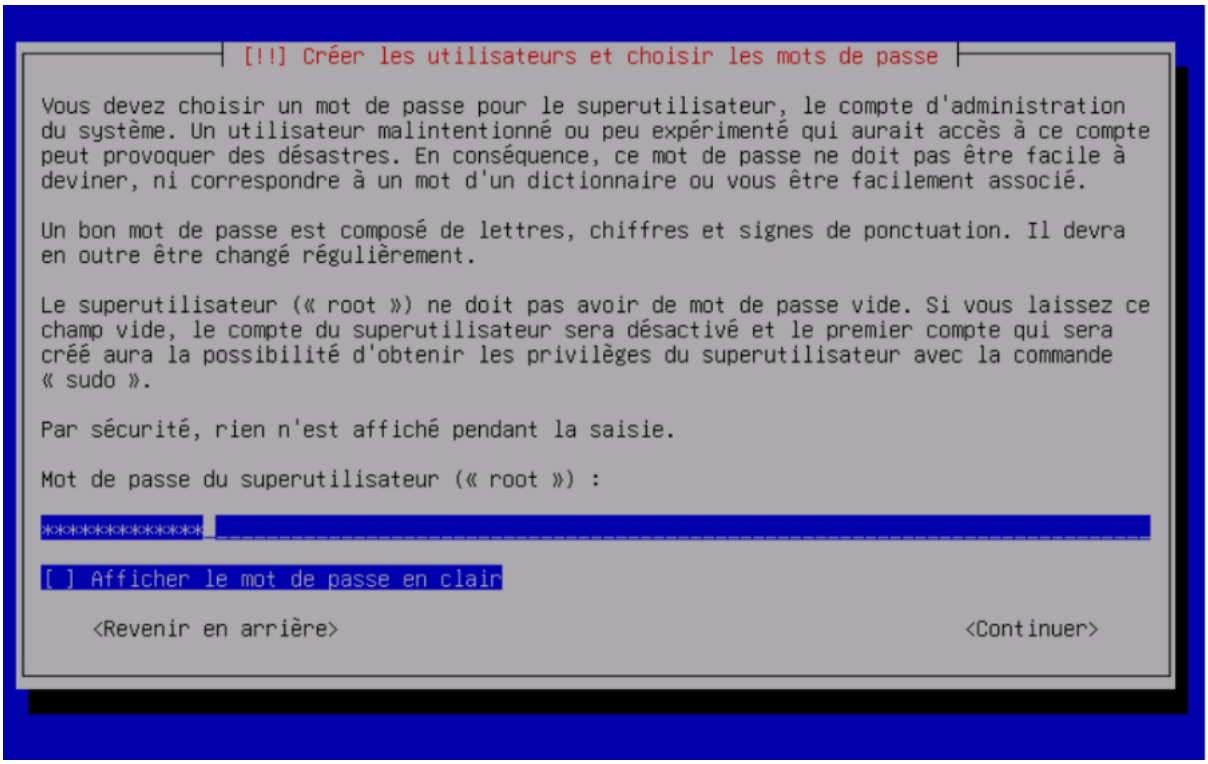
Choisir la langue française pour les paramètres suivants, puis attendre la fin du chargement.

Ne pas configurer de réseau pour le moment.

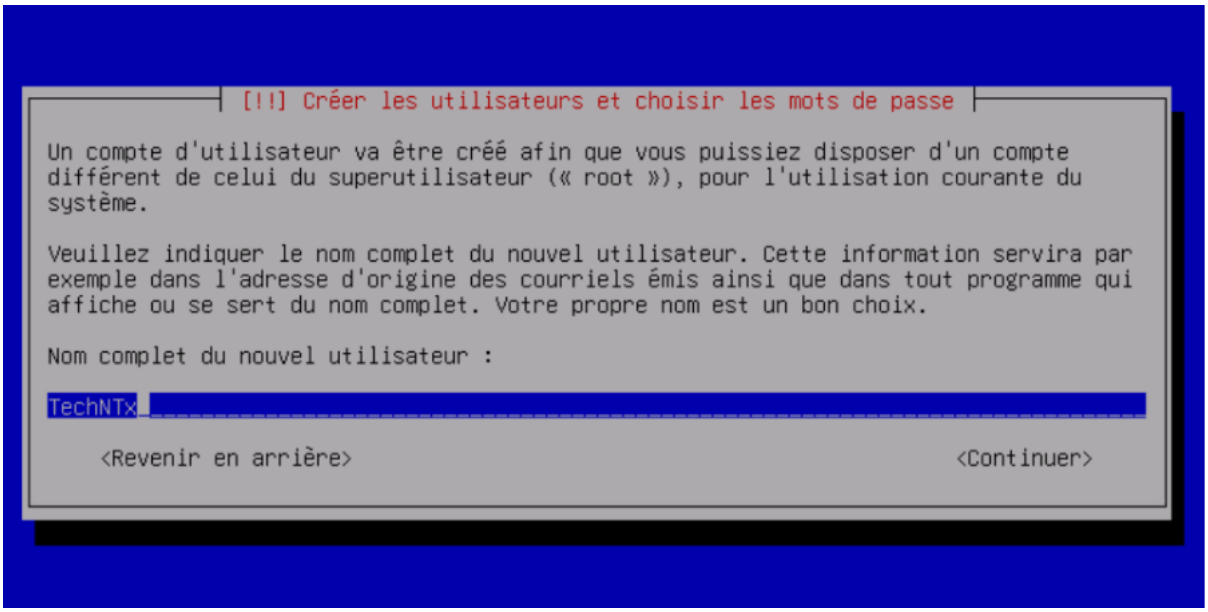
Nommer la machine selon la convention de nommage.



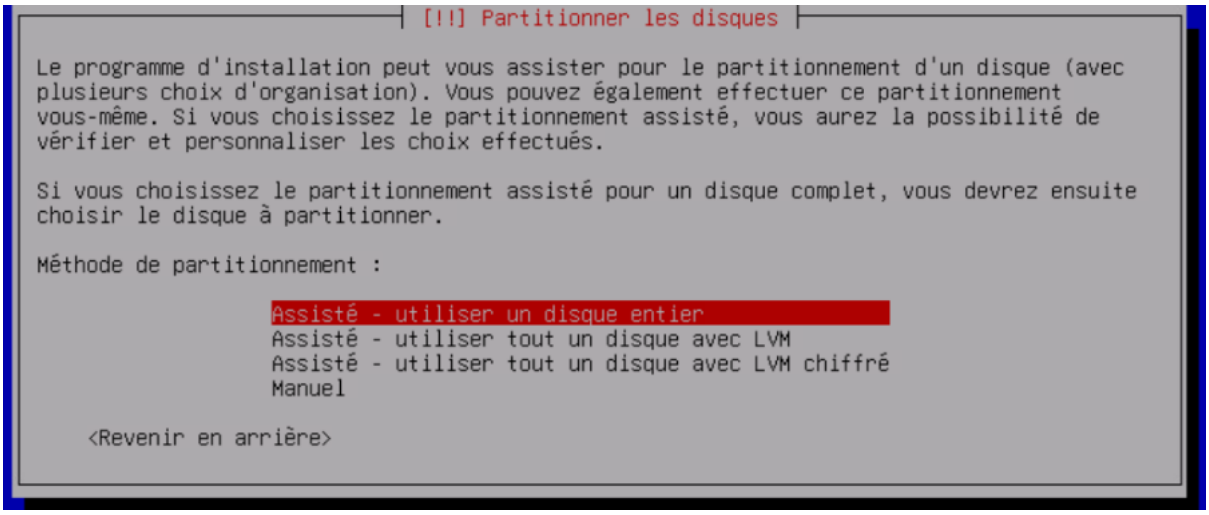
Ensuite, définir un mot de passe “root” selon la convention interne de mot de passe.



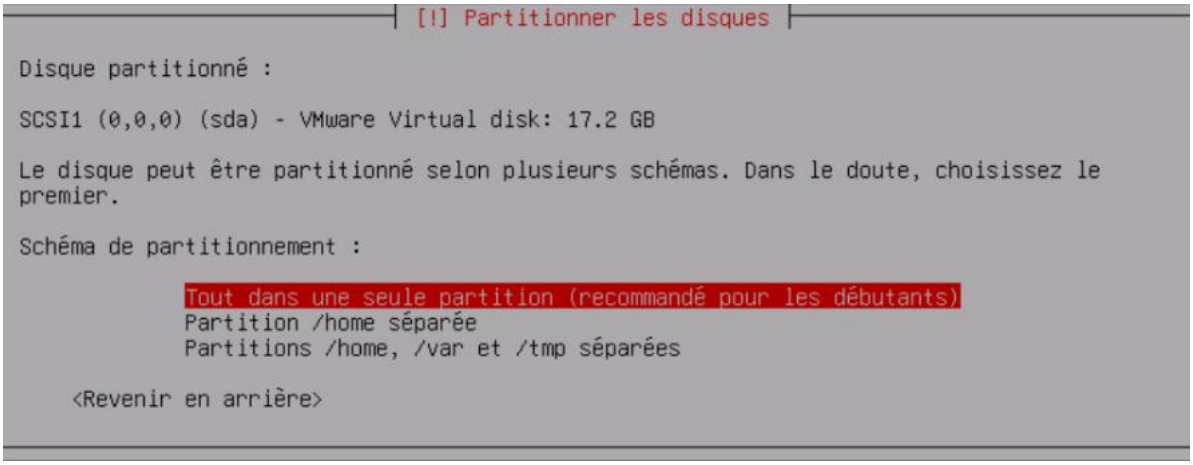
Définir un compte utilisateur TechNTx, et lui donner un mot de passe selon la convention interne de mot de passe.



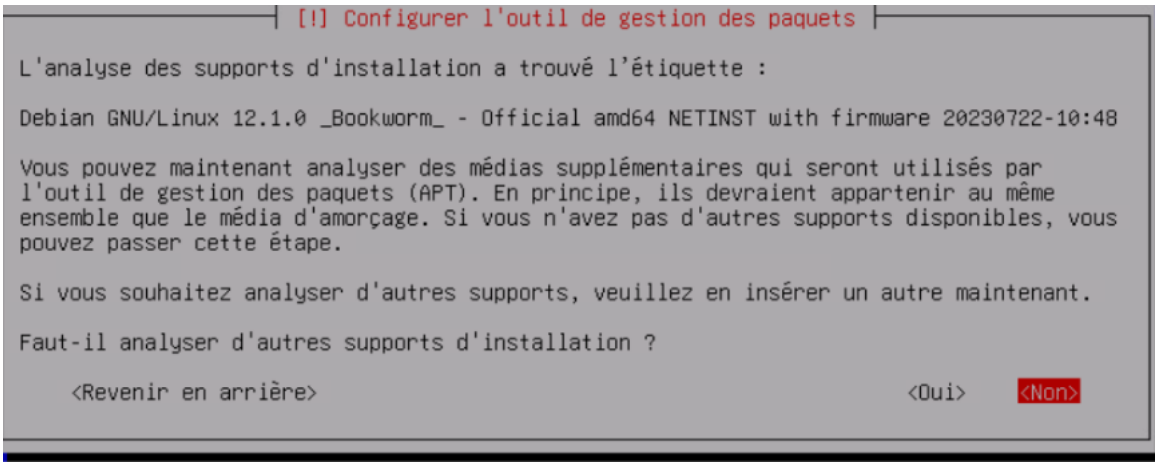
Choisir “Utiliser un disque entier” puis partitionner le disque.



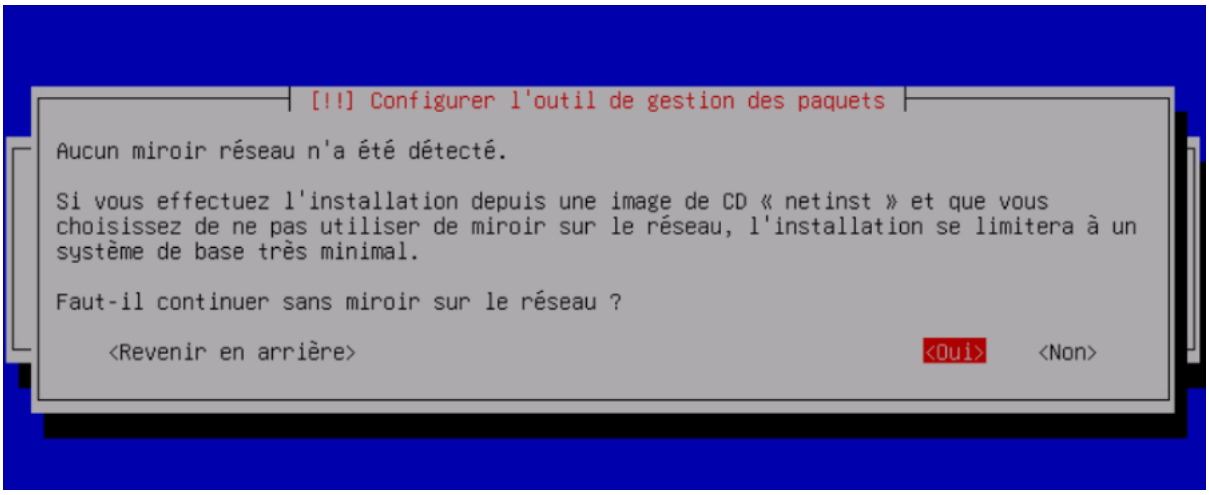
Sélectionner “Tout dans une seule partition” pour simplifier le fonctionnement, et appliquer les changements.



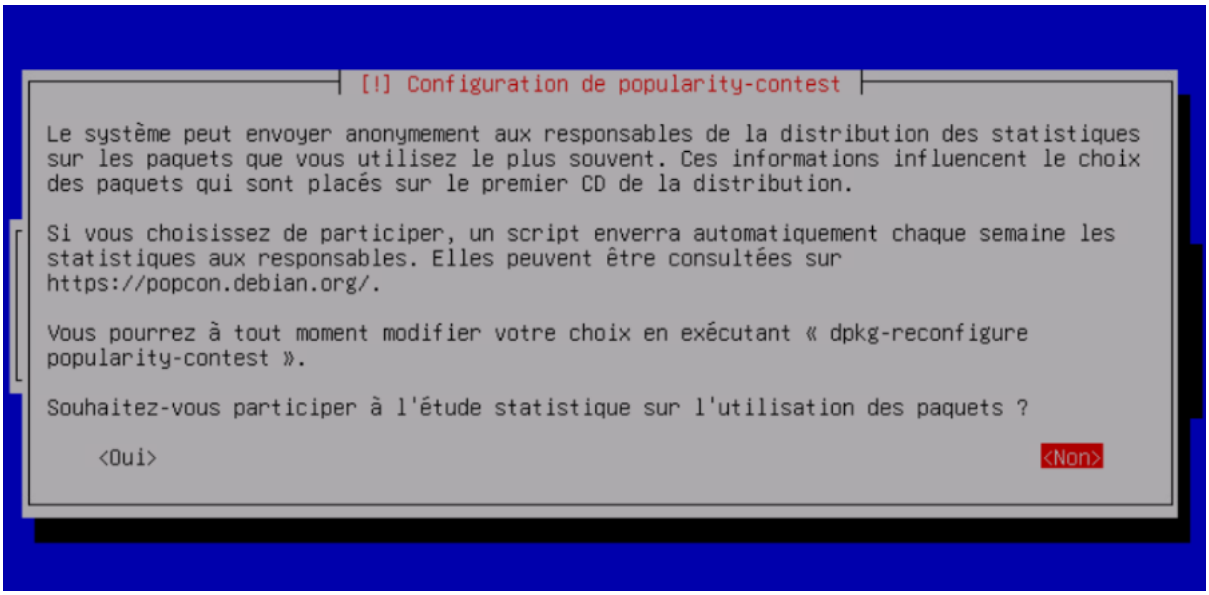
Pour l’outil de gestion de paquets sélectionner “Non”



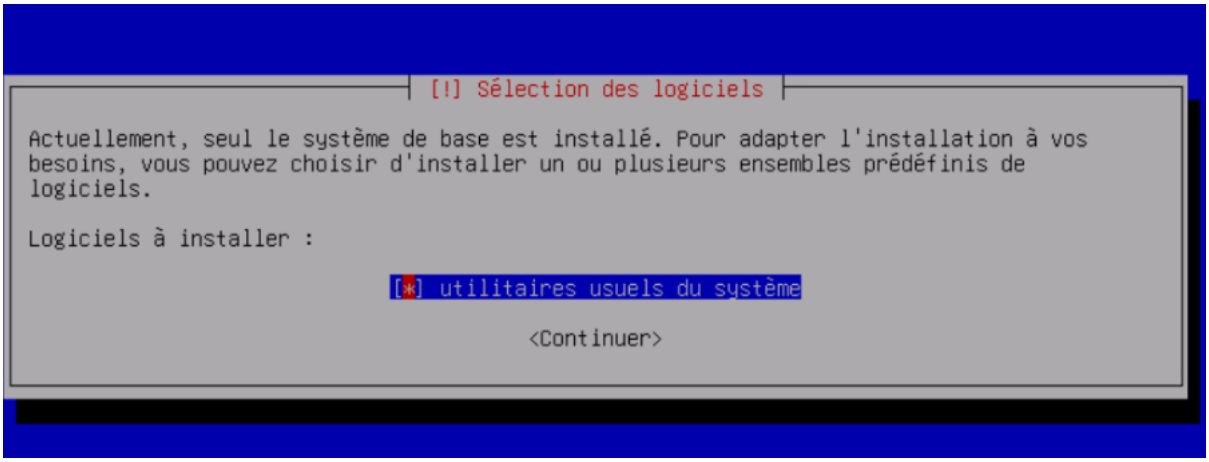
Puis, continuer sans miroir sur le réseau en sélectionnant “Oui”.



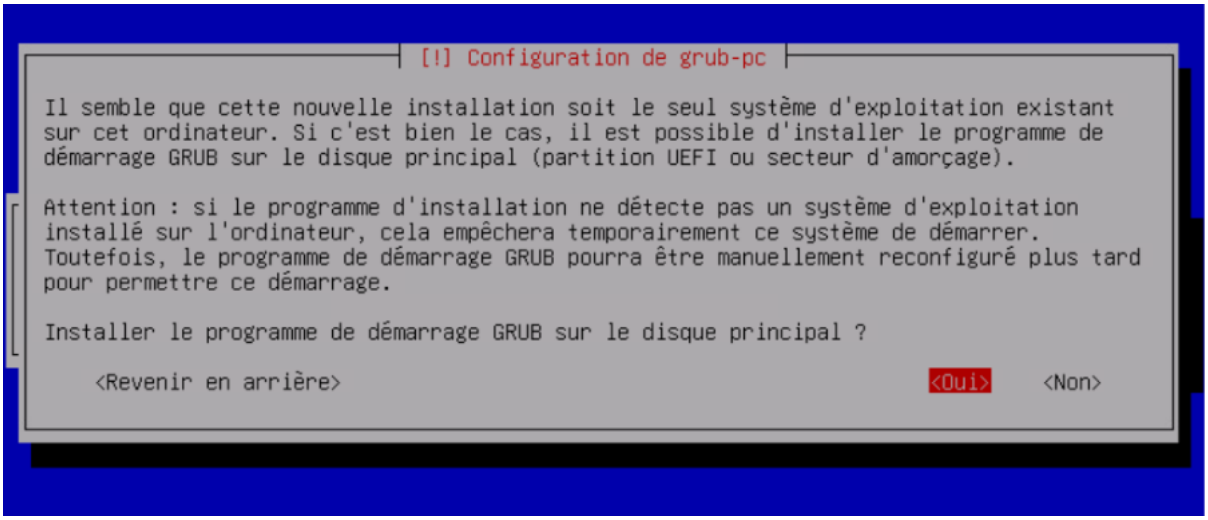
Sélectionner ”Non” afin de ne pas participer à l’étude statistique sur l’utilisation des paquets.



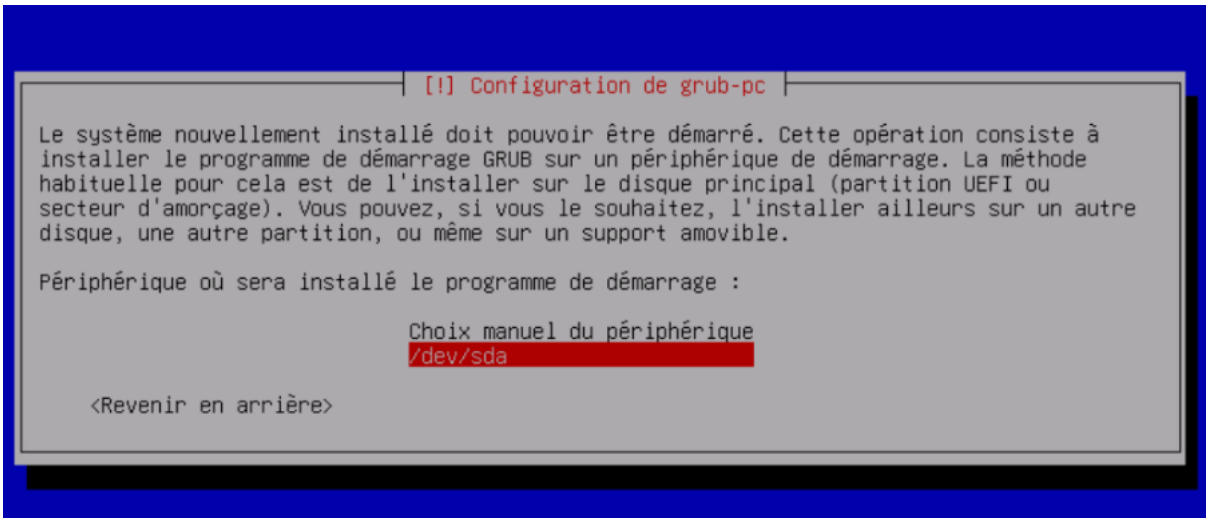
Pour la sélection des logiciels, seul ”Utilitaires usuels du système” est à sélectionner.



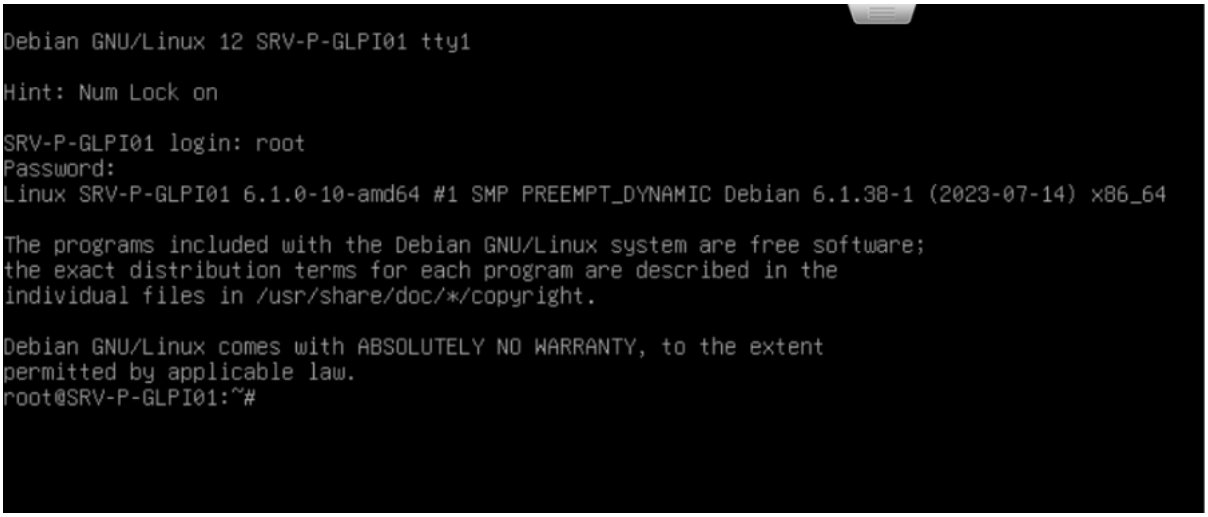
Installer le programme de démarrage Grub.



Et choisir le disque existant ”/dev/sd(a)”

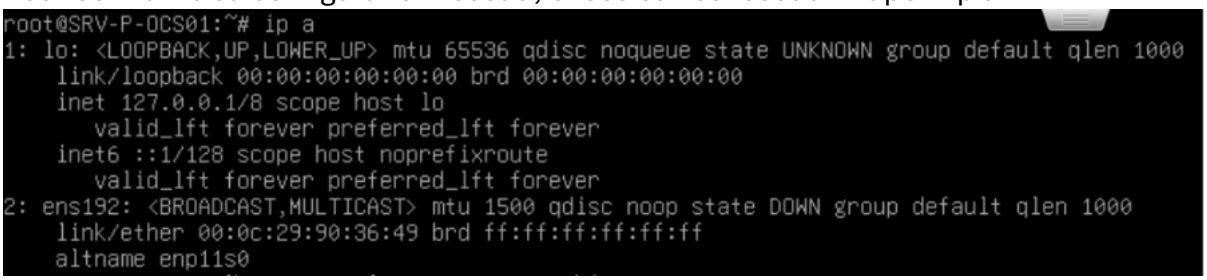


Nous voilà sur la machine virtuelle Debian sans interface graphique.



5.1.5. Configuration Réseau

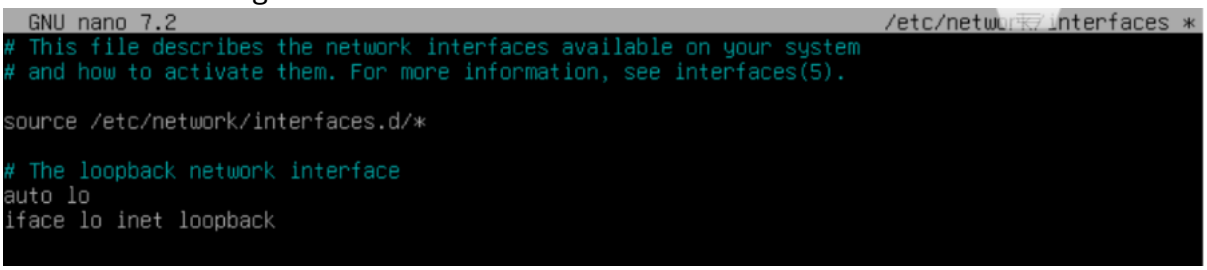
Pour connaitre sa configuration réseau, et ses cartes réseaux. Taper “ip a”.



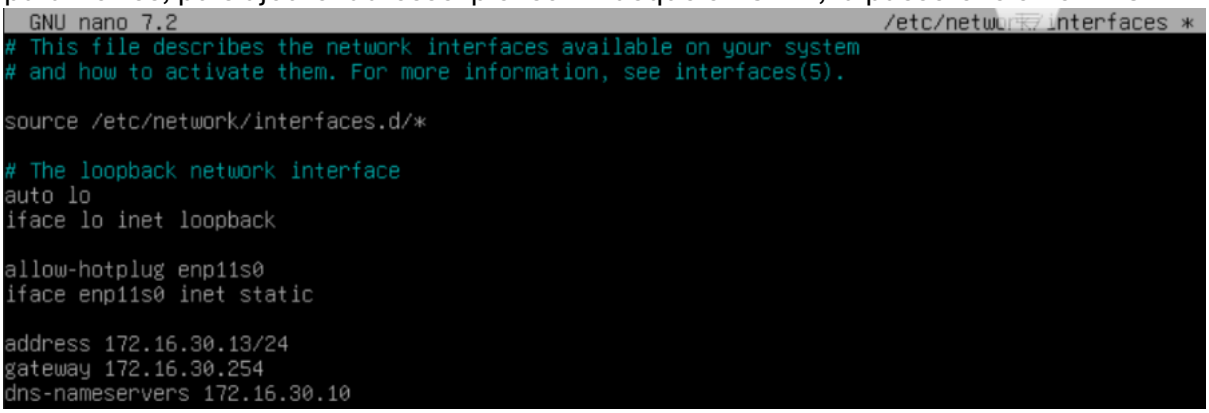
Il n’y a aucune configuration IP et on repère la carte réseau à configurer ”enp11s0”.

Pour se faire, taper “nano /etc/network/interfaces“.
Nano est un éditeur de texte natif, pas besoin d‘installer de paquet.

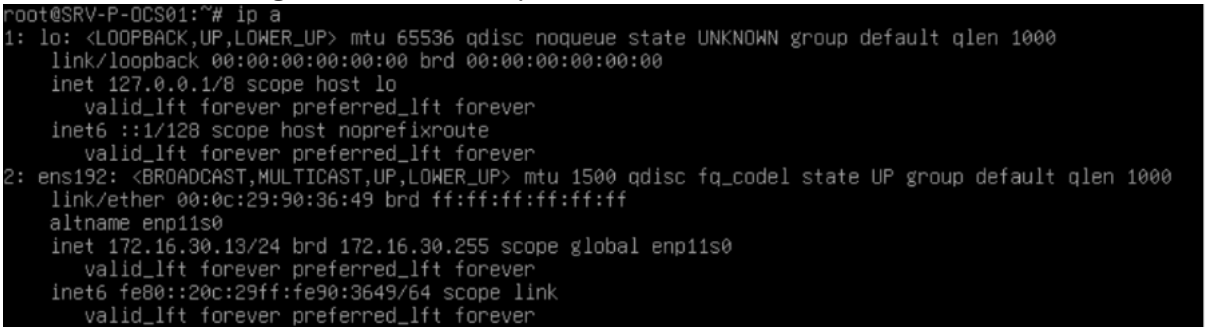
Par défaut la configuration ressemble à cela :



Pour ajouter une configuration sur la carte réseau ”enp11s0”, initialiser la carte avec des paramètres, puis ajouter adresse ip et son masque en CIDR, la passerelle et le DNS.



Taper la commande : ”systemctl restart networking” afin de redémarrer la carte réseau.
Puis vérifier la configuration IP avec ”ip a”.



5.1.6. Sources

Si l’installation de paquet échoue, il peut être bon de vérifier si les sources sont encore d’actualités, pour se faire il peut être important de mettre à jour les sources.

Se rendre sur le site https://wiki.debian.org/SourcesList

Chercher les sources pour Debian 12.

sources.list

Below is an example of a `sources.list` for Debian 12/Bookworm (stable) released 10th June 2023.

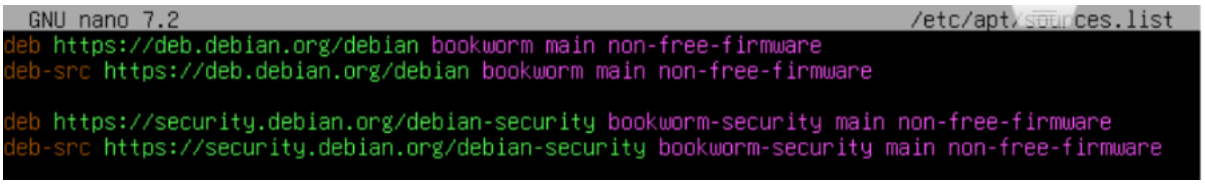
```
deb https://deb.debian.org/debian bookworm main non-free-firmware
deb-src https://deb.debian.org/debian bookworm main non-free-firmware

deb https://security.debian.org/debian-security bookworm-security main non-free-firmware
deb-src https://security.debian.org/debian-security bookworm-security main non-free-firmware

deb https://deb.debian.org/debian bookworm-updates main non-free-firmware
deb-src https://deb.debian.org/debian bookworm-updates main non-free-firmware
```

Se rendre dans le fichier des sources via ”nano /etc/apt/sources.list”

Remplacer ce qu‘il y a dans le fichier par les 4 premières lignes données sur le site.



5.2. Annexe 2 : Glossaire

SNMP (Simple Network Management Protocol) : Protocole utilisé pour superviser les équipements réseau.

NRPE (Nagios Remote Plugin Executor) : Permet d’exécuter des commandes à distance sur un serveur supervisé.

Supervision : Processus de surveillance continue des équipements et services informatiques afin de détecter les anomalies et garantir la disponibilité.

Poller (ou collecteur) : Serveur chargé d’exécuter les contrôles (checks) sur les équipements et de remonter les résultats vers Centreon.

UDP (User Datagram Protocol) : Protocole de transport non connecté permettant l’envoi rapide de données sans garantie de livraison, d’ordre ou de duplication. Utilisé notamment pour les services nécessitant de faibles latences (DNS, streaming, supervision SNMP).

TCP (Transmission Control Protocol) : Protocole de transport orienté connexion garantissant la livraison fiable, ordonnée et sans erreur des données. Utilisé pour des communications critiques (HTTP, SSH, bases de données).

ZMQ : Bibliothèque de messagerie asynchrone haute performance permettant la communication entre applications distribuées. Dans Centreon, elle peut être utilisée pour optimiser les échanges de données entre composants.

MariaDB : Système de gestion de base de données relationnelle (SGBDR) open source, dérivé de MySQL, utilisé par Centreon pour stocker les configurations et les données de supervision.

WAN (Wide Area Network) : Réseau étendu reliant plusieurs réseaux locaux (LAN) sur de grandes distances géographiques, souvent via Internet ou des liaisons privées.

DMZ (Demilitarized Zone) : Zone réseau isolée située entre le réseau interne et Internet, utilisée pour héberger des services accessibles depuis l'extérieur (serveurs web, supervision, etc.) tout en renforçant la sécurité du réseau interne.

LAN (Local Area Network) : Réseau local reliant des équipements informatiques sur une zone géographique restreinte (bâtiment, entreprise, domicile).

VPN : Le VPN (Virtual Private Network) est un outil qui permet de créer un tunnel sécurisé entre deux réseaux distants. Il permet de chiffrer les communications afin de garantir la confidentialité des données échangées entre les différents sites.

Pare-feu (Firewall) : Un pare-feu est un outil de sécurité réseau qui permet de filtrer et de contrôler le trafic entrant et sortant d'un réseau.

LDAP : Le LDAP (Lightweight Directory Access Protocol) est un protocole qui permet d'accéder à un annuaire d'entreprise. Il est utilisé pour centraliser l'authentification des utilisateurs en se basant sur un Active Directory.

5.3. Annexe 3 : Plan d'adressage IP

5.3.1. Site de Paris

VLAN 10

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.10.252	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-01 VLAN 10
FW-P-01	172.16.10.253	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-02 VLAN 10
CARP Firewall	172.16.10.254	255.255.255.0	172.16.10.0	172.16.10.254	Passerelle du VLAN 10

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.10.100-150	172.16.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Paris

VLAN 20

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
B-P-WIFI	172.16.20.50	255.255.255.0	172.16.20.0	172.16.20.254	Administration borne Wifi
FW-P-02	172.16.20.252	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-02 VLAN 20
FW-P-01	172.16.20.253	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-01 VLAN 20
CARP Firewall	172.16.20.254	255.255.255.0	172.16.20.0	172.16.20.254	Passerelle du VLAN 20

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.20.100-150	172.16.20.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Employés

VLAN 21

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.21.252	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-02 VLAN 21
FW-P-01	172.16.21.253	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-01 VLAN 21
CARP Firewall	172.16.21.254	255.255.255.0	172.16.21.0	172.16.21.254	Passerelle du VLAN 21

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.21.100-150	172.16.21.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Invité

VLAN 30

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-DC01	172.16.30.10	255.255.255.0	172.16.30.0	172.16.30.254	DC 1
SRV-P-DC02	172.16.30.20	255.255.255.0	172.16.30.0	172.16.30.254	DC 2
SRV-P-DFS01	172.16.30.50	255.255.255.0	172.16.30.0	172.16.30.254	DFS01
SRV-P-FOG01	172.16.30.11	255.255.255.0	172.16.30.0	172.16.30.254	Fog
SRV-P-OCS01	172.16.30.13	255.255.255.0	172.16.30.0	172.16.30.254	OCS Inventory
SRV-P-GLPI01	172.16.30.14	255.255.255.0	172.16.30.0	172.16.30.254	GLPI
SRV-P-BCK01	172.16.30.15	255.255.255.0	172.16.30.0	172.16.30.254	Veeam
SRV-P-CLOUD01	172.16.30.16	255.255.255.0	172.16.30.0	172.16.30.254	Nextcloud
SRV-P-RSAT-T0	172.16.30.30	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T0
SRV-P-RSAT-T1	172.16.30.31	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T1
SRV-P-RSAT-T2	172.16.30.32	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T2
SRV-P-EDR01	172.16.30.19	255.255.255.0	172.16.30.0	172.16.30.254	EDR
SRV-P-ANS01	172.16.30.21	255.255.255.0	172.16.30.0	172.16.30.254	Ansible Lille
SRV-P-NETBOX01	172.16.30.22	255.255.255.0	172.16.30.0	172.16.30.254	Outil d'infrastructure
SRV-P-POL01	172.16.30.25	255.255.255.0	172.16.30.0	172.16.30.254	Centreon Poller
FW-P-02	172.16.30.252	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-02 VLAN 30
FW-P-01	172.16.30.253	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-01 VLAN 30
CARP Firewall	172.16.30.254	255.255.255.0	172.16.30.0	172.16.30.254	Passerelle du VLAN 30

VLAN 40

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.40.252	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-02 VLAN 40
FW-P-01	172.16.40.253	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-01 VLAN 40
CARP Firewall	172.16.40.254	255.255.255.0	172.16.40.0	172.16.40.254	Passerelle du VLAN 40

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.40.100-150	172.16.40.254	172.16.30.10	172.16.30.20	Plage DHCP Déploiement

VLAN 50

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SW-P-01	172.16.50.1	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 1 Paris
SW-P-02	172.16.50.2	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 2 Paris
SRV-P-ESXI01	172.16.50.10	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
SRV-P-ESXI02	172.16.50.20	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
PAW-P-T0	172.16.50.50	255.255.255.0	172.16.50.0	172.16.50.254	Machine d'administration
FW-P-02	172.16.50.252	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-02 VLAN 50
FW-P-01	172.16.50.253	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-01 VLAN 50
CARP Firewall	172.16.50.254	255.255.255.0	172.16.50.0	172.16.50.254	Passerelle du VLAN 50

VLAN 60

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-01	172.16.60.1	255.255.255.252	172.16.60.0	-	IP FW-P-01 VLAN 60
FW-P-02	172.16.60.2	255.255.255.252	172.16.60.0	-	IP FW-P-02 VLAN 60

VLAN 99

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-HAProxy	172.16.99.10	255.255.255.0	172.16.99.0	172.16.99.254	HAProxy
FW-P-02	172.16.99.252	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-02 VLAN 99
FW-P-01	172.16.99.253	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-01 VLAN 99
CARP Firewall	172.16.99.254	255.255.255.0	172.16.99.0	172.16.99.254	Passerelle du VLAN 99

5.3.2. Site Marseille

Marseille

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-M-01	172.17.10.254	255.255.255.0	172.17.10.0	172.17.10.254	IP FW-M-01 VLAN 10 Marseille
FW-M-01	10.44.110.112	255.255.255.0	10.44.110.0	10.44.110.254	IP WAN Marseille

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.17.10.100-150	172.17.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Marseille

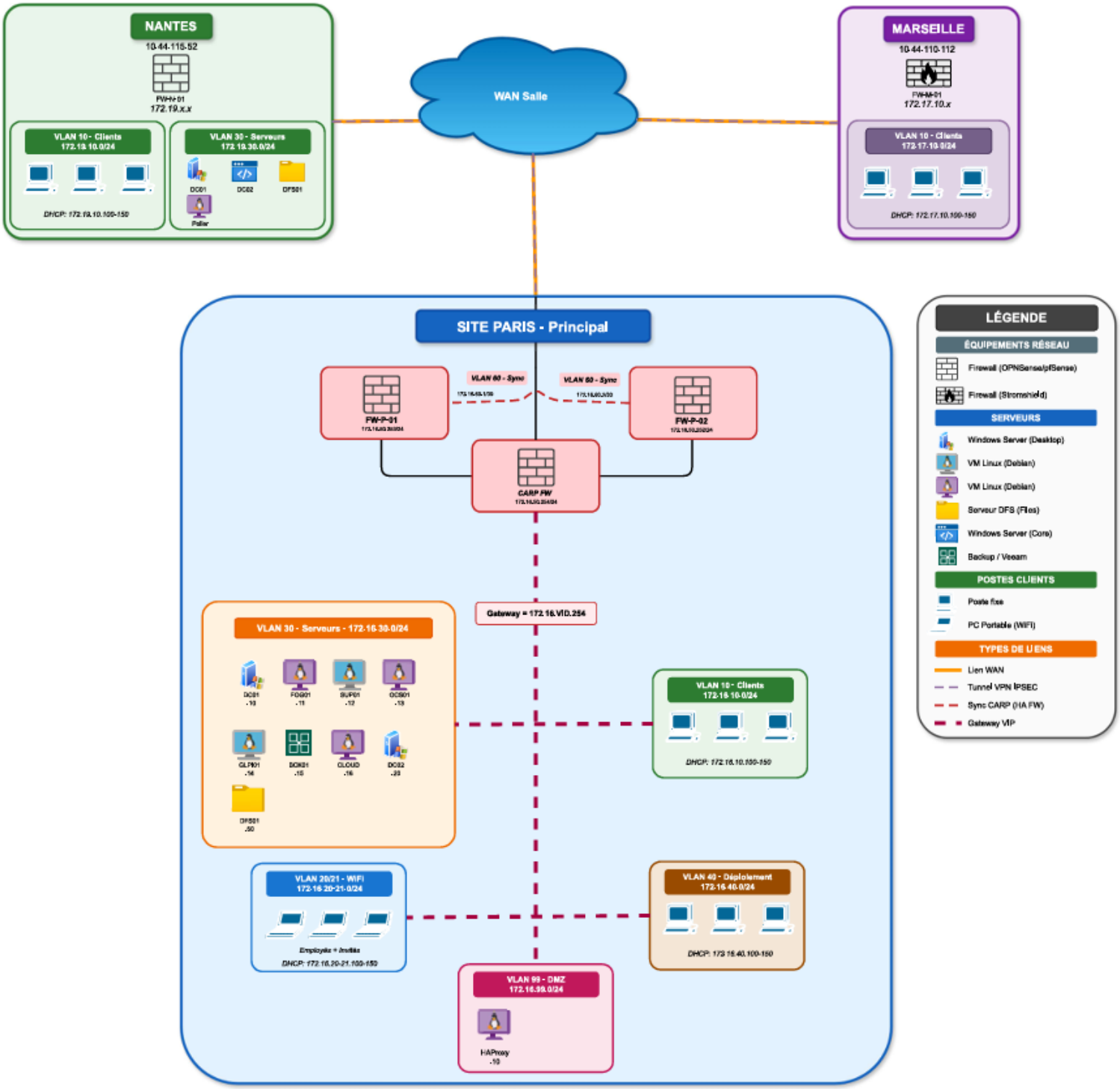
5.3.3. Site Nantes

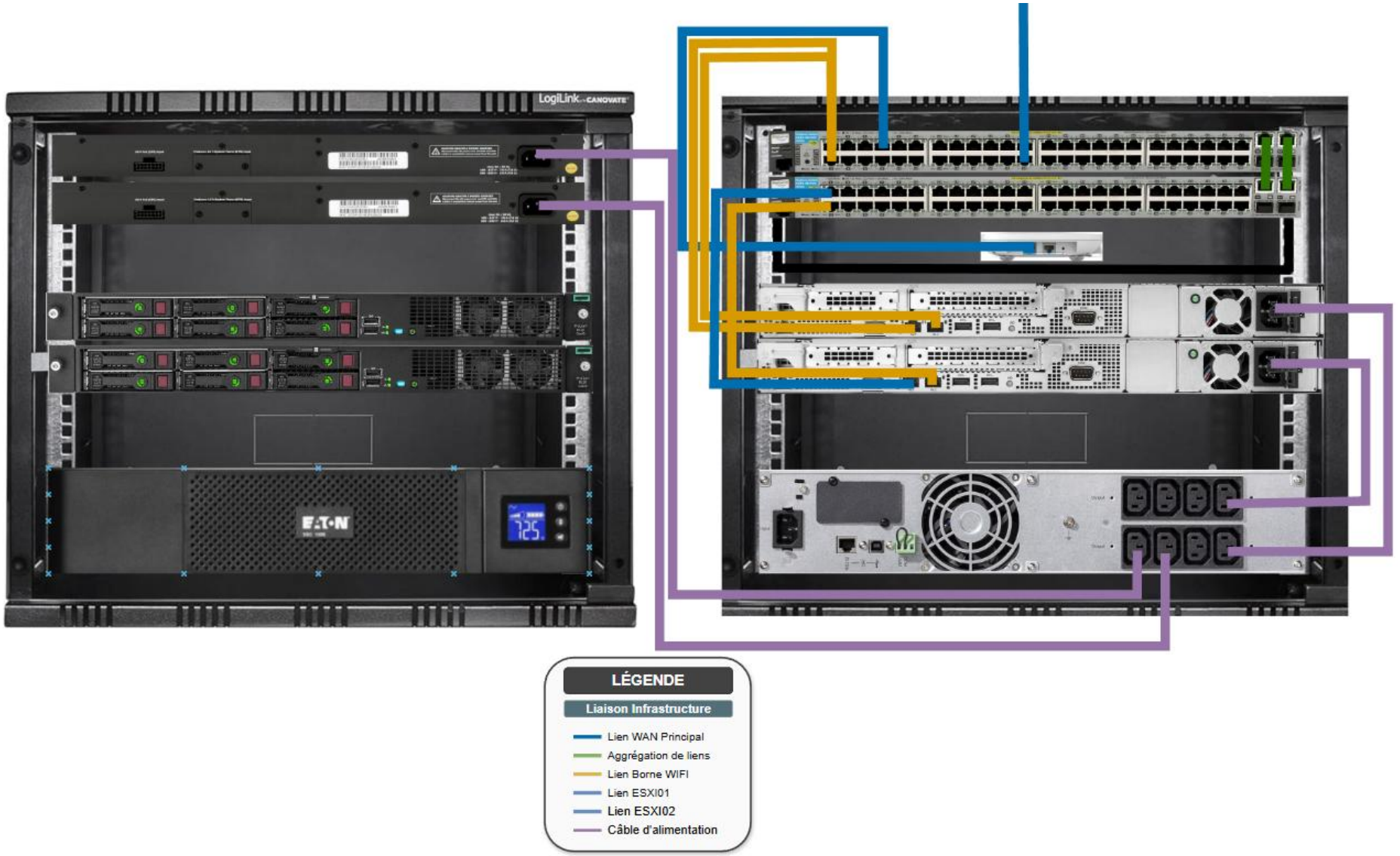
Nantes

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-N-DC01	172.19.30.10	255.255.255.0	172.19.30.0	172.19.30.254	DC1 Nantes
SRV-N-DC02	172.19.30.11	255.255.255.0	172.19.30.0	172.19.30.254	DC2 Core Nantes
SRV-N-SUP01	172.19.30.12	255.255.255.0	172.19.30.0	172.19.30.254	Centreon Central
SRV-N-POL01	172.19.30.25	255.255.255.0	172.19.30.0	172.19.30.254	Centreon Poller
FW-N-01	172.19.10.254	255.255.255.0	172.19.10.0	172.19.10.254	IP FW-N-01 NAN Nantes
FW-N-01	172.19.30.254	255.255.255.0	172.19.30.0	172.19.30.254	IP FW-N-01 SRV Nantes
FW-N-01	172.19.99.254	255.255.255.0	172.19.99.0	172.19.99.254	IP FW-N-01 DMZ Nantes
FW-N-01	10.44.115.52	255.255.255.0	10.44.115.0	10.44.115.254	IP WAN Nantes

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.19.10.100-150	172.19.10.254	172.19.30.10	172.19.30.20	Plage DHCP Client Nantes

5.4. Annexe 4 : Schéma logique de l'ensemble de l'infrastructure d'OASIS et physique du site de Paris




LÉGENDE
Liaison Infrastructure
Lien WAN Principal
Aggrégation de liens
Lien Borne WIFI
Lien ESXI01
Lien ESXI02
Câble d'alimentation