XXII

Guide d’installation

XXII CORE REAL TIME
V.2.0.0

Version guide (Milestone) **- 2.0**

Auteurs & historique des modifications.

Contributeurs

Auteurs	Postes
Nathan LAFONTAINE	Technical Manager
Stanislas MAHIEUX	Directeur de la formation

Historique du document

Auteurs	Date	Modifs
Nathan LAFONTAINE	5 Janvier 2023	Création du document
Stanislas MAHIEUX	18 Janvier 2023	Création du document

Sommaire.

Guide de paramétrage (MILESTONE) - XXII CORE REAL TIME

[1] Pré-requis

Voici la liste des prérequis avant de continuer l'installation, attention cette liste est pour la version R1 2021 du XProtect Corporate :

Name	Description
Operating System	Microsoft® Windows® 8.1 Pro (64 bit)
	Microsoft® Windows® 8.1 Enterprise (64 bit)
	Microsoft® Windows® 10 Pro (64 bit)
	Microsoft® Windows® 10 Enterprise (64 bit)
	Microsoft® Windows® 10 IoT Enterprise LTSB (Long-Term Servicing Branch)2016 (version 1607 or later)
	Microsoft® Windows® 10 IoT Enterprise, version 1803 or later (64 bit), IoT Core
	Microsoft® Windows® Server 2012 (64 bit): Standard and Datacenter
	Microsoft® Windows® Server 2012 R2 (64 bit): Standard and Datacenter
	Microsoft® Windows® Server 2016 (64 bit): Essentials, Standard and Datacenter
	Microsoft® Windows® Server 2019 (64 bit): Essentials, Standard and Datacenter
	To run clustering/failover management servers, you need a Microsoft® Windows® Server 2012/2012 R2 Standard or Datacenter edition, Microsoft® Windows® Server 2016 Standard or Datacenter edition, or a Microsoft® Windows® Server 2019 Standard or Datacenter edition
File system	For the Recording Storage Location, NTFS file system is recommended
SQL Versions	Microsoft SQL Server® 2012 SP1
	Microsoft SQL Server® 2014
	Microsoft SQL Server® 2016
	Microsoft SQL Server® 2017
	Microsoft SQL Server® 2019 (Only supported on Microsoft® Windows® 10 or greater and Microsoft® Windows® Server 2016 or greater)
Software	Microsoft® .NET 4.7.2 Framework
	Microsoft® .NET Core 3.1.13 Framework
	DirectX 11 or newer
Hardware acceleration	Hardware acceleration with Intel® Quick Sync requires an Intel® CPU from 4th generation up to 11th generation, supporting Intel Quick Sync and Intel® GPU enabled in BIOS.
	Decoding with NVIDIA graphics card is supported with GPU capability version 6.x (Pascal) or newer.

Prérequis pour les autres système de Milestone, rendez-vous sur cette page : https://www.milestonesys.com/fr/support/tools-and-references/system-requirements/

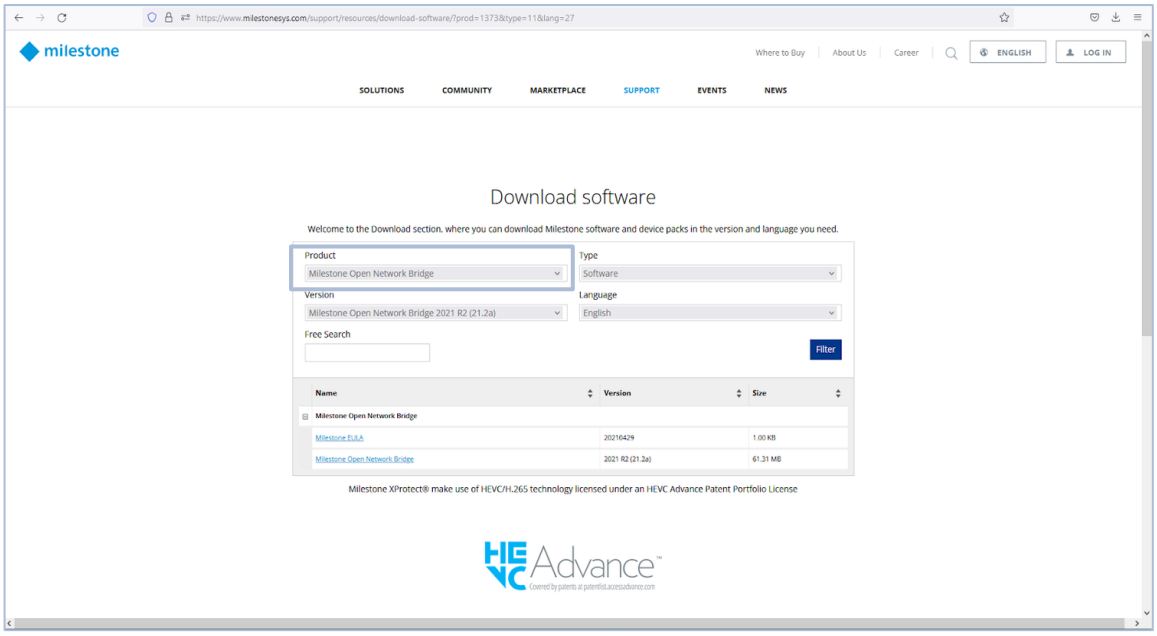
[2] Milestone Open Network Bridge

1 - Pourquoi XXII Core a besoin du Milestone Open Network Bridge ?

- XXII Core a besoin du Milestone Open Network Bridge afin d'accéder aux flux RTSP des caméras enregistrées dans le logiciel Milestone XProtect. Les flux RTSP sont ensuite lus par XXII Core afin de réaliser les traitements programmés par l'utilisateur.

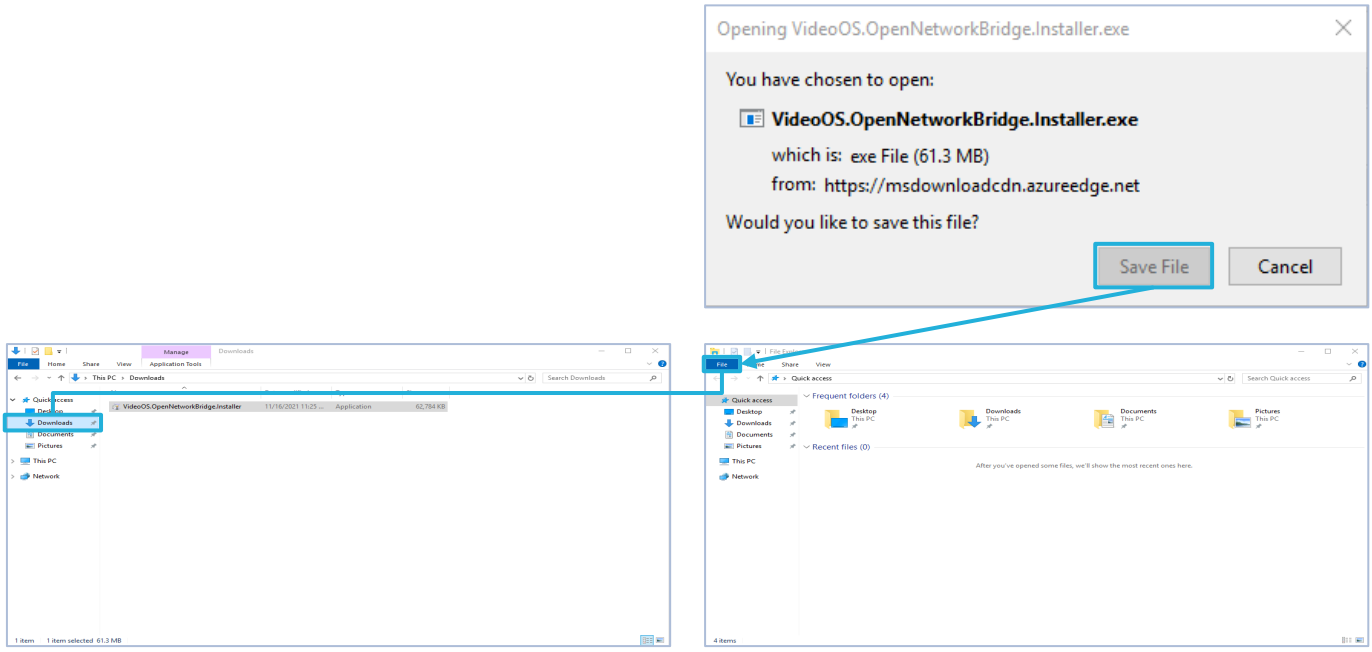
2 - Télécharger Milestone Open Network Bridge

- Rendez-vous sur le centre de téléchargement de Milestone à l'adresse suivante : https://www.milestonesys.com/fr/support/ressources/download-software/



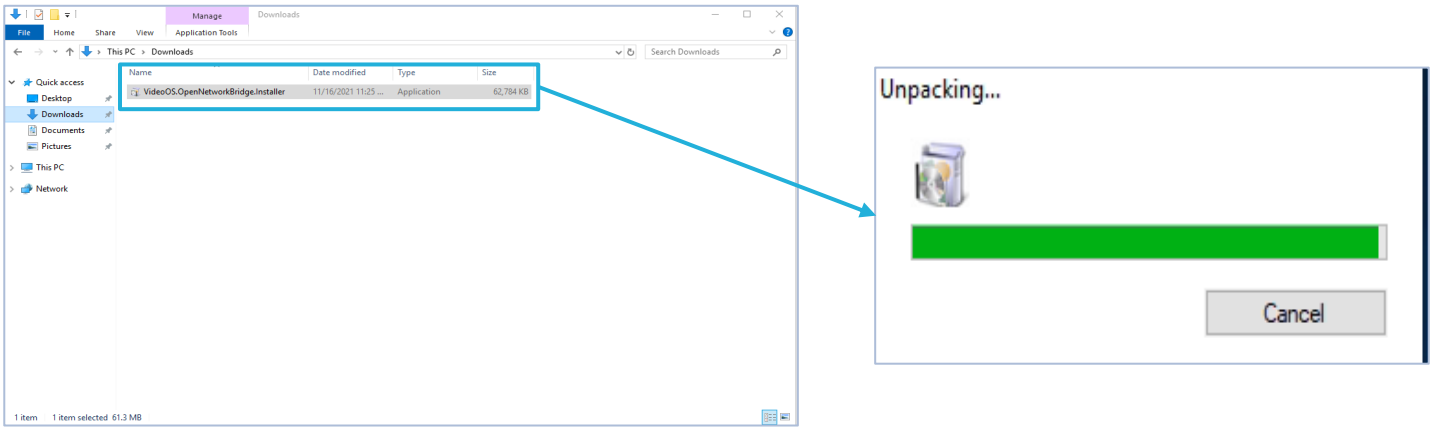
- Sélectionner Milestone Open Network Bridge pour le télécharger.

- Cliquer sur “Save File” puis aller dans l’explorateur de fichier Windows, puis dans Download.

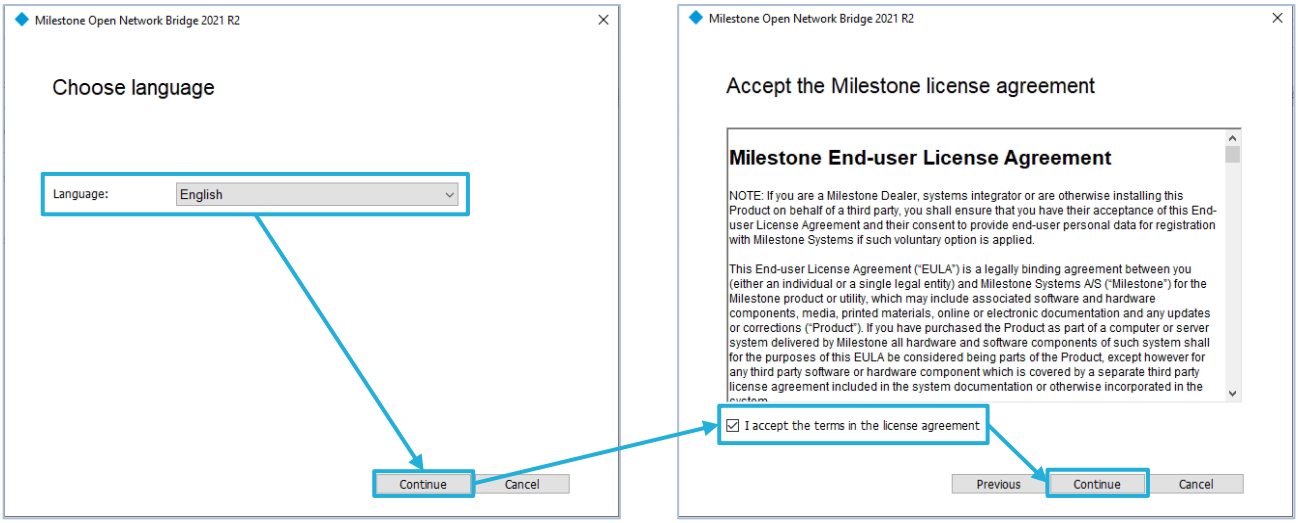


3 - Installation du Milestone Open Network Bridge

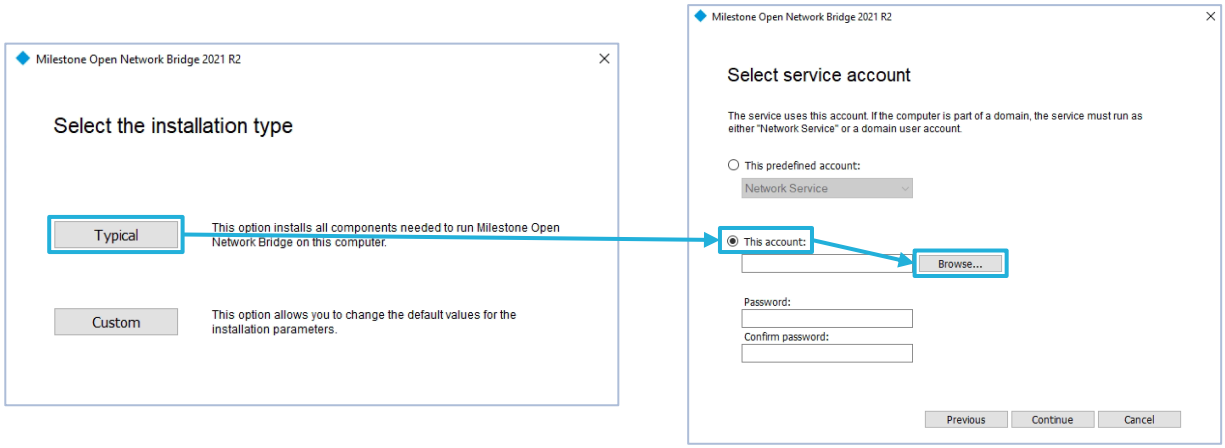
- Clique droit sur VideoOS[...].Installer, puis “Run as administrator”



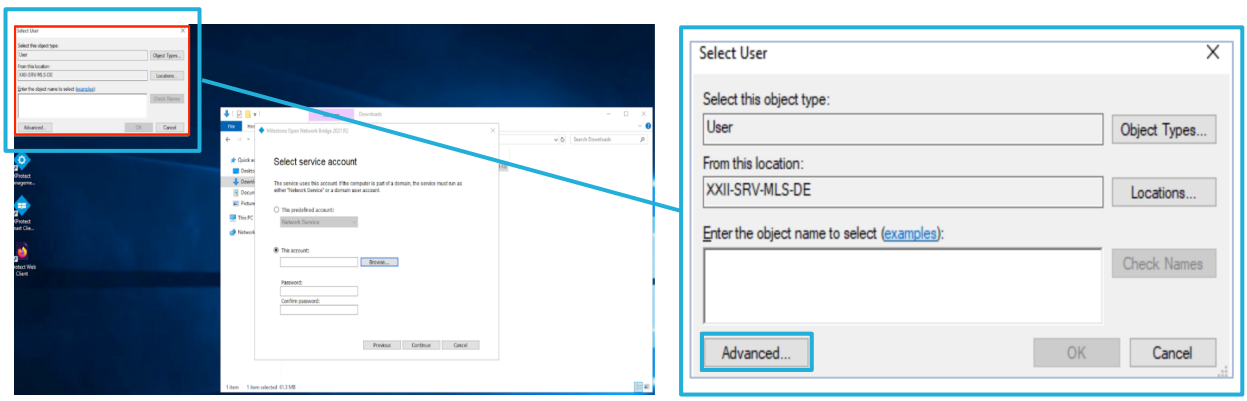
- Sélectionner la langue et cliquer sur continue.



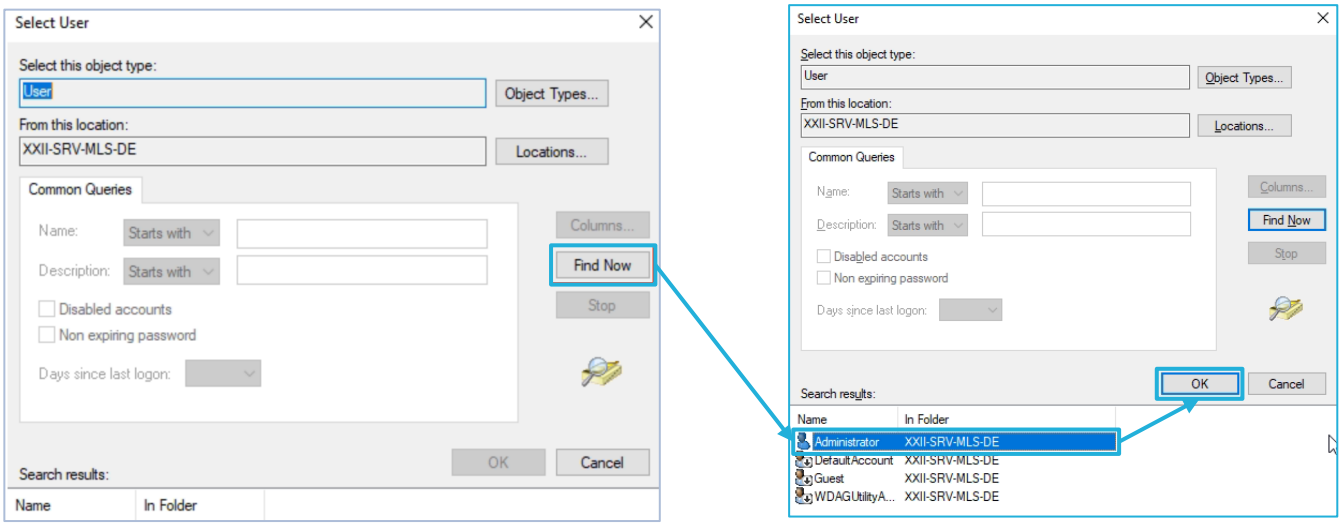
- Type d'installation : choisir "Typical"
- Cliquer sur "This account" puis sur "browse"



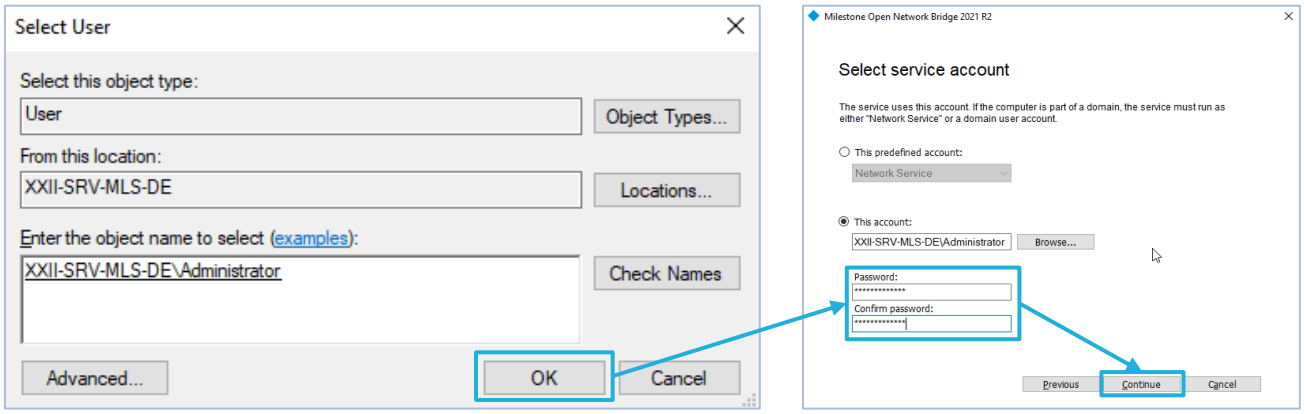
- Cliquer sur "advanced"



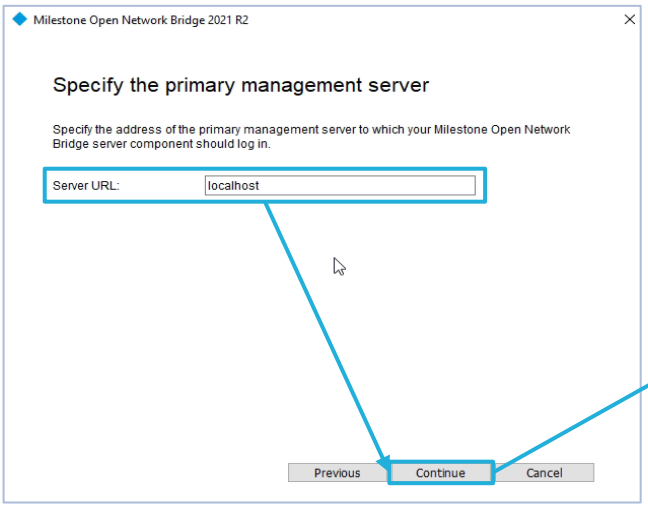
- Cliquer sur “**Find Now**”
- Sélectionner “**Administrator**“ et cliquer sur “**OK**”

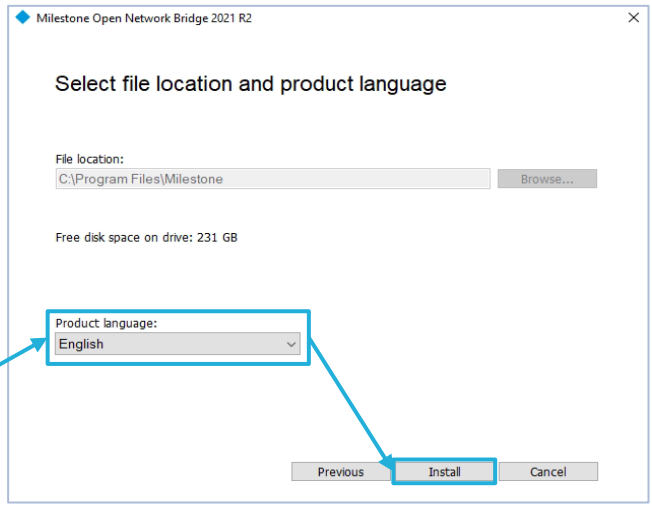


- Voici l’affichage désirée, cliquez sur “**OK**”
- Entrez le “**mot de passe**” du compte Windows Administrator ou Administrateur précédemment choisi, puis cliquez sur “**Continue**”

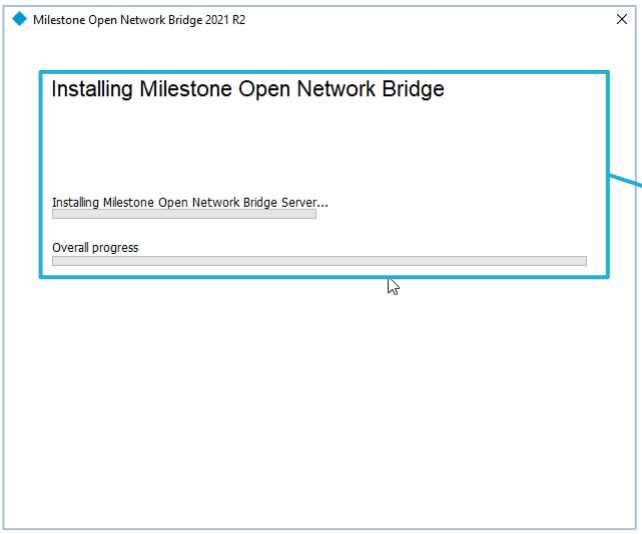


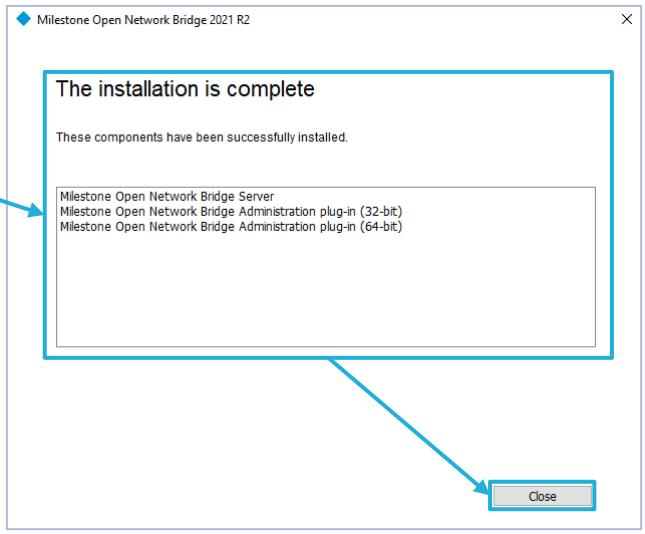
- Laisser “**localhost**” dans le champ “**Server URL**” et cliquer sur “**Continue**”
- Choisir la langue et cliquer sur “**Install**”





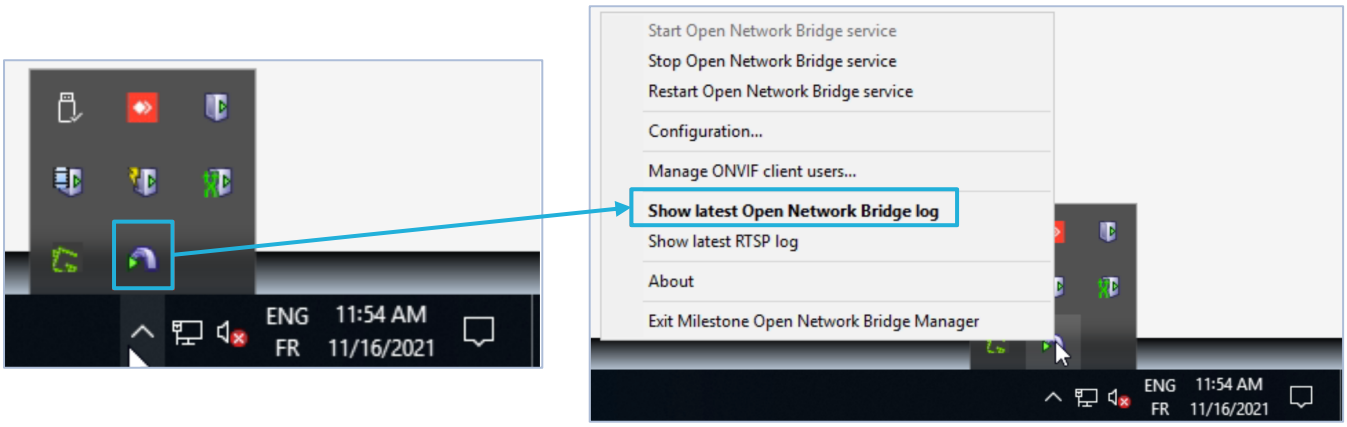
- Lorsque le téléchargement est terminé, cliquer sur “**Close**”





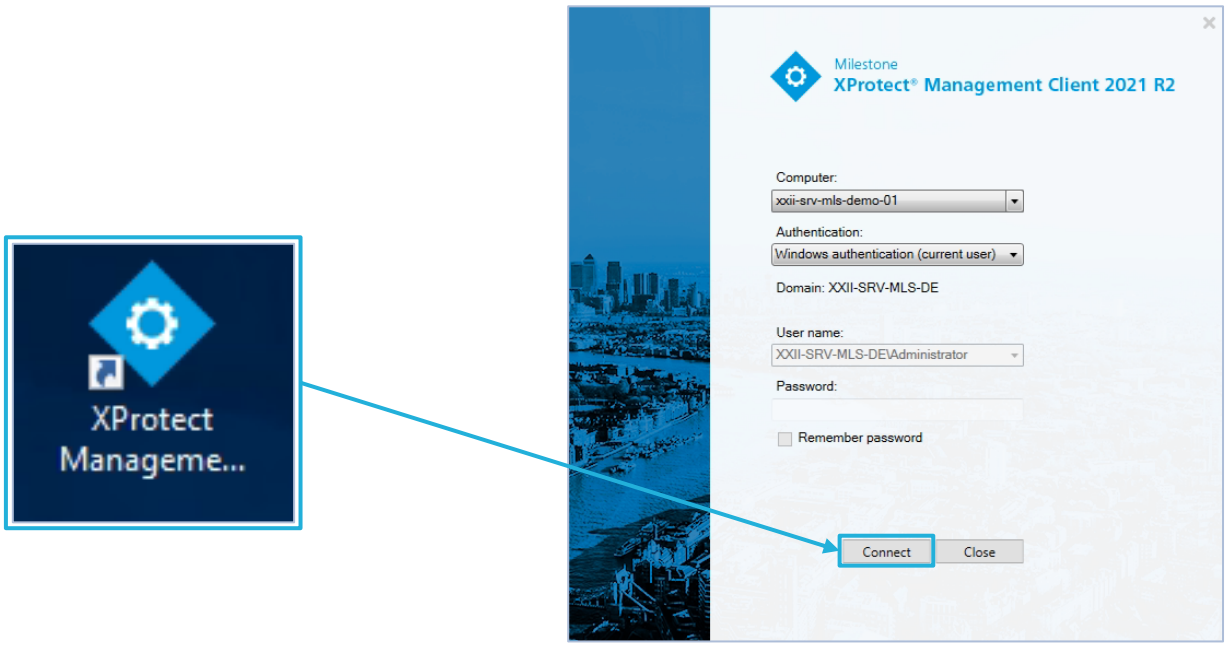
4 - Vérification du statut du Milestone Open Network Bridge

- Une fois l'installation complète, le logiciel Milestone Open Network Bridge est lancé. Vérifiez dans la barre d'état des programmes Windows.
- Sélectionner, à l'aide du "clic droit", l'icône du Milestone Open Bridge, puis "**Show [...] Bridge log**"

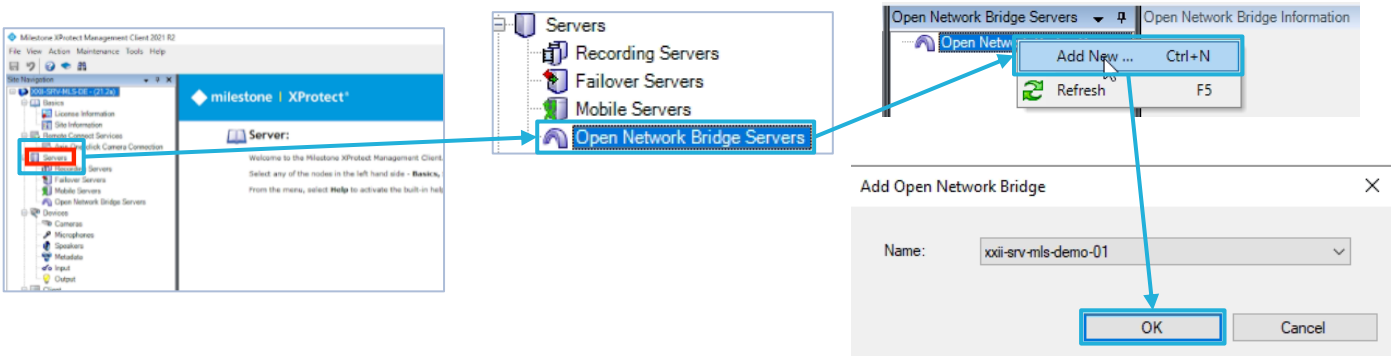


5 - Ajout du Milestone Open Network Bridge

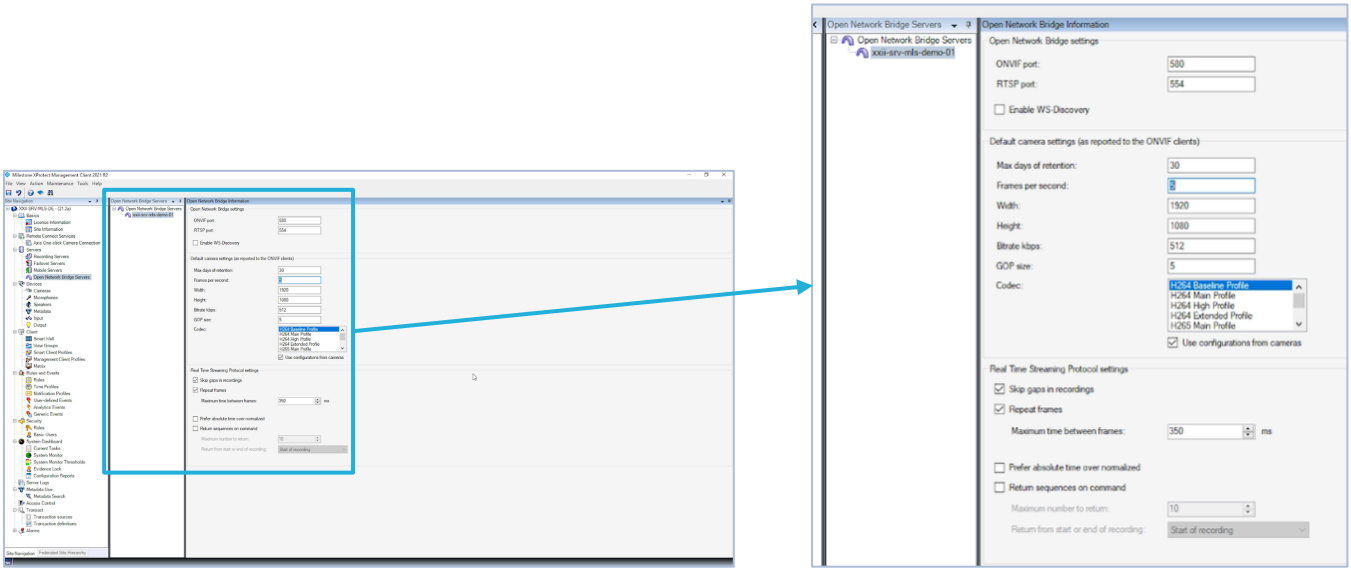
- Ouvrir le programme "**XProtect Management**"
- S'identifier et cliquer sur "**Connect**"



- Sur la page principale du Management Client, cliquer sur “Server” dans le menu de gauche
- Dans la liste des serveurs, choisir “Open Network Bridge”
- “clic droit” et cliquer sur “Add New” puis “OK”

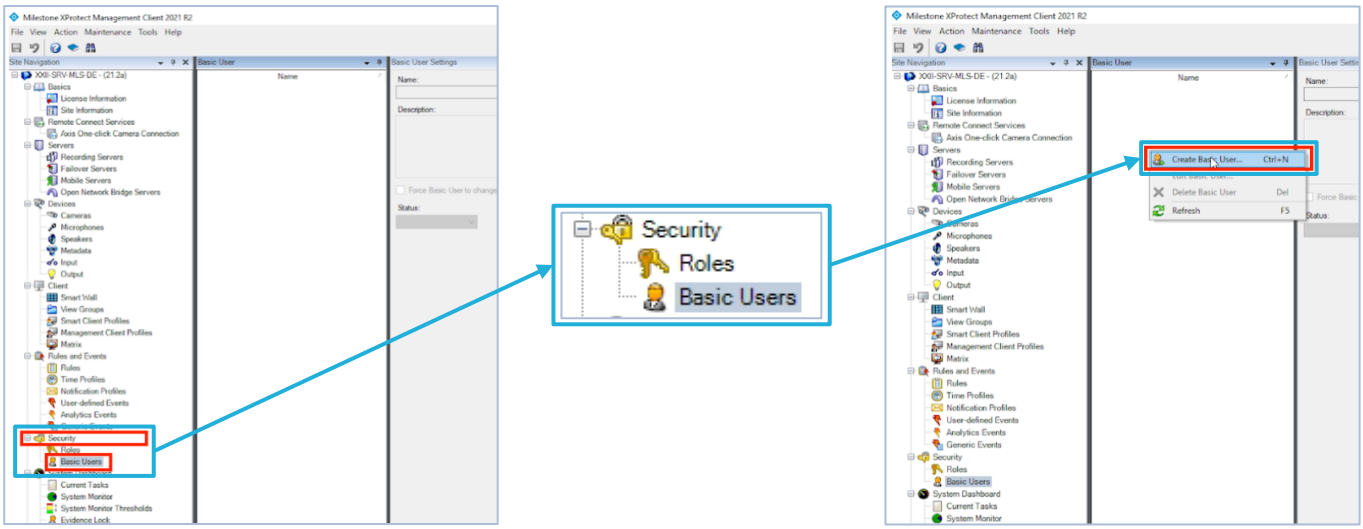


- L’Open Network Bridge est correctement ajouté

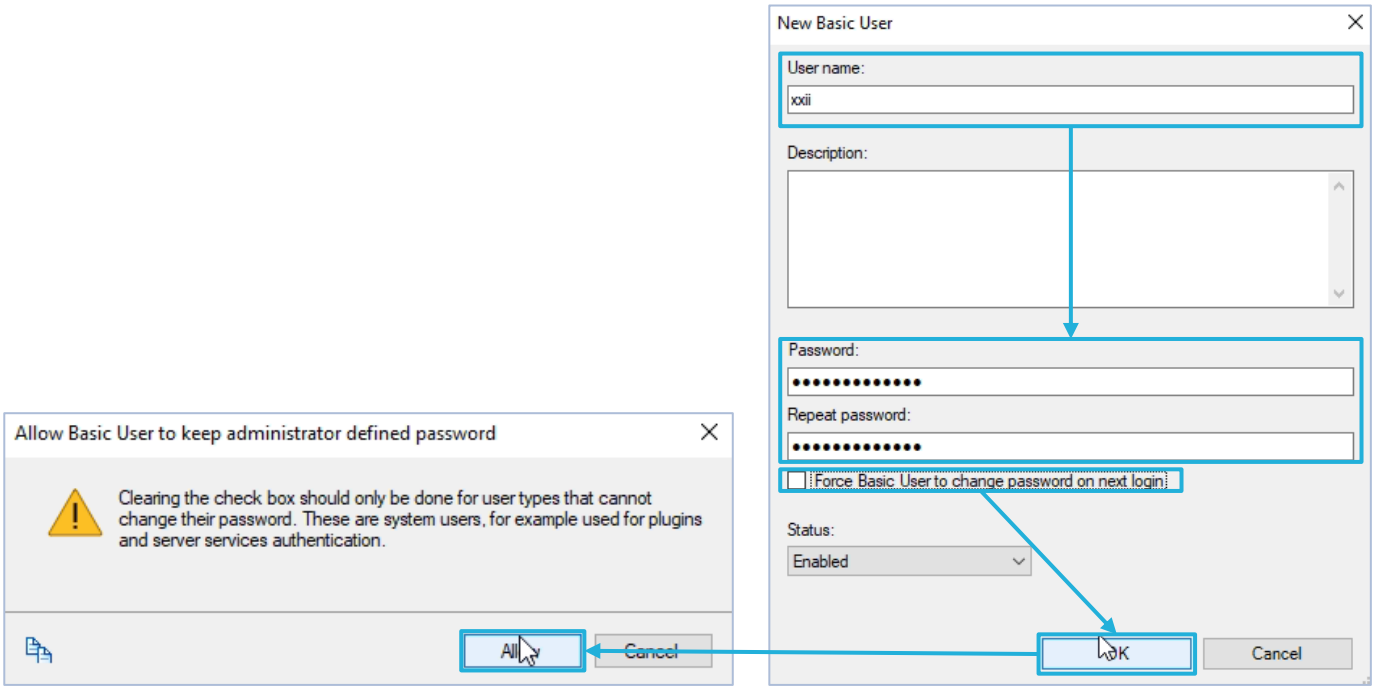


6 - Création d'utilisateur de Milestone Management Client

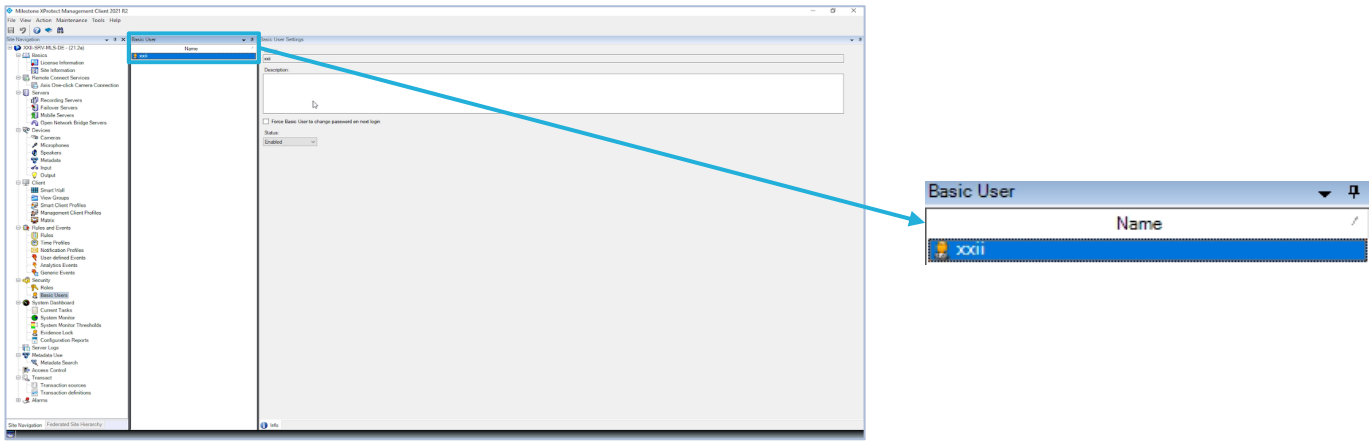
- Dans la colonne de gauche de l'écran, aller dans “Security”, puis “Basic User”
- Faire un “clic droit” sur “Basic Users”, puis cliquer sur “Create Basic User”



- Une nouvelle fenêtre s’ouvre pour ajouter un utilisateur, entrer les informations d’utilisateur
- Décocher la case “Force Basic [...] Login” puis cliquer sur “OK”

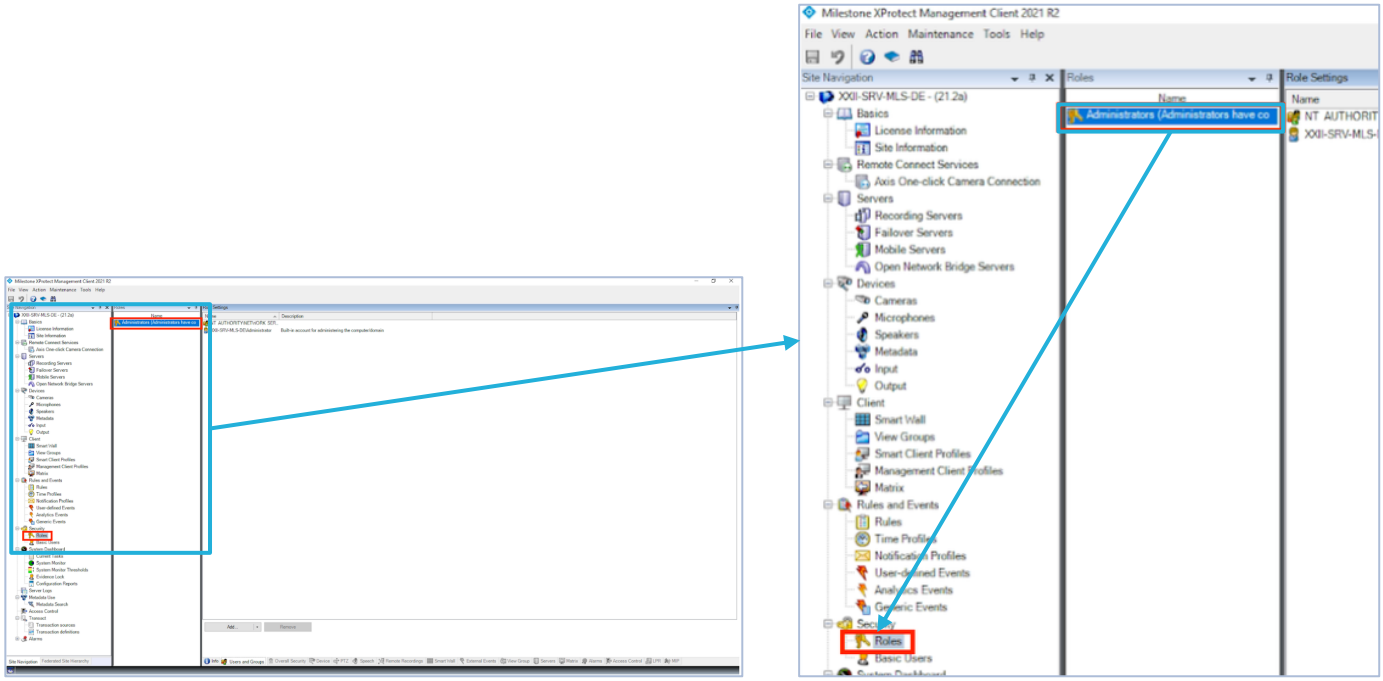


- Après avoir ajouté un utilisateur au Milestone Open Network Bridge, un utilisateur est maintenant disponible dans la partie “Basic User” sur la partie gauche de l'écran.



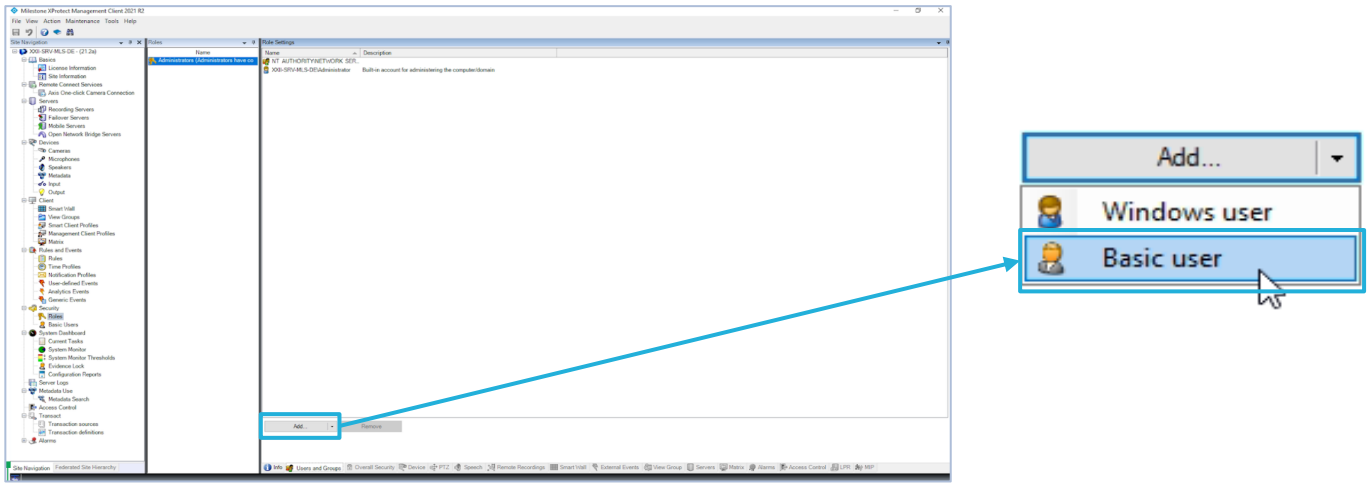
7 - Création de rôles pour l’utilisateur du Management Client

- Dans la partie gauche de l'écran, aller dans “Security”, puis “Rôles”

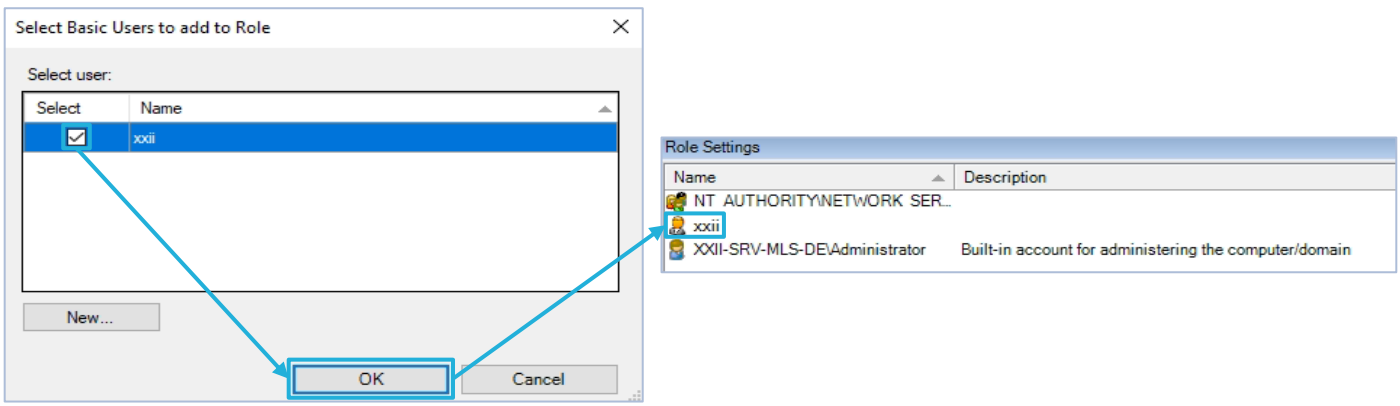


- En bas de l'écran sélectionner “Users and Groups”

- Cliquer sur “Add”, puis “Basic user”

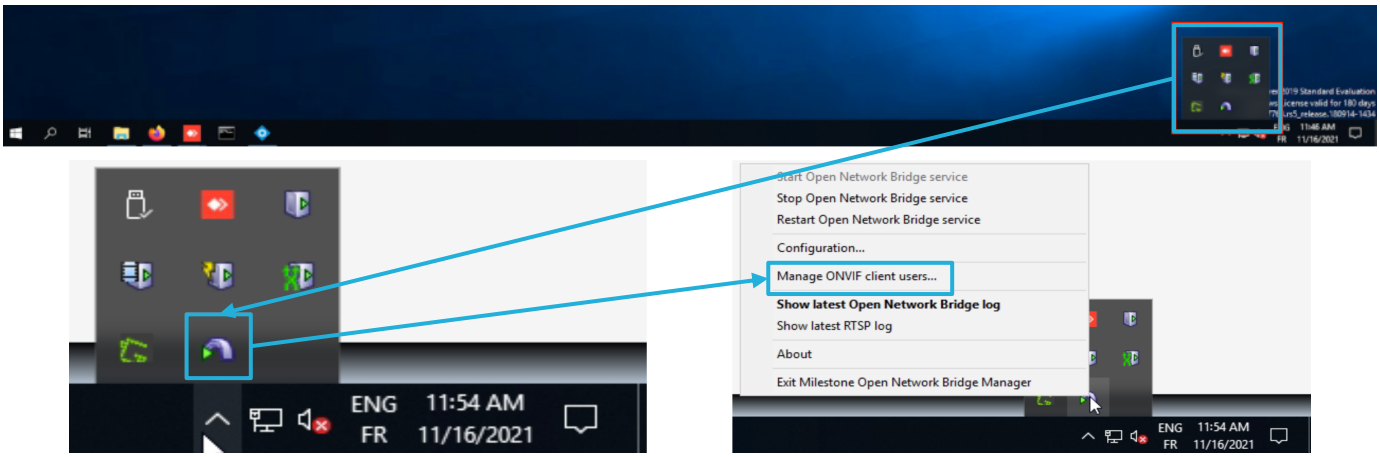


- Sélectionner l’utilisateur récemment ajouté et cliquer sur “OK”
- L’utilisateur est maintenant dans la liste des rôles

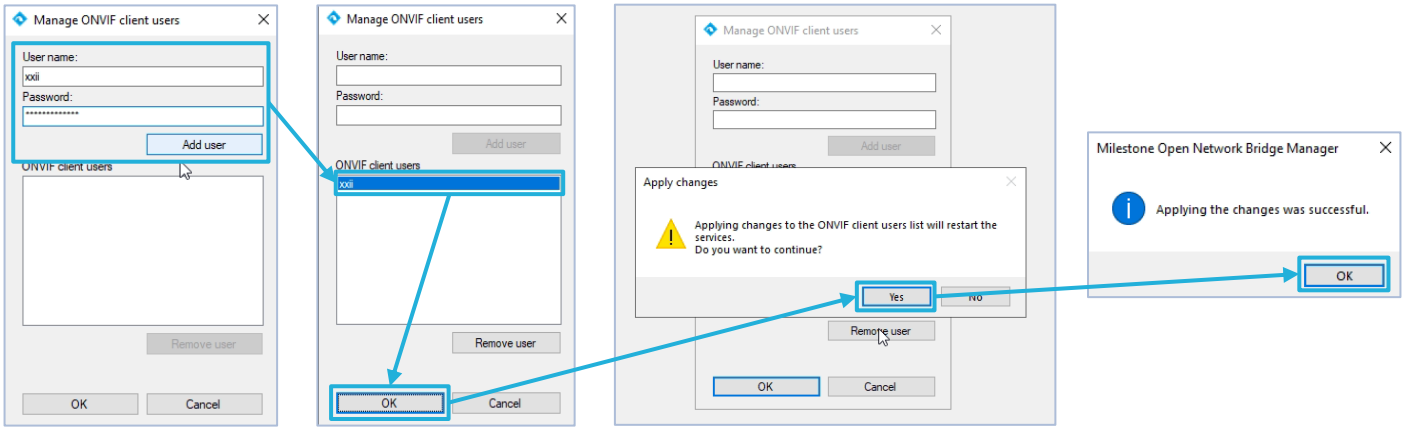


8 - Création de l'utilisateur du Milestone Open Network Bridge

- Dans la barre d'état des programmes Windows, cliquer sur la petite flèche, sur la droite.
- Faire un "clic droit" sur l'icône du Milestone Open Bridge, puis "Manage [...] user..."

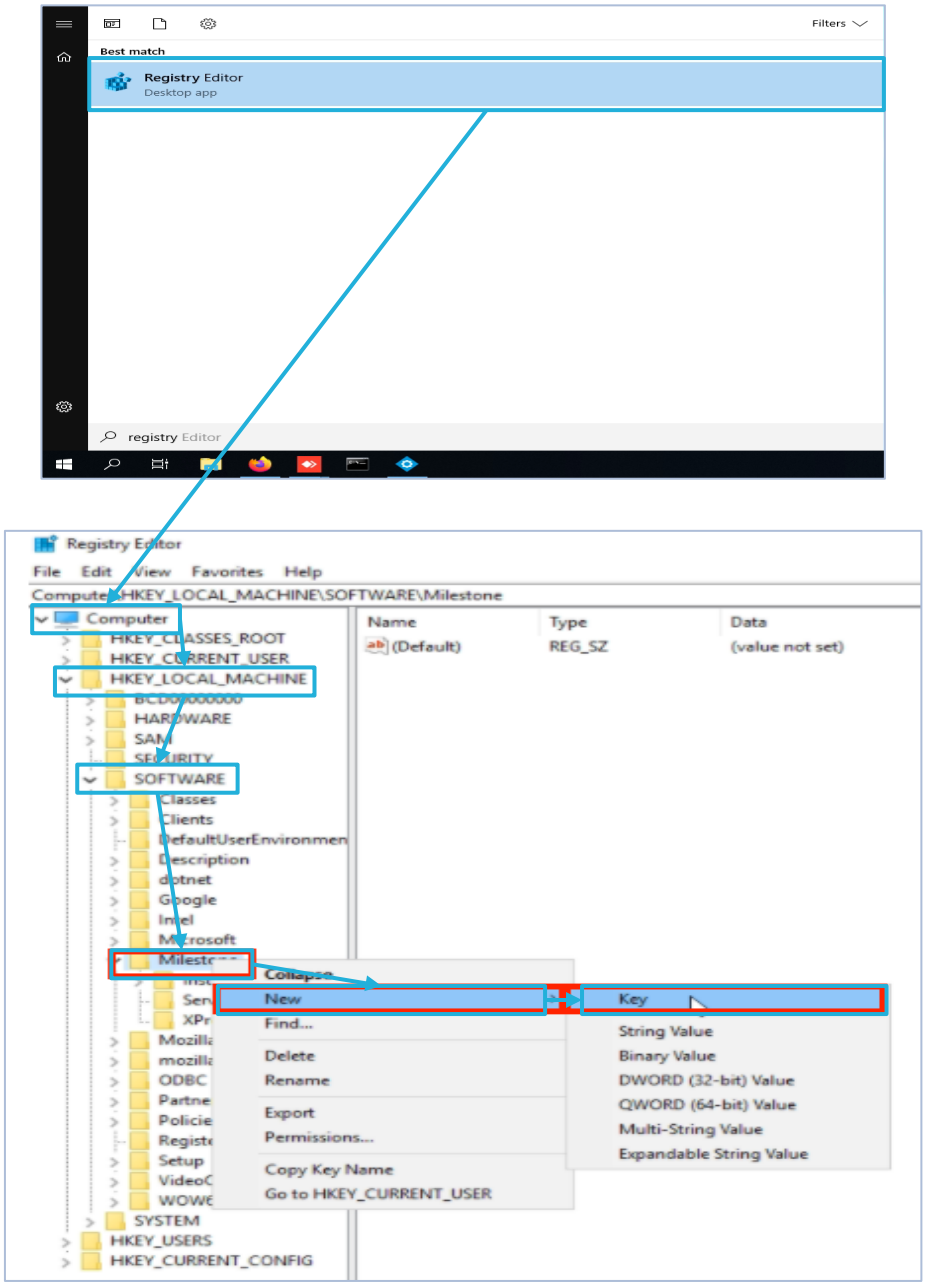


- Ajouter un nouvel utilisateur et un mot de passe, puis cliquer sur "Add user"
- L'utilisateur est à présent visible dans la liste, cliquer sur "Ok", puis sur "Yes" et enfin sur "OK"

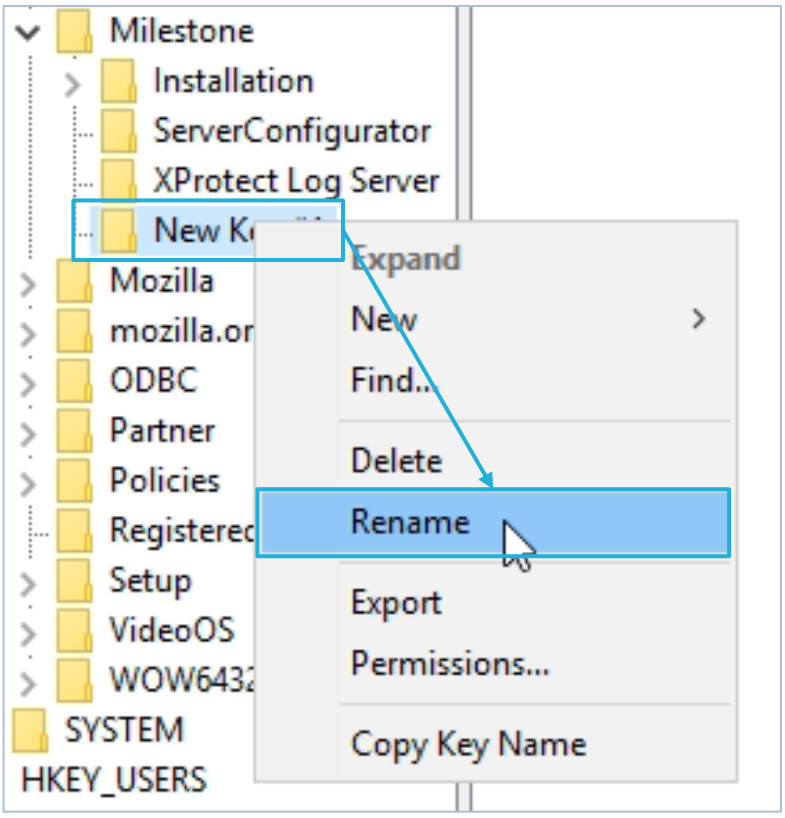


9 - Ajouter le Registry

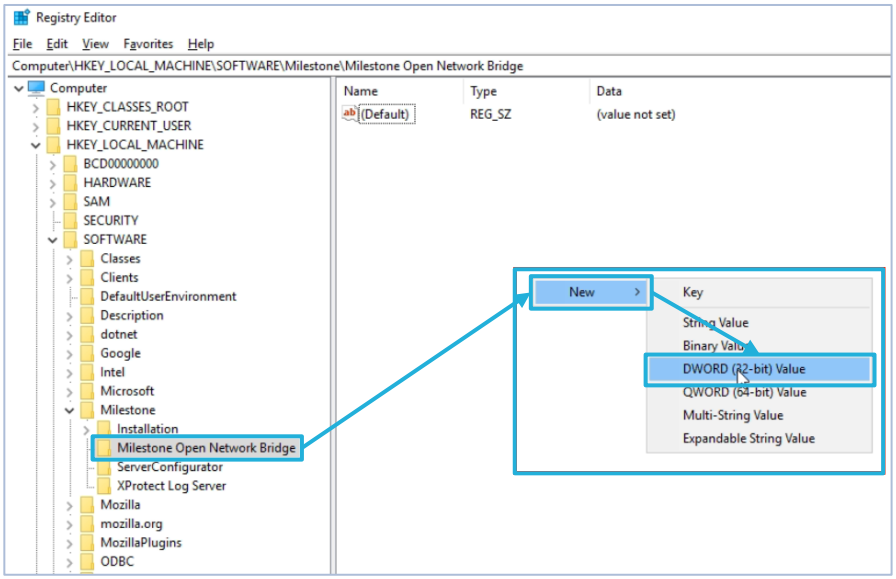
- Dans la barre de recherche Windows, saisir “Registry Editor” et sélectionner le programme.
- Sur la page d’accueil de ce programme, ajouter une nouvelle clé au registre. Pour se faire, allez dans :
    1. HKEY_LOCAL_MACHINE
    2. Software
- Puis “clic droit” sur “Milestone”, passer la souris sur “New” et cliquer sur “Key”



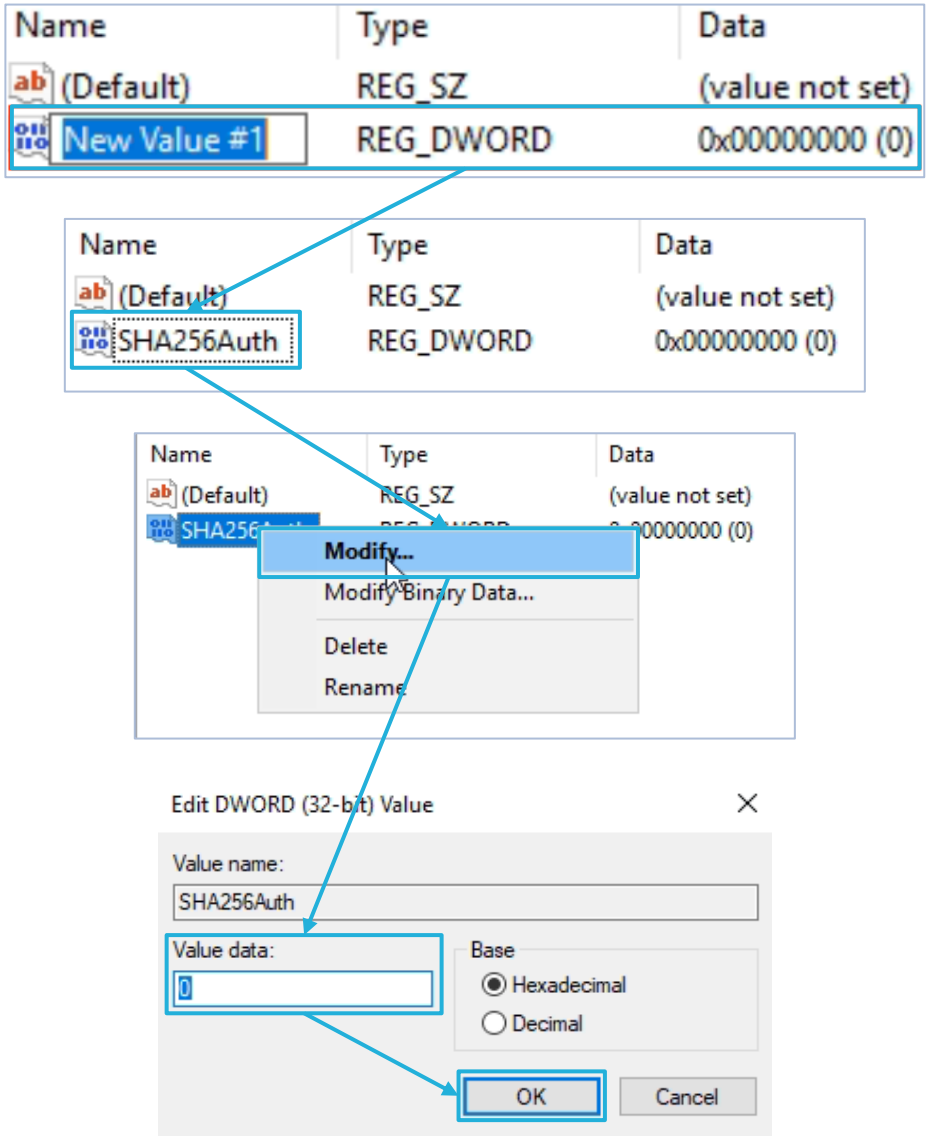
- Une nouvelle clé est ajoutée, avec comme nom par défaut “New Key #1”.
- Faire un “clic droit” sur “New Key #1”, puis cliquer sur “Rename”
- Renommer avec le nom “Milestone Open Network Bridge”



- Faire un “clic droit” sur ce même dossier “Milestone Open Network Bridge”. Puis passer la souris sur “New” et cliquer sur “DWORD (32-bit) Value”

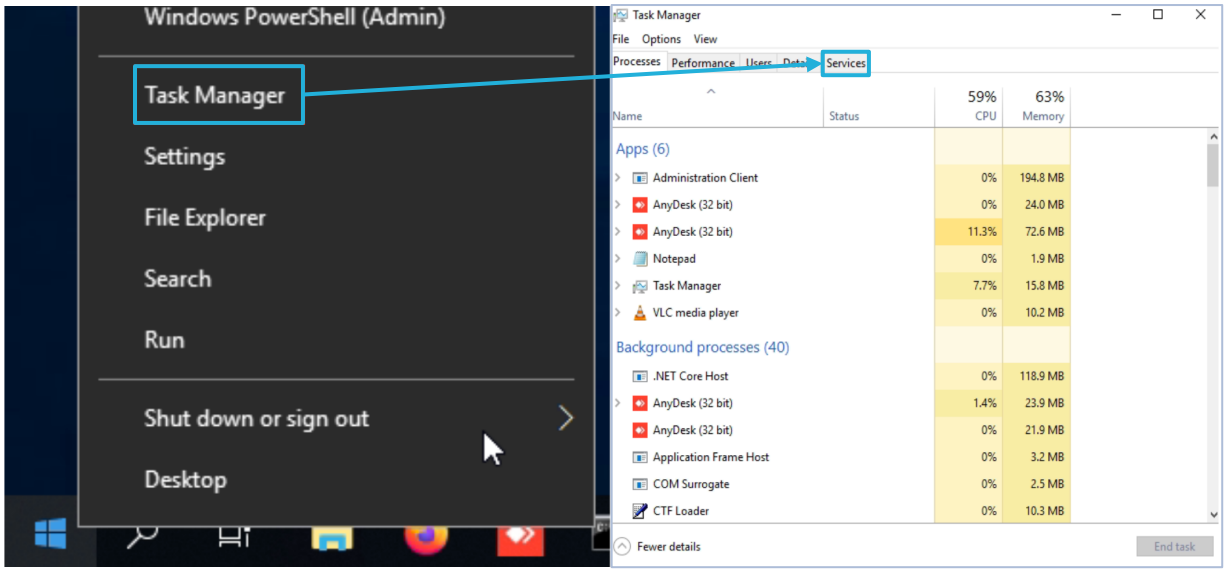


- Sur la partie haute de l'écran, une nouvelle ligne vient de s'ajouter
- Renommer la ligne "New Value #1" en "SHA256Auth"
- Faire un "clic droit" sur la ligne "SHA256Auth" et "Modify"
- Vérifier si la valeur dans "Value data" est à "0", si ce n'est pas le cas entrer la valeur "0".
- Pour finir, cliquer sur "OK"

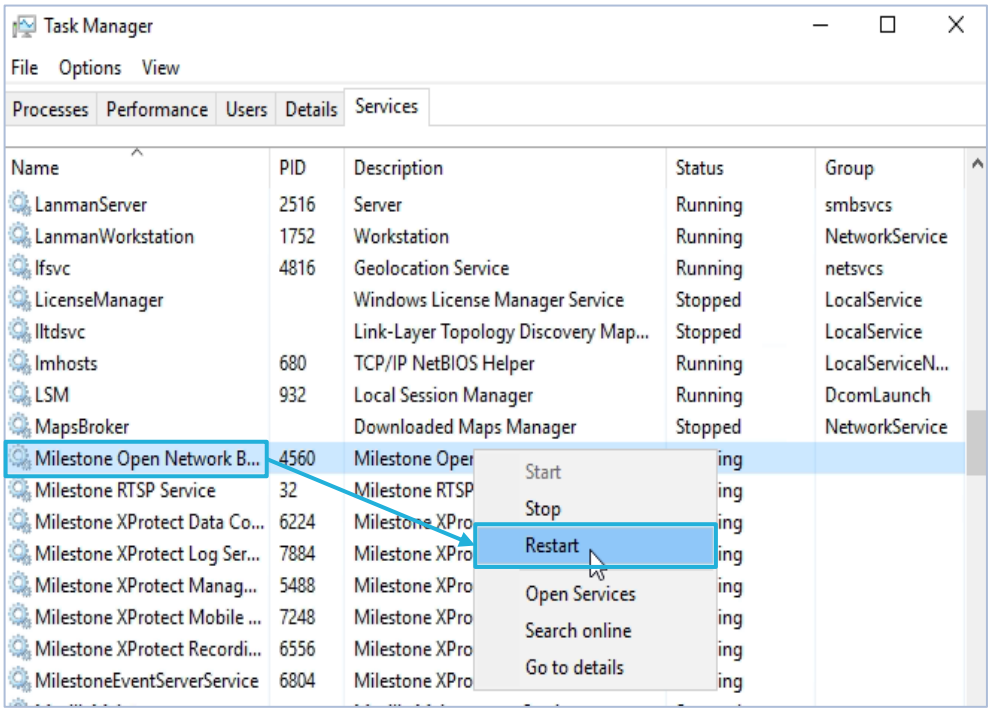


10 - Re démarrage du Milestone Open Bridge

- Faire un “clic droit” sur le bouton Windows, puis cliquer sur “Task Manager”
- Cliquer sur “service”



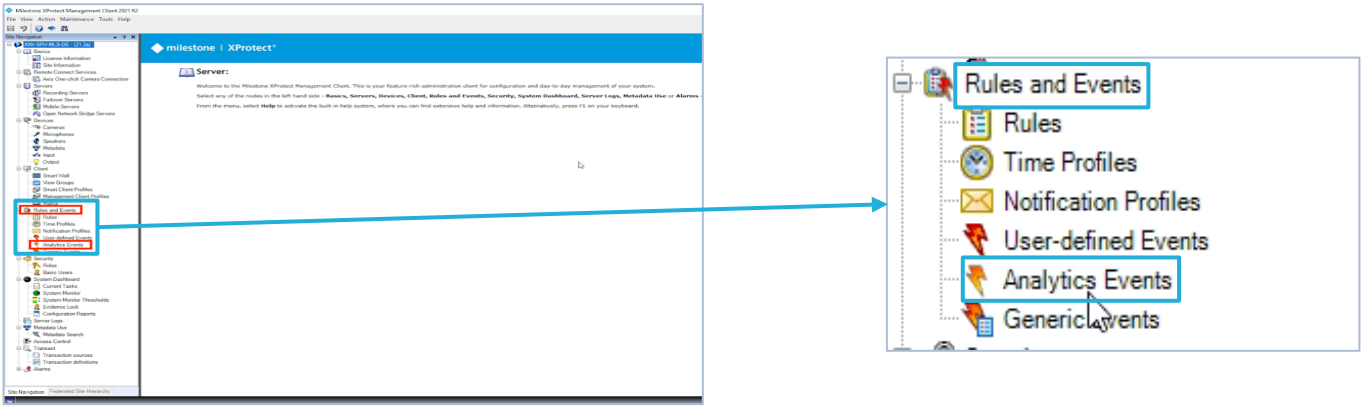
- Chercher la ligne “Milestone Open Network Bridge”, faire un “clic droit” et cliquer sur “Restart”
- Remarque : si le service ne redémarre pas automatiquement, faire un “clic droit” et cliquer sur “Start”. Passer ensuite à la configuration de XXII Core.



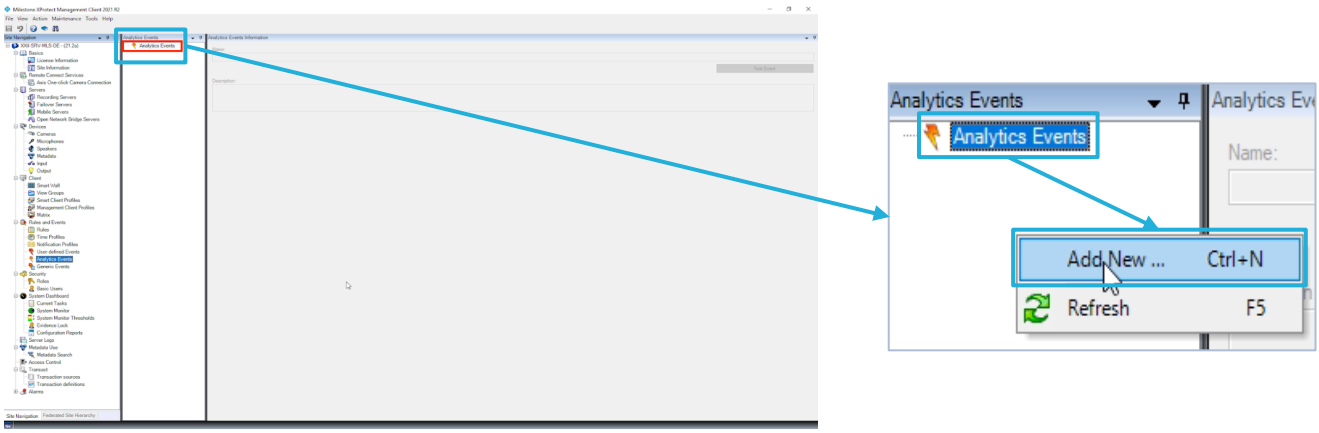
[3] Milestone xProtect Management Client

1 - Création d'évènements analytiques

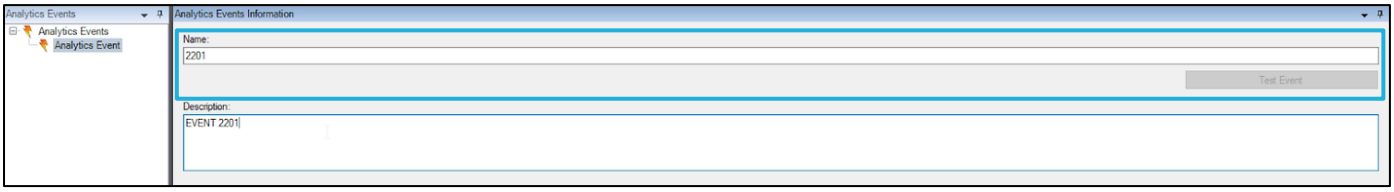
- Cette partie est dédié à la création d'alarmes et d'événements. C'est grâce à cela que **XXII Core** va envoyer des informations (événements ou alarmes) à Milestone.
- Cliquer sur l'onglet "**règles et évènements**" du DESKTOP puis cliquer sur "**Règles**".
- Dérouler le menu {Règle et événements} puis, aller dans {Événement Analytique}.



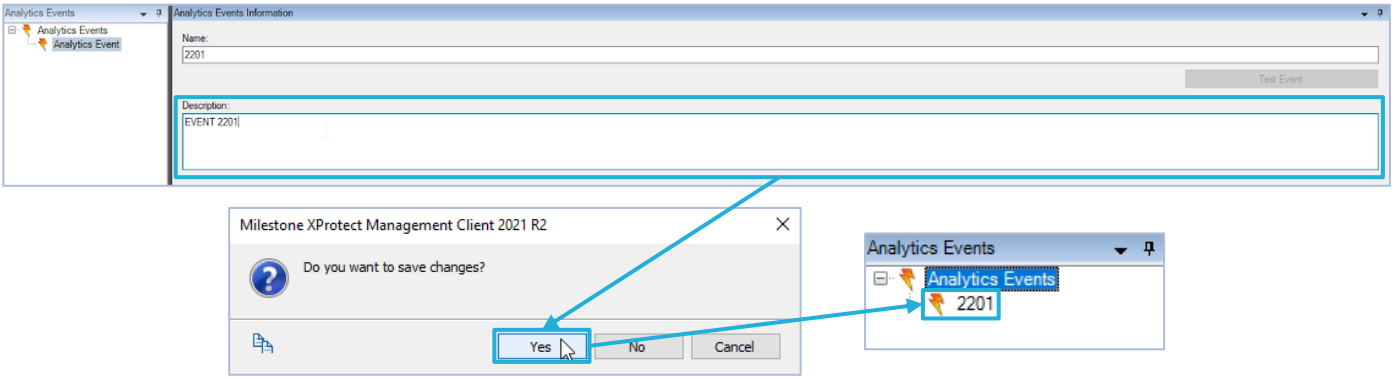
- Faire un "clic droit" sur "Analytics Events" puis "Add New ...".



- Dans le champ [Nom] saisir l'ID de l'événement identique à celui rentré dans la plateforme de configuration de XXII CORE.
- **Remarque** : saisir uniquement des caractères numériques.

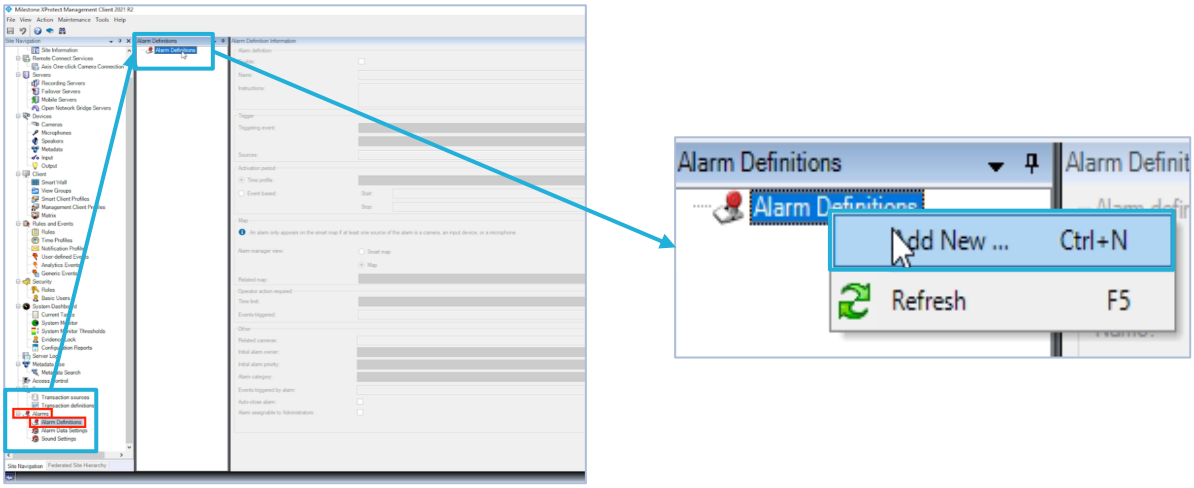


- La description de l'événement n'est pas obligatoire, saisir une indication qui aidera à organiser la liste des caméras. (Ex : Caméra 16 - Événement 2011 - Zone interdite aux véhicules).
- Cliquer sur "Yes" pour sauvegarder l'événement. L'événement est à présent dans la liste.

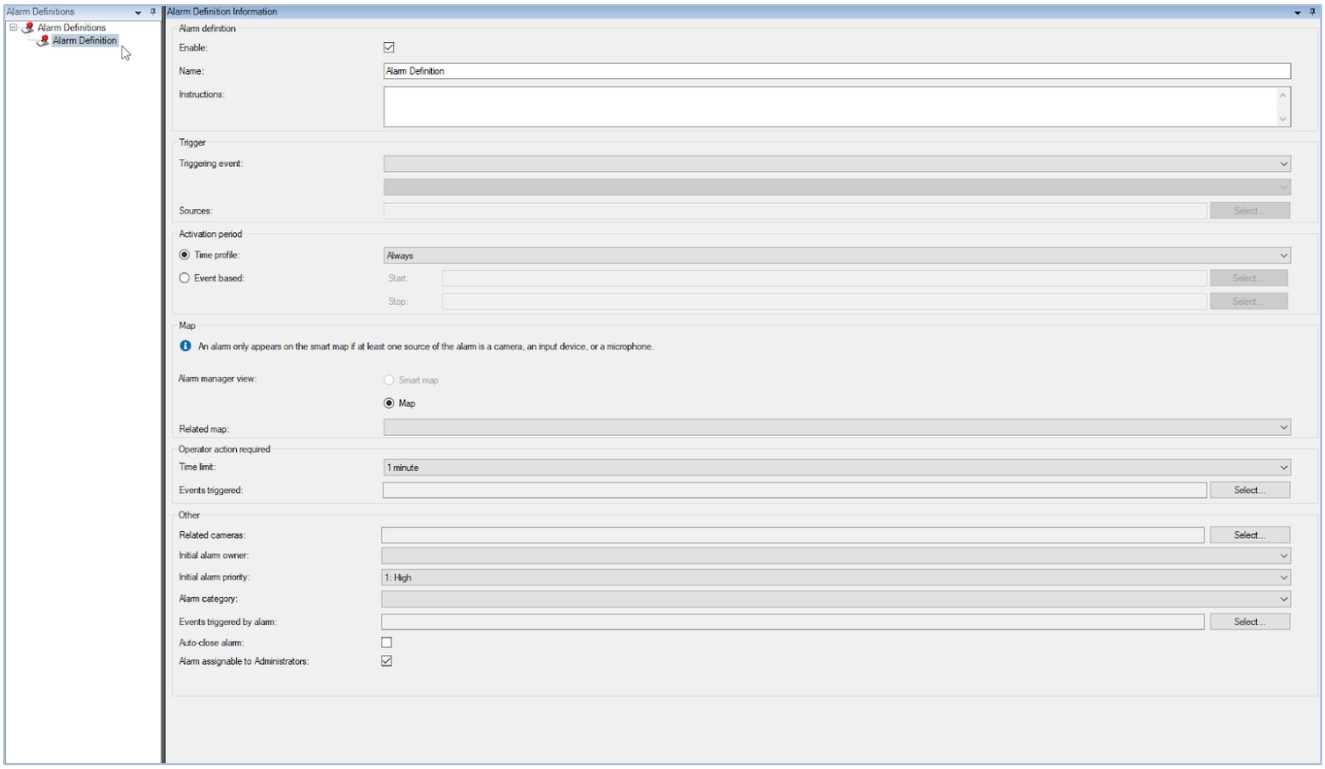


2 - Création d'alarme

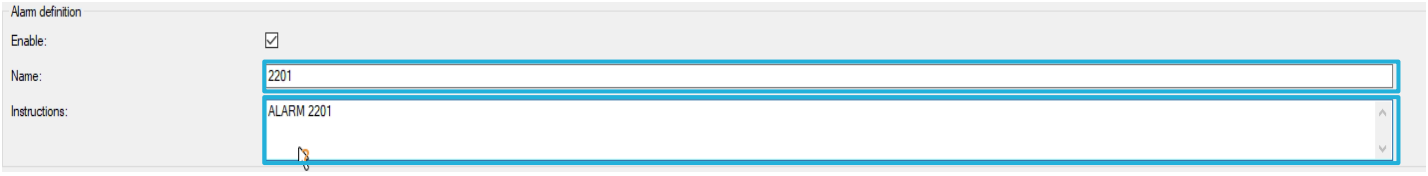
- Dans la partie gauche, sélectionner la section "Alarms", puis sélectionner "Alarm Definition"
- Faire un "clic droit" sur "Alarm Definition", puis "Add New ..."



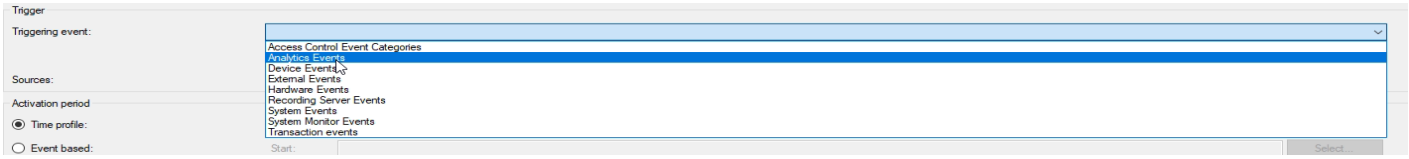
- La section de droite est maintenant disponible, saisir les informations suivantes dans celle-ci :



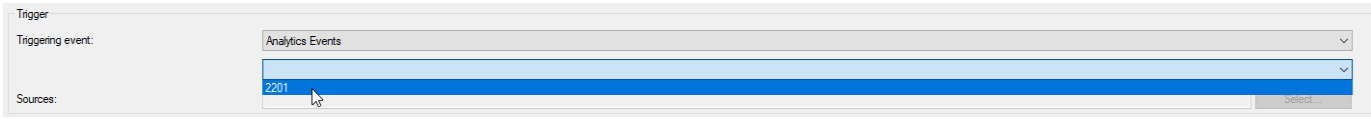
- Alarm definition
    - Name : entrer le même numéro que pour l'événement analytics vu précédemment
    - Instructions : entrer une indication qui aidera à reconnaitre sur quelle caméra est l'alarme.
    - Exemple : Caméra 16 - Événement 2011 - Zone interdite aux véhicules.



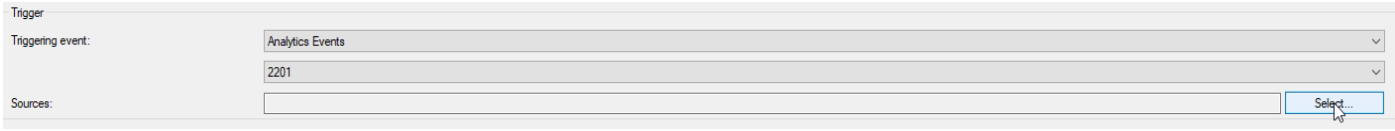
- Trigger
    - Sélectionner le menu déroulant “triggering event” puis “Analytics Event”



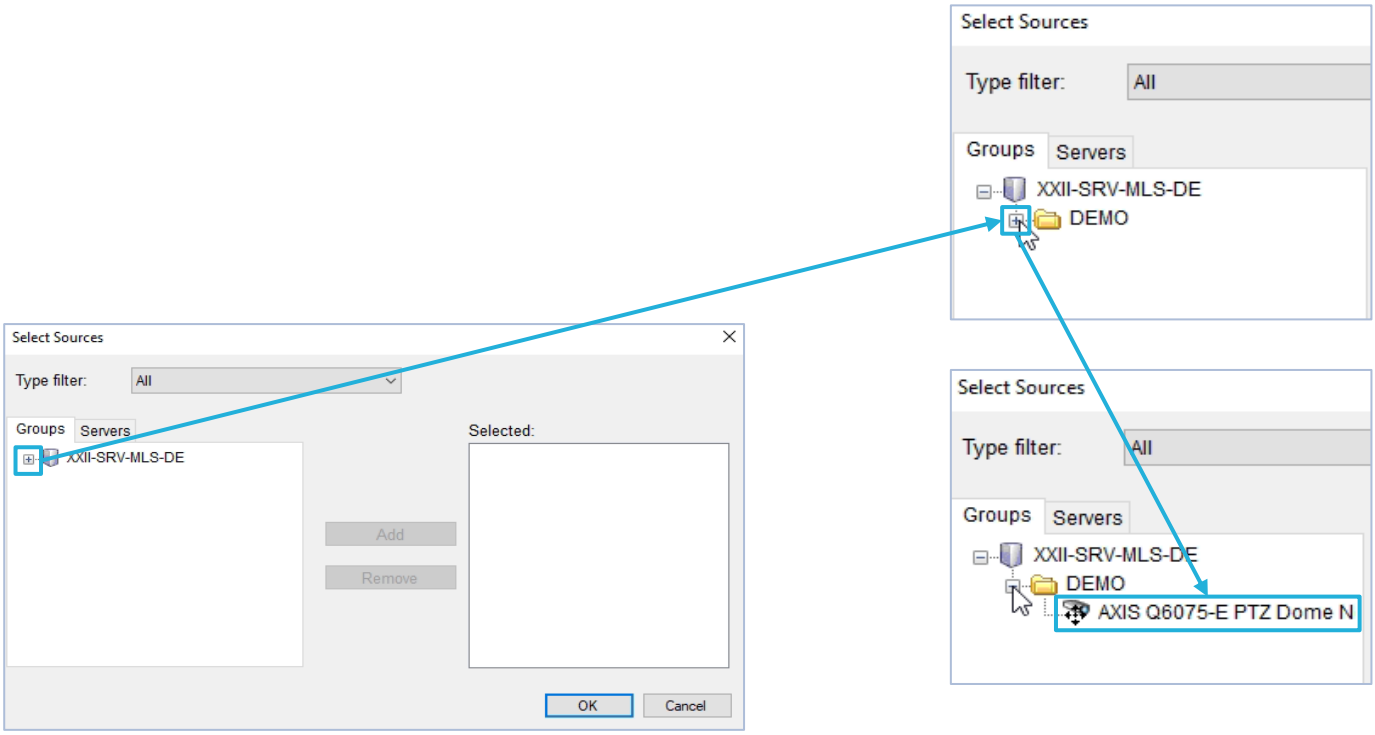
- Sélectionner le menu déroulant “Sources“ et puis l'événement analytique paramétré précédemment.



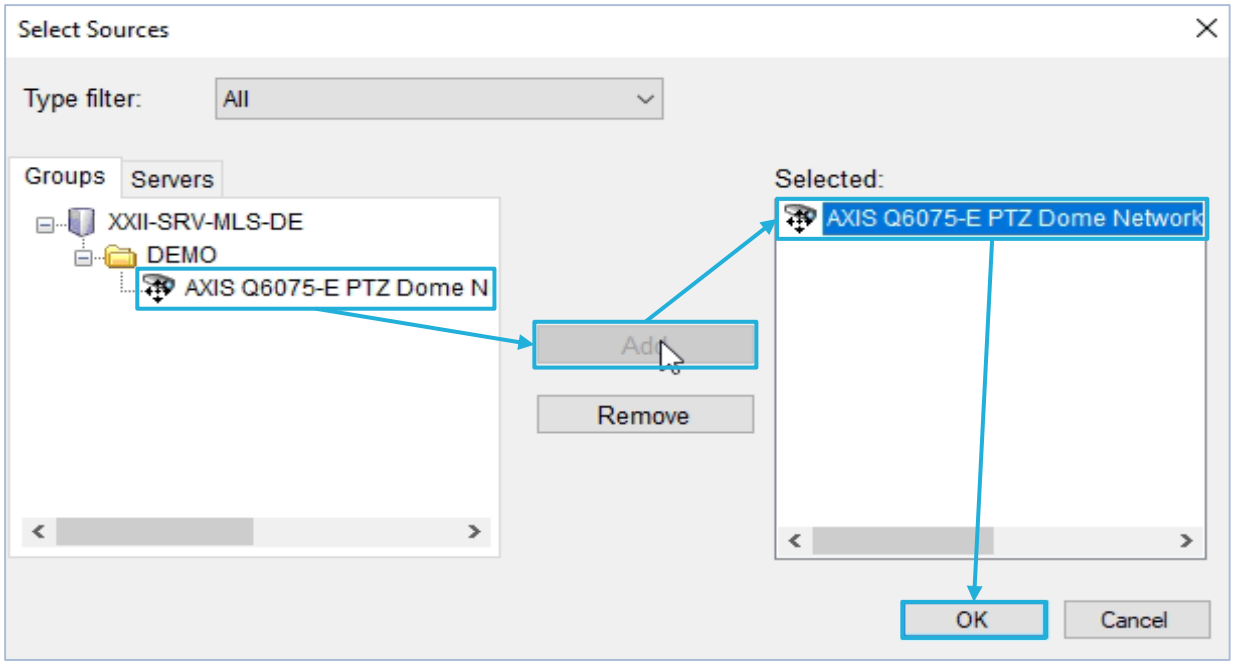
- Puis cliquer sur “select”



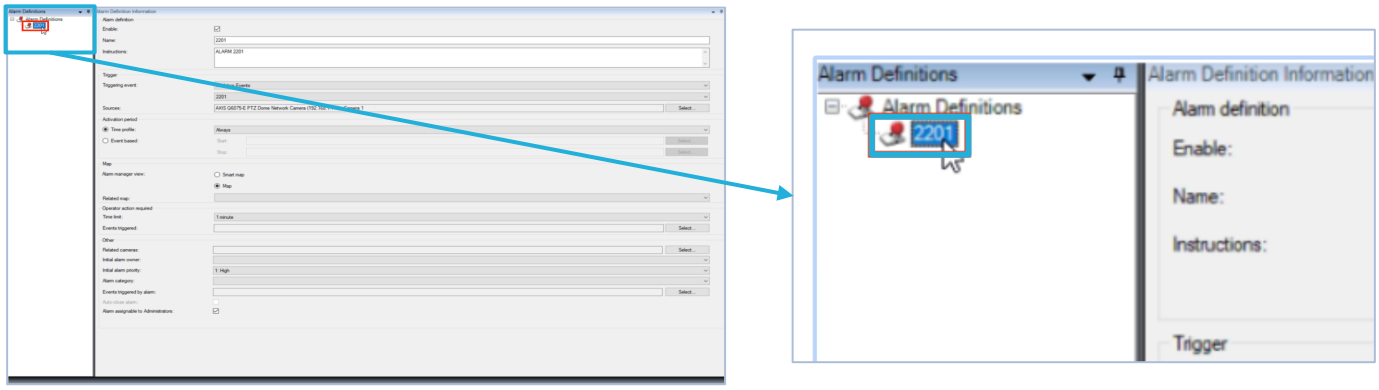
- La fenêtre “Select Sources” s’ouvre : cliquer sur le bouton “+” jusqu'à afficher la caméra à analyser. Ici, la caméra nommée “AxisQ6075”.



- Cliquer sur la caméra, puis cliquer sur le bouton “Add” (la caméra est ajoutée au menu “Selected”).
- Cliquer sur “OK” pour valider la sélection

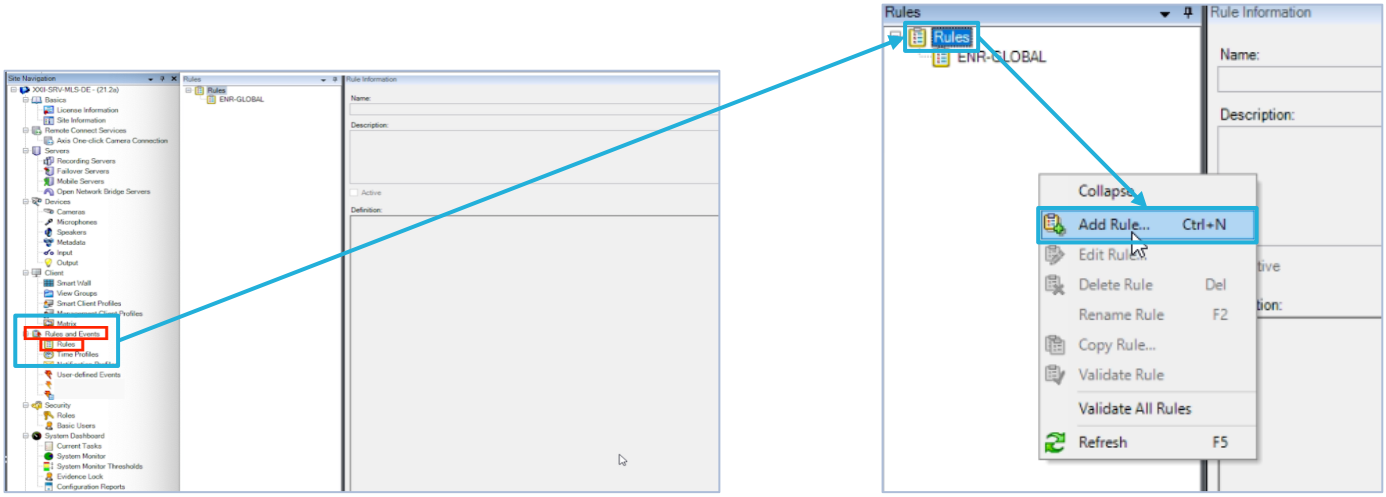


- L’alarme est à présent affichée dans la colonne “Alarm Definitions”.

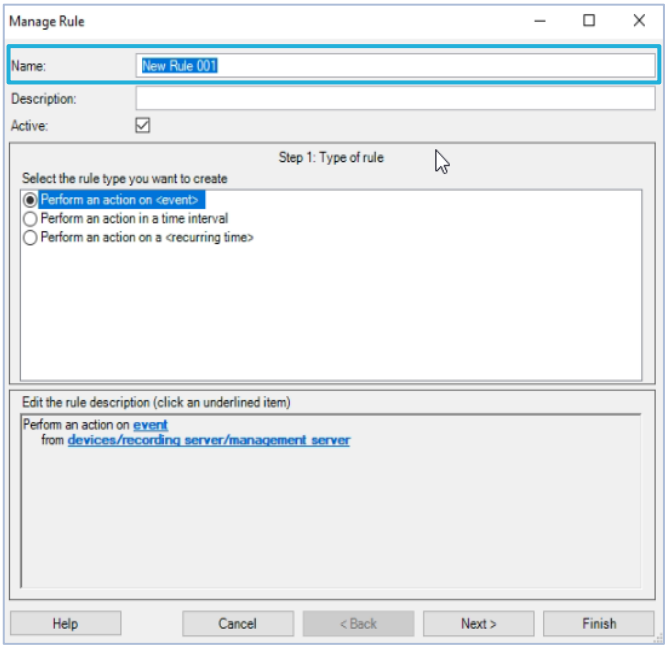


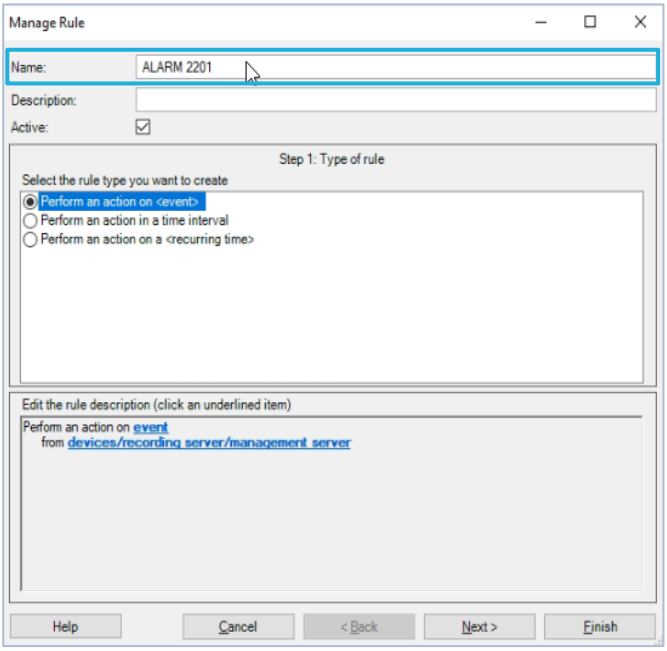
3 - Création de règles

- Dans la colonne de gauche, cliquer sur la section “Rules and Events”, puis sélectionner “Rules”
- Faire un clic droit sur “Rules” et cliquer sur “Add Rule…”

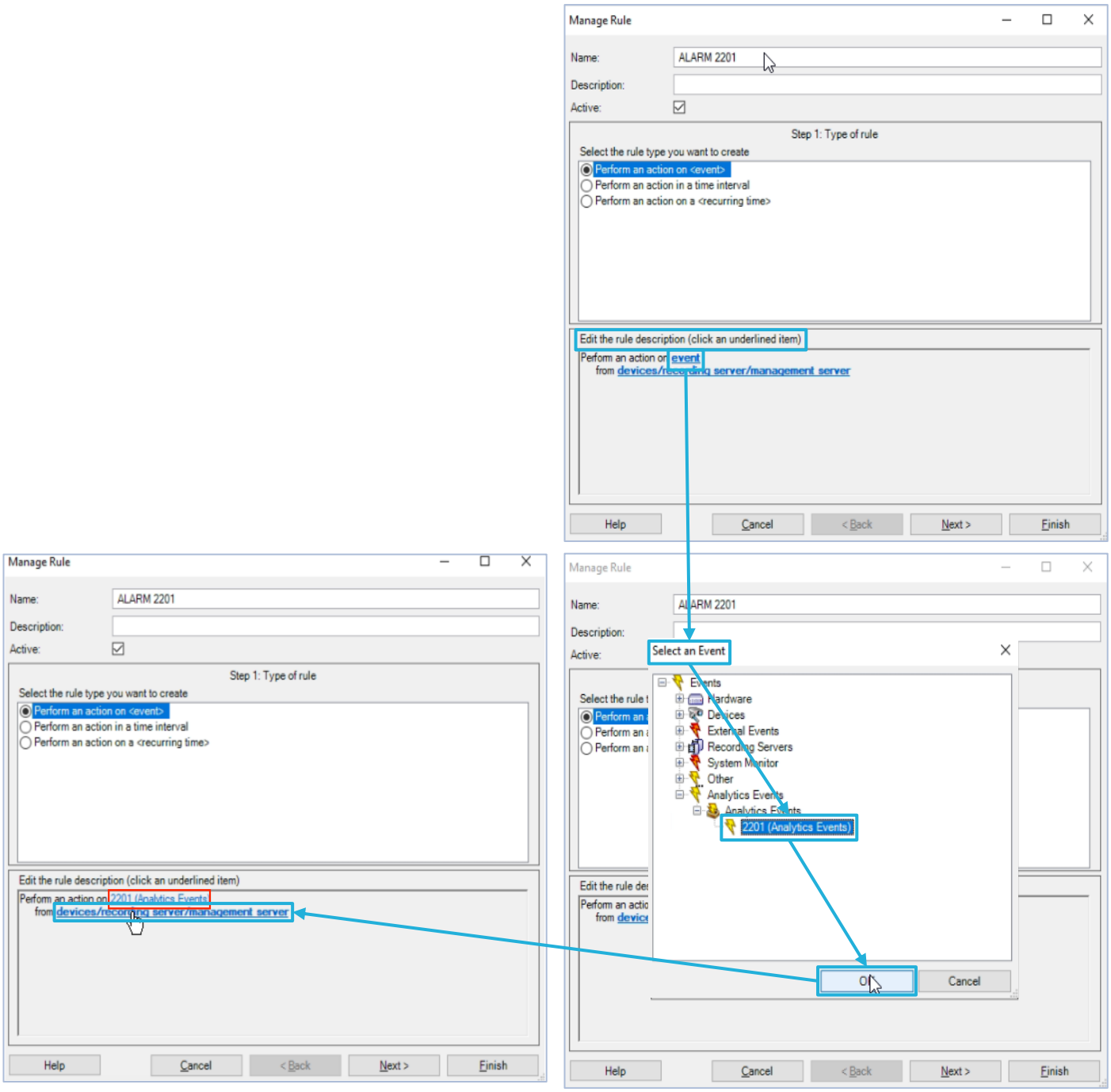


- La fenêtre “Manage Rule” s’ouvre, renseigner le nom et la description de la règle.
- Name = renseignez le nom (au choix) de la règle.

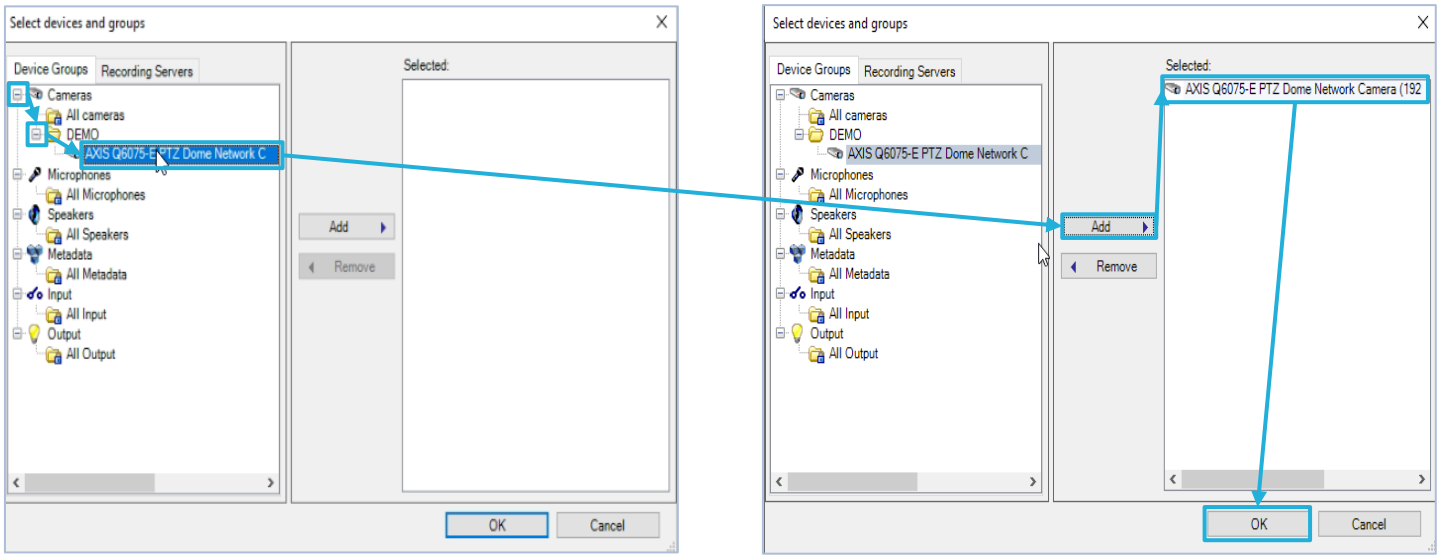




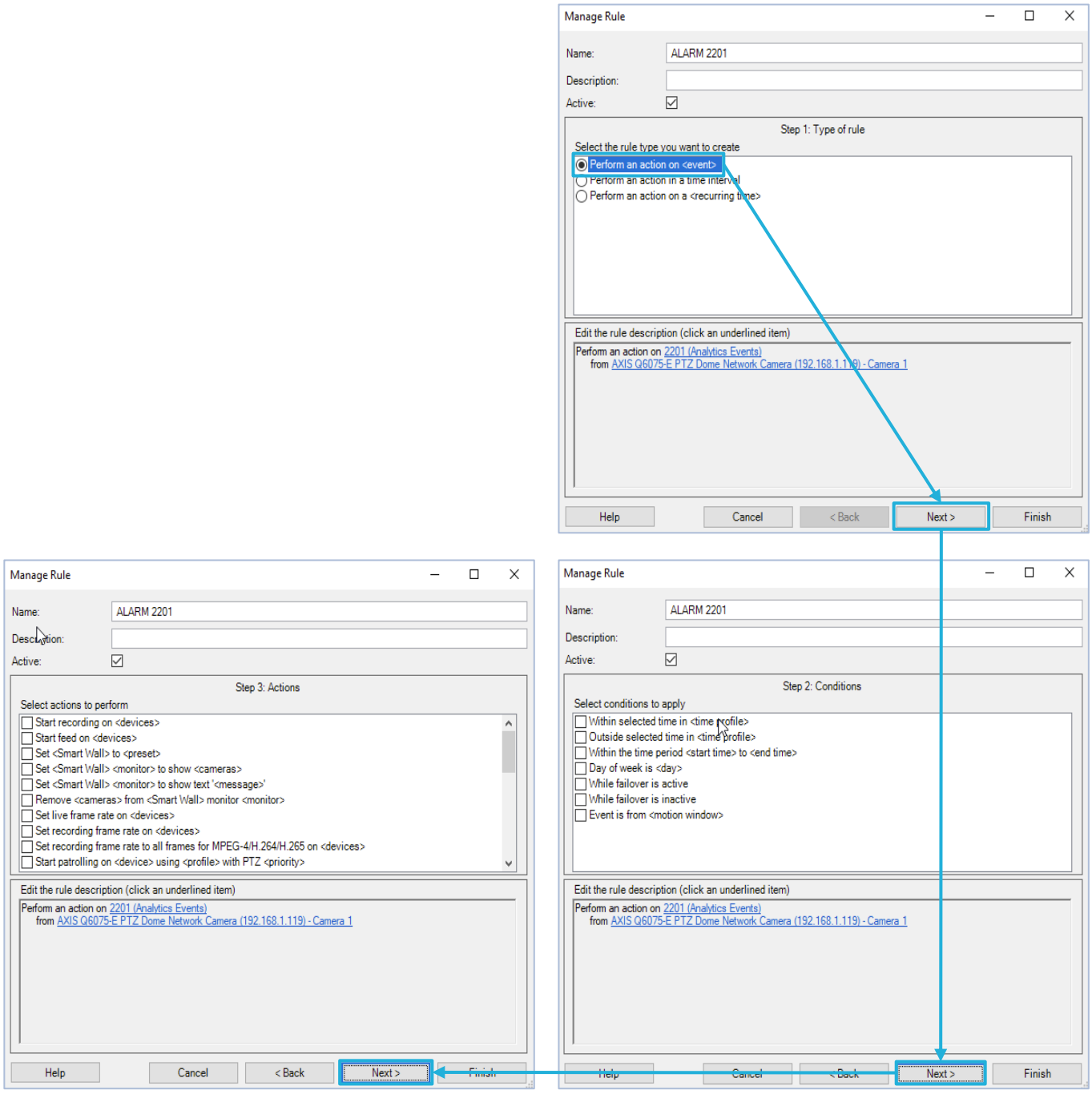
- Éditer les paramètres de la règle
    - Cliquer sur “Event” dans l’encart “Edit rule description”.
    - Une fenêtre “select an event” s’ouvre. Sélectionner l'événement associé à la règle. Cliquer sur les boutons “+” jusqu'à le trouver, puis “OK”.
    - L'événement est associé à la règle, cliquer sur “device/recording server/management server”.



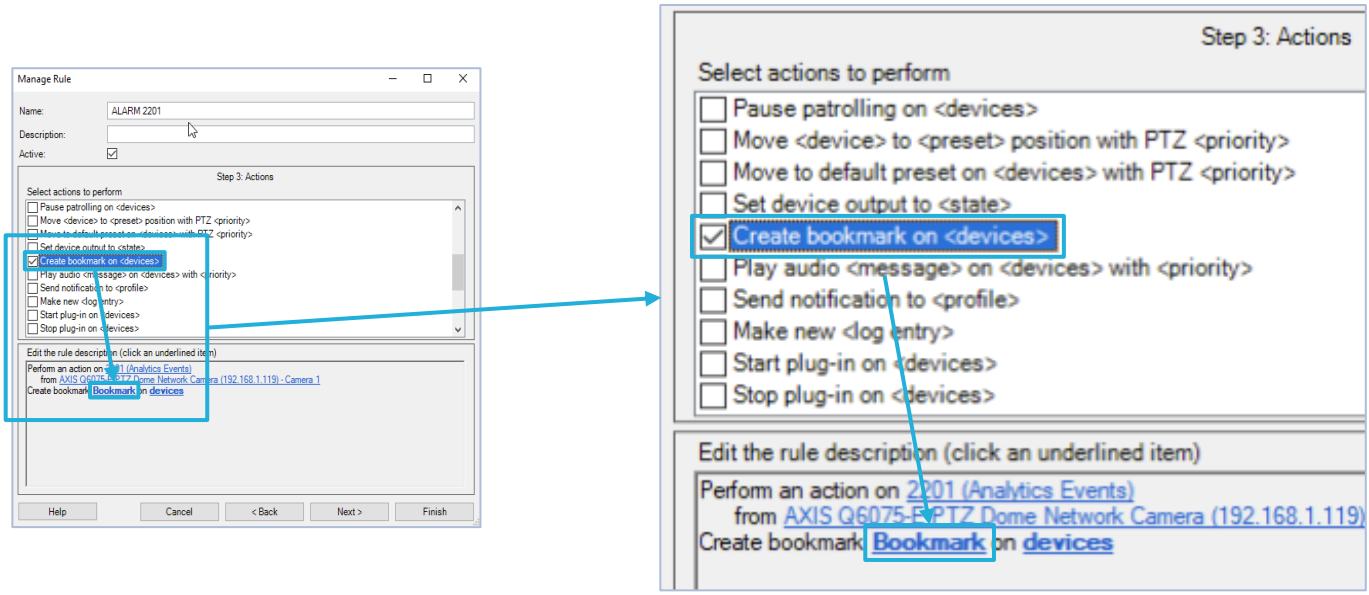
- Dans la fenêtre “Select devices and groups”, cliquer sur : “Device groups”, puis “+” jusqu’à afficher la/les caméra(s) désirée(s).
- Cliquer sur “Add” pour ajouter les caméras. Pour finir, cliquer sur “Ok”.



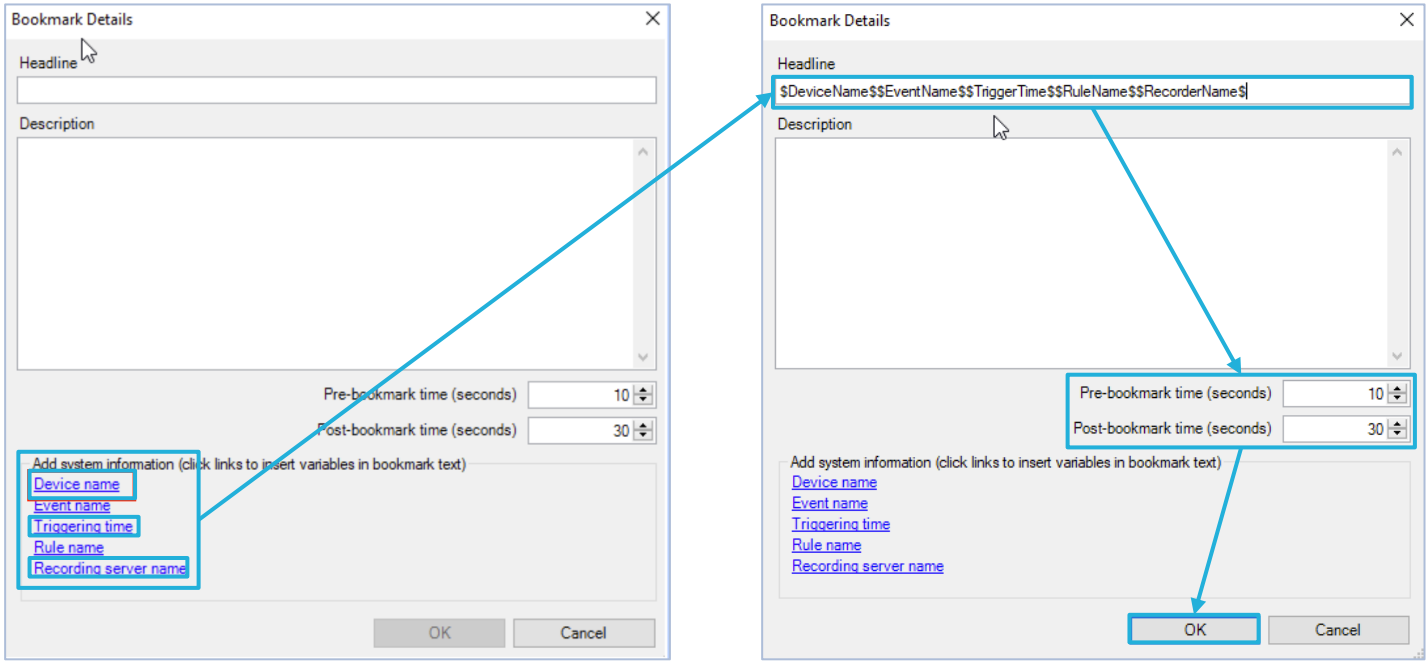
- Dans la fenêtre “Step 1 : Type of rule”, cliquer sur “Perform an action <event>”, puis cliquer sur “Next”.
- Dans la fenêtre “Step 2 : Conditions”, ne rien cocher, puis cliquer sur “Next”.
- Dans la fenêtre “Step 3 : Actions”, ne rien cocher, puis cliquer sur “Next”.



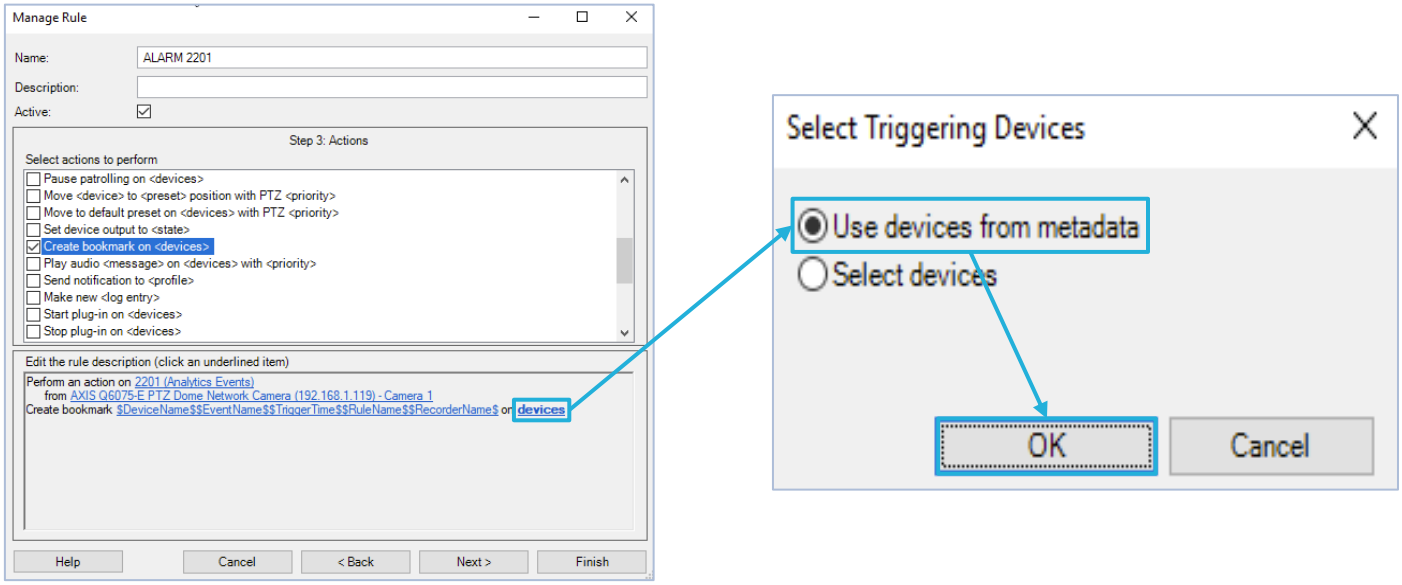
- Cocher la case “Create bookmark on <device>” et cliquer sur “Next”.
- Puis cliquer sur “Bookmark” dans la ligne “Create bookmark” pour modifier le texte du bookmark.



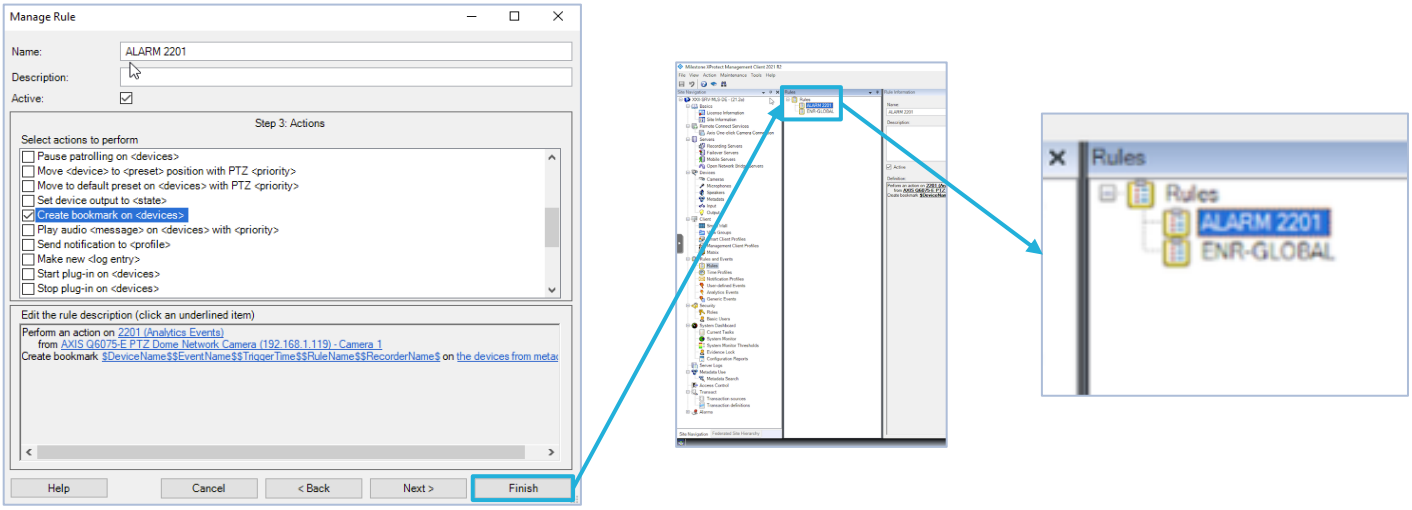
- Cliquer sur “Device name” puis “Event Name” puis “Triggering Time” puis “Rule Name” puis “Recording serveur Name”.
- Laisser les valeurs du pre-signet à 10s et post-signet à 30s par défaut puis cliquer sur “OK”.



- Cliquer sur “Devices” pour sélectionner une source.
- Sélectionner “use devices from metadata” puis sur “OK”.



- Cliquer sur “Finish” pour faire apparaître la nouvelle règle dans la liste des règles.



4 – Flux vidéo et GUID Milestone

- Cliquer sur l'onglet "serveurs" du DESKTOP puis cliquer sur "serveurs d'enregistrement".
- Sélectionner le flux caméra souhaité puis "ctl+clique" sur la vidéo pour faire apparaître "l'ID" du flux de la caméra dans la colonne "propriétés" et enfin, copier/coller le "GUID".
- Ouvrir "VLC media player" puis cliquer sur "ouvrir un flux réseau…" puis saisir l'URL.
    - Saisir l'URL suivante (identique pour tous les utilisateurs) :
        - rtsp://(user name):(mot de passe)@(IP du serveur):(port RTSP)/live/(GUID du flux de la caméra)
        - Cliquer sur "lire" pour visualiser le flux vidéo.
- Pour finir, saisir le flux rtsp complet dans XXII CORE REAL TIME.

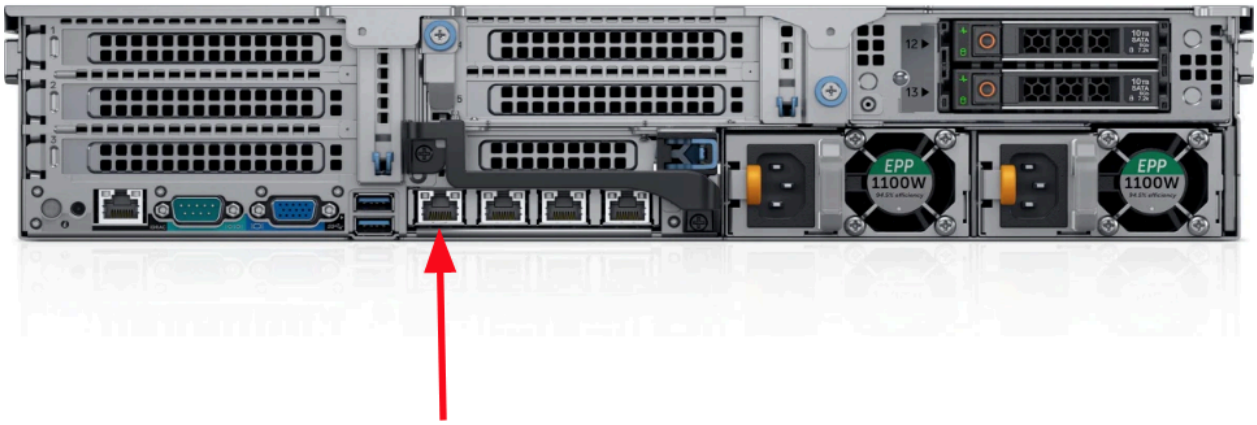
[4] - Installation physique dans la baie

1 - Liste pré-requis avant installation : **version R1 2021 du XProtect Corporate**

Operating System	
Microsoft® Windows® 8.1 Pro (64 bit)	Microsoft® Windows® Server 2012 (64 bit): Standard and Datacenter
Microsoft® Windows® 8.1 Enterprise (64 bit)	Microsoft® Windows® Server 2012 R2 (64 bit): Standard and Datacenter
Microsoft® Windows® 10 Pro (64 bit)	Microsoft® Windows® Server 2016 (64 bit): Essentials, Standard and Datacenter
Microsoft® Windows® 10 Enterprise (64 bit)	Microsoft® Windows® Server 2019 (64 bit): Essentials, Standard and Datacenter
Microsoft® Windows® 10 IoT Enterprise LTSB (Long-Term Servicing Branch)2016 (version 1607 or later)	To run clustering/failover management servers, you need a Microsoft® Windows® Server 2012/2012 R2 Standard or Datacenter edition, Microsoft® Windows® Server 2016 Standard or Datacenter edition, or a Microsoft® Windows® Server 2019 Standard or Datacenter edition
Microsoft® Windows® 10 IoT Enterprise, version 1803 or later (64 bit), IoT Core	

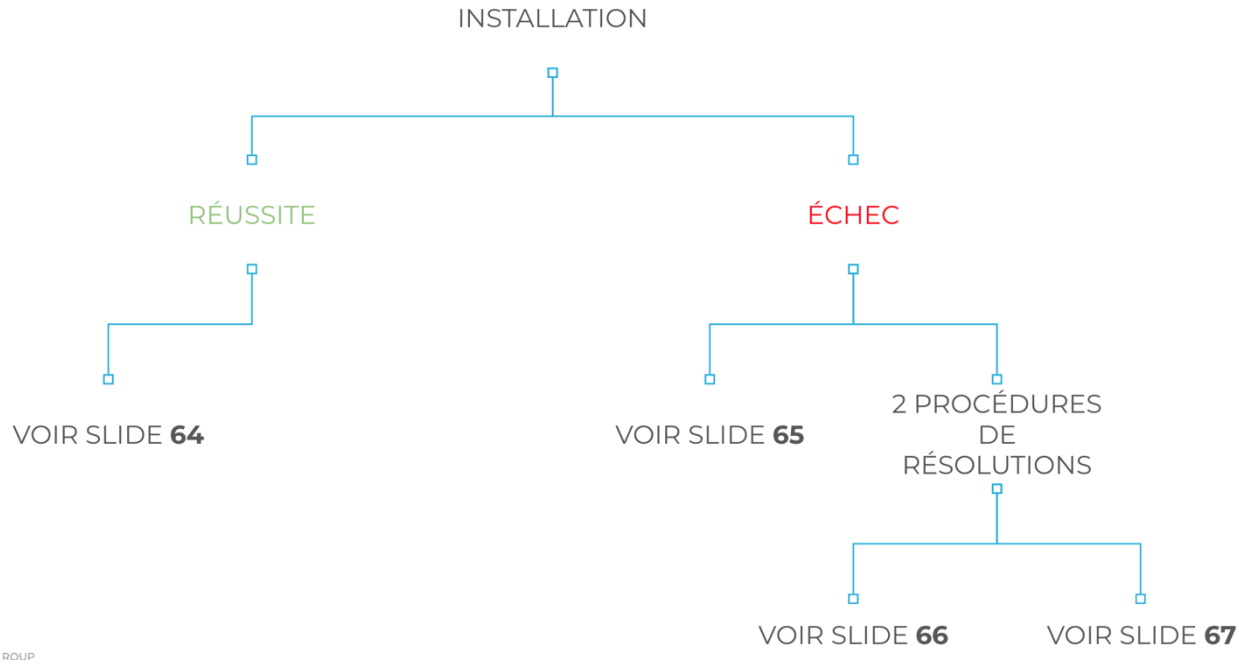
2 - Étape 1 : serveur et baie de serveurs

- **Racker** le serveur XXII Core dans la baie informatique “dédiée” (**19” - Minimum. 800 de profondeur**).
- **Raccorder** les alimentations électriques (les 2).
- **Raccorder** le câble ethernet en sortie de serveur sur la prise ENO1 (gauche) sur le VLAN VMS.
- **Allumer** la machine.



3 - Étape 2 : serveur et communication

- **Ouvrir** un terminal sur un autre ordinateur et sur le même VLAN pour pinger le serveur.
    - Sur Windows :
        - **Touche Windows**
        - **Taper “cmd”**
        - **Touche entrée**
    - Sur Mac :
        - **command + espace**
        - **Taper “terminal”**
        - **Ouvrir ‘terminal”**
- **Lancer** la commande « ping $IP_Server ».
    - Exemple : ping 192.168.1.100
- **Si le serveur** réponds au ping, alors celui-ci est correctement raccordé au bon VLAN.



- **Étape 2 (suite) :** serveur et communication - réussite

```
nathan@xxii:~$ ping 192.168.1.100
PING 192.168.1.133 (192.168.1.133) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.037 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.069 ms
```

- **Étape 2 (suite) :** serveur et communication - échec de communication

```
nathan@xxii:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.250) 56(84) bytes of data.
From 192.168.1.99 icmp_seq=1 Destination Host Unreachable
From 192.168.1.99 icmp_seq=2 Destination Host Unreachable
From 192.168.1.99 icmp_seq=3 Destination Host Unreachable
From 192.168.1.99 icmp_seq=4 Destination Host Unreachable
```

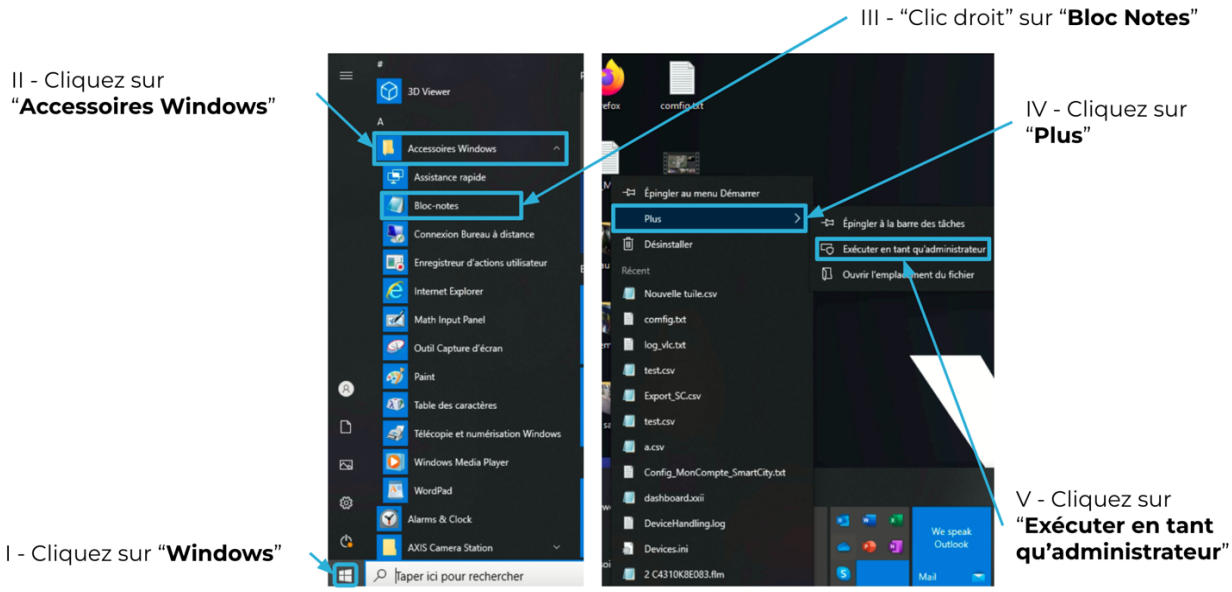
- **Étape 2 (suite) :** serveur et communication - vérification de la configuration ip

```
xxii@node1:~$ ifconfig | more
cni0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.233.64.1  netmask 255.255.255.0  broadcast 10.233.64.255
        inet6 fe80::bc6b:64ff:fe57:eedf  prefixlen 64  scopeid 0x20<link>
        ether be:6b:64:57:ee:df  txqueuelen 1000  (Ethernet)
        RX packets 106170290  bytes 1565761646558 (1.5 TB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 122917347  bytes 1580935517151 (1.5 TB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:dfff:feb0:f456  prefixlen 64  scopeid 0x20<link>
        ether 02:42:df:b0:f4:56  txqueuelen 0  (Ethernet)
        RX packets 158  bytes 42404 (42.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 134  bytes 43769 (43.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::b67a:f1ff:fea4:12f4  prefixlen 64  scopeid 0x20<link>
        ether b4:7a:f1:a4:12:f4  txqueuelen 1000  (Ethernet)
        RX packets 31381687  bytes 17016622963 (17.0 GB)
        RX errors 0  dropped 101343  overruns 0  frame 0
        TX packets 6604058  bytes 2231936114 (2.2 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16
```

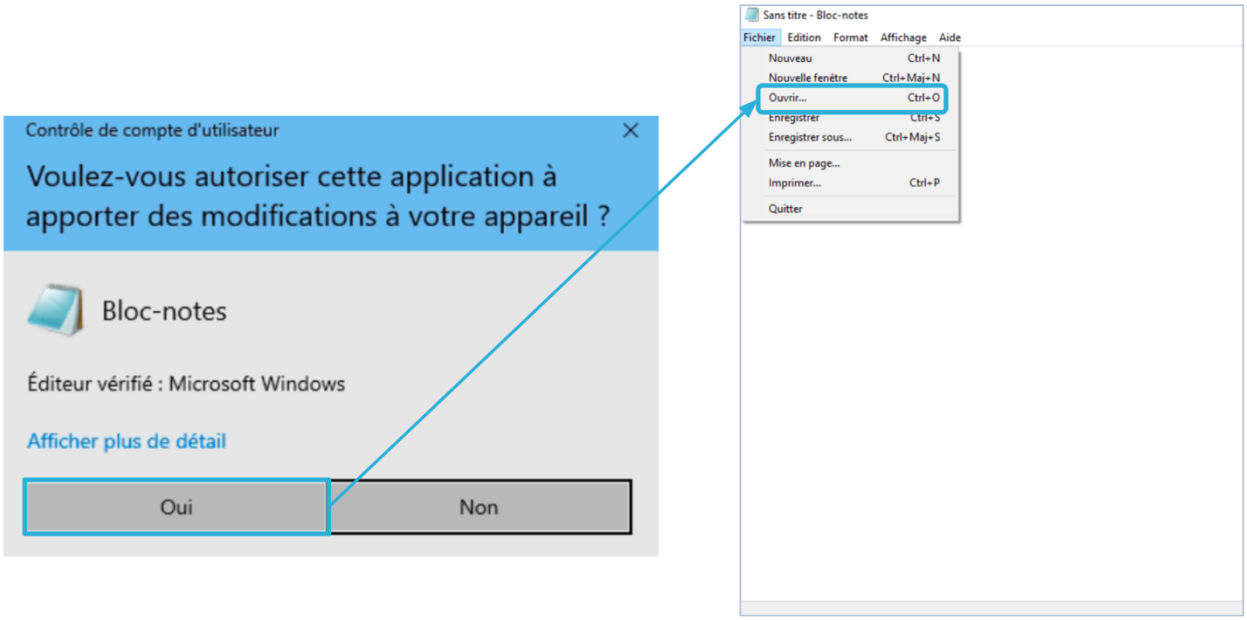

- **Étape 2 (fin) :** serveur et communication - vérification du netplan

```
xxii@node1:~$ cat /etc/netplan/00-installer-config.yaml
network:
    ethernets:
        eno1:
            addresses: [192.168.1.100/24]
            gateway4: 192.168.1.1
            nameservers:
                addresses: [8.8.8.8, 8.8.4.4]
            dhcp4: false
            dhcp6: false
    version: 2
```

4 - Étapes 3 : les ingress - ajout & méthodes (Windows)



- Cliquer sur “**Oui**” puis sur “**Ouvrir**”

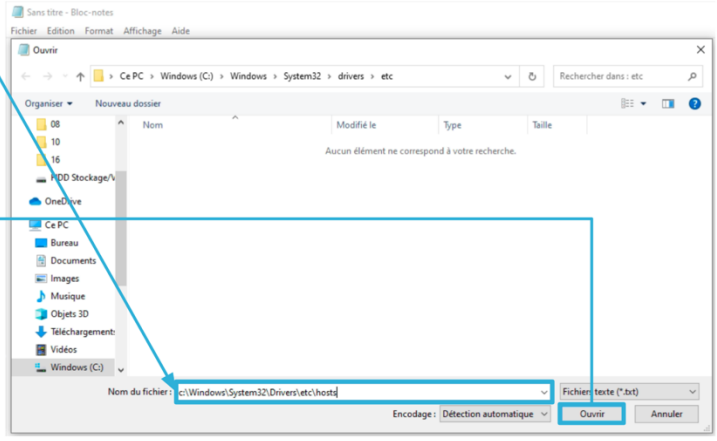


I - Saisir :

c:\Windows\System32\Drivers\etc\hosts

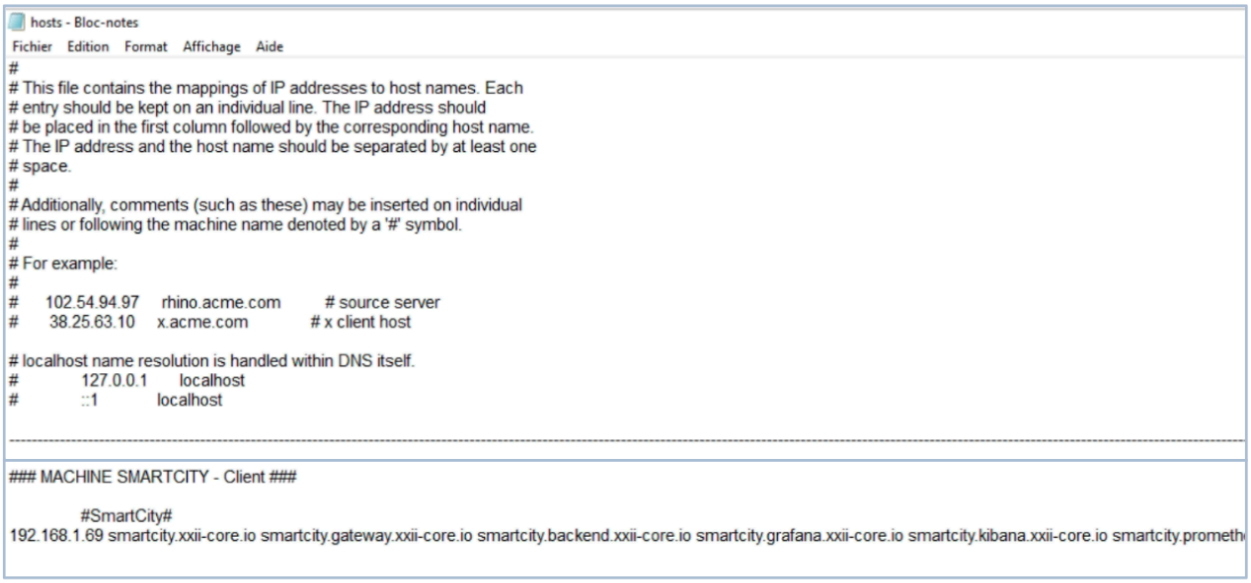
II - Cliquer sur :

Ouvrir



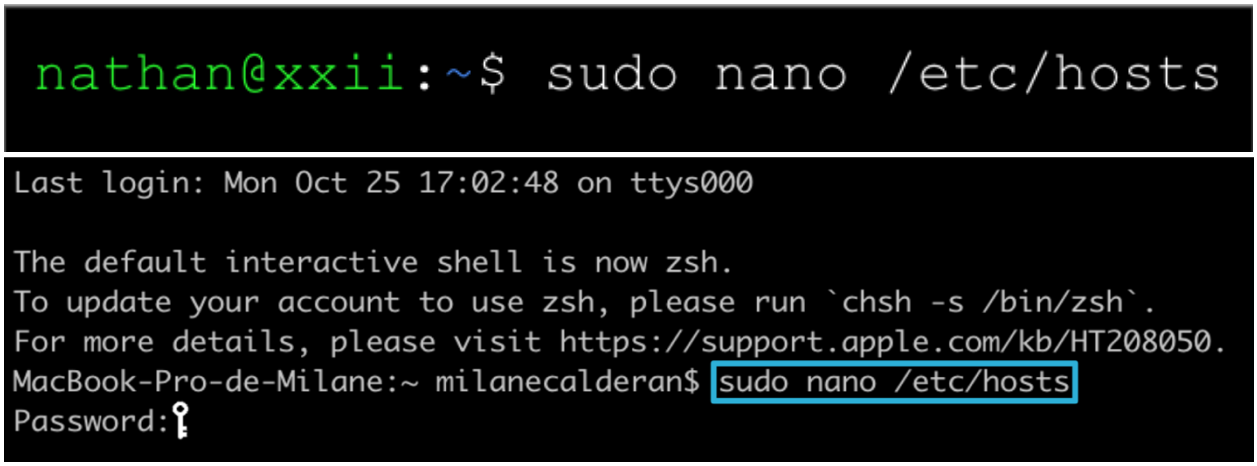
Remarque : Si le fichier n’est pas affiché, il faut « **afficher les fichiers cachés** ».

- **Le fichier host** est maintenant **ouvert**, il suffit maintenant de **copier coller les ingress** à l’intérieur.
  - **Exemple** : 192.168.1.100
  - smartcity.xxii-core.io smartcity.backend.xxii-core.io smartcity.gateway.xxii-core.io smartcity.grafana.xxii-core.io smartcity.kibana.xxii-core.io smartcity.prometheus.xxii-core.io smartcity.alertmanager.xxii-core.io smartcity.results.xxii-core.io
- **Cliquer** sur **ctrl+s** ou sur **sauvegarder**
- **Fermer** le fichier.



Remarques : Il y a un espace entre l'adresse IP et chaque URL.

- **Saisir** la commande : sudo nano /etc/hosts
- **Cliquer** sur "**entrer**"
- **Entrer** votre "**mot de passe**" (Note : le mot de passe ne s'affiche pas à la saisie, vous tapez à "l'aveugle").
- **Cliquer** sur "**entrer**"
- **Remarque** : Quand vous tapez des caractères rien ne s'affiche à l'écran, c'est normal c'est une question de sécurité.



- **Sauter** une ligne, et copier coller les ingress à la suite.
- **Remarques** : Il y a un espace entre l'adresse IP et chaque URL.

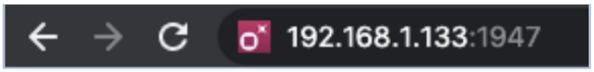
```
127.0.0.1       localhost
127.0.1.1       xps

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

#Node1
192.168.1.100 node1

#SmartCity
192.168.1.100 smartcity.xxii-core.io smartcity.backend.xxii-core.io smartcity.gateway.xxii-core.io
smartcity.results.xxii-core.io smartcity.kibana.xxii-core.io smartcity.alertemanager.xxii-core.io
```

- **Étape 3 bis : Ajouter les Ingress dans le DNS du réseau local**
  - Ajouter les ingress sur le serveur DNS
  - **Récupérer les ingress en se connectant en SSH au serveur et en tapant la commande :** kubectl get ingress -A

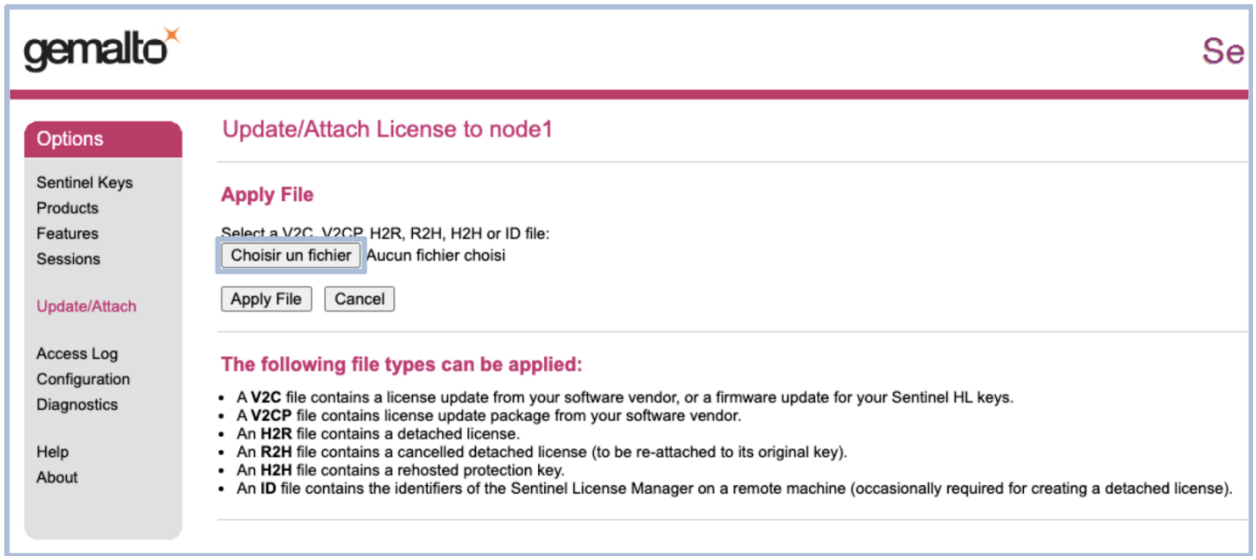
```
xxii@node1:~$ kubectl get ingress -A
NAMESPACE    NAME                                    CLASS    HOSTS                                ADDRESS          PORTS   AGE
default      platform-resultapi                      <none>   smartcity.results.xxii-core.io       10.233.26.238    80      174d
default      platform-web-frontend                   <none>   smartcity.xxii-core.io               10.233.26.238    80      174d
default      platform-web-gateway                    <none>   smartcity.gateway.xxii-core.io       10.233.26.238    80      131d
default      processor-debug                         <none>   smartcity.debug.xxii-core.io         10.233.26.238    80      43d
monitoring   monitoring-efk-kb-http                  <none>   smartcity.kibana.xxii-core.io        10.233.26.238    80      174d
monitoring   monitoring-prometheus-oper-alertmanager <none>   smartcity.alertmanager.xxii-core.io  10.233.26.238    80      174d
monitoring   monitoring-prometheus-oper-prometheus   <none>   smartcity.prometheus.xxii-core.io    10.233.26.238    80      174d
monitoring   monitoring-prometheus-operator-grafana  <none>   smarcity.grafana.xxii-core.io        10.233.26.238    80      174d
```


5 - Étape 4 : activation des licences XXII CORE

- **Saisir** l'URL suivante : ipdelamachine:1947
- **Cliquer** sur **Update/Attach** pour ouvrir cette page.



- **Sélectionner** "**choisir un fichier**" et "**charger**" le fichier " → **.v2c** qui vous a été transmis lors de la souscription de contrat. Félicitations, **XXII CORE est activé !**



6 - Étape 5 : **mise en action de XXII Core**

- **Ouvrir** la page de configuration web de XXII Core
- **Saisir** dans un navigateur internet l'adresse suivante :
    - Attention, il ne faut surtout pas oublier le port 32080, sinon l'adresse sera inaccessible
- **Identifiez-vous** en renseignant :
    - Identifiant
    - Mot de passe
- **Si vous avez égaré ces informations**, vous pouvez appeler le support XXII : 01 84 20 48 22