



Document de présentation des Réalizations professionnelles

Documentation détaillant les Réalisations

BTS Service Informatique aux Organisations
Option Solution D'infrastructure, système et Réseaux



Akaki
Miminoshvili

I. Présentation

A- OpenVPN

OpenVPN peut être utilisé pour créer des réseaux VPN à la fois pour les entreprises et les particuliers. Il permet aux utilisateurs d'accéder à distance à des ressources réseau telles que des fichiers, des applications et des imprimantes, tout en garantissant la sécurité des données.

OpenVPN est un logiciel open-source qui permet de créer des connexions VPN (Virtual Private Network) sécurisées entre deux ou plusieurs ordinateurs via Internet. Il s'agit d'un protocole de VPN largement utilisé pour ses fonctionnalités de sécurité avancées et sa facilité d'utilisation.

OpenVPN utilise des certificats et des clés pour authentifier les utilisateurs et chiffre les données qui transitent sur le réseau VPN. Il prend en charge différents protocoles de chiffrement, tels que AES, Blowfish et DES, pour garantir une sécurité maximale. Il prend également en charge les protocoles de tunneling SSL/TLS et UDP pour une flexibilité et une compatibilité accrue avec les systèmes d'exploitation et les appareils réseau.



B- Veeam Backup



Backup & Replication™

Backup offre des fonctionnalités de sauvegarde et de récupération complètes pour les environnements VMware vSphere et Microsoft Hyper-V.

Veeam Backup est une solution de sauvegarde et de récupération de données pour les environnements virtuels et physiques. Elle est principalement utilisée par les entreprises pour protéger leurs données et garantir la continuité de leur activité en cas de perte de données ou d'interruption de service. Veeam

Veeam Backup offre également des fonctionnalités de restauration granulaire pour les machines virtuelles, les fichiers, les e-mails et les applications, ainsi que des fonctionnalités de réplication de données pour une protection contre les pannes et les catastrophes. Elle prend en charge la déduplication et la compression des données pour une utilisation efficace de l'espace de stockage.



II. Procédure de configuration des équipements

A- OpenVPN

Prérequis :

- Un pare-Feu Netgate sg-3100
- Un accès Internet Procédure d'installation :

1-Création des certificats d'autorités et de serveur.

The screenshot shows the pfSense web interface for the Certificate Manager. The breadcrumb trail is: System / Certificate Manager / Certificates / Edit. The 'Certificates' tab is active. The form is titled 'Add/Sign a New Certificate' and includes the following sections:

- Method:** Create an internal Certificate (dropdown)
- Descriptive name:** (text input)
- Internal Certificate:**
 - Certificate authority:** ASM-CERTIF (dropdown)
 - Key type:** RSA (dropdown)
 - Key length:** 2048 (dropdown). Note: The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
 - Digest Algorithm:** sha256 (dropdown). Note: The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.
 - Lifetime (days):** 3650 (text input). Note: The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
 - Common Name:** ASM-VPN-CERTIF (text input). Note: The following certificate subject components are optional and may be left blank.
 - Country Code:** FR (dropdown)
 - State or Province:** e.g. Texas (text input)
 - City:** e.g. Austin (text input)
 - Organization:** e.g. My Company Inc (text input)
 - Organizational Unit:** e.g. My Department Name (optional) (text input)
- Certificate Attributes:**
 - Attribute Notes:** The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode. For Internal Certificates, these attributes are added directly to the certificate as shown.
 - Certificate Type:** Server Certificate (dropdown). Note: Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.
 - Alternative Names:** FQDN or Hostname (dropdown). Includes fields for Type and Value.

The screenshot shows the pfSense web interface for the Certificate Manager. The breadcrumb trail is System / Certificate Manager / CAs. The 'CAs' tab is selected. A search bar is present with a search term field and a dropdown menu set to 'Both'. Below the search bar is a table of Certificate Authorities. The table has columns for Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. One entry is visible: ASM-CERTIF, which is internal, self-signed, has 2 certificates, and is in use for the OpenVPN Server. The distinguished name is CN=internal-ca, C=FR. The validity period is from Fri, 17 Feb 2023 22:23:54 +0100 to Mon, 14 Feb 2033 22:23:54 +0100. An 'Add' button is at the bottom right.

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
ASM-CERTIF	<input checked="" type="checkbox"/>	self-signed	2	CN=internal-ca, C=FR Valid From: Fri, 17 Feb 2023 22:23:54 +0100 Valid Until: Mon, 14 Feb 2033 22:23:54 +0100	OpenVPN Server	

2-Création d'un utilisateur avec son certificat

The screenshot shows the 'User Properties' configuration page in pfSense. The 'Users' tab is selected. The user is defined by 'USER'. The 'Disabled' checkbox is unchecked. The 'Username' is 'Userasm'. The 'Password' field is masked with dots. The 'Full name' field is empty. The 'Expiration date' field is empty. The 'Custom Settings' checkbox is unchecked. The 'Group membership' is set to 'admins'. The 'Certificate' checkbox is unchecked. There are buttons to move the user between the 'Member of' and 'Not member of' lists.

User Properties

Defined by: USER

Disabled: This user cannot login

Username: Userasm

Password: [masked]

Full name: [empty]

Expiration date: [empty]

Custom Settings: Use individual customized GUI options and dashboard layout for this user.

Group membership: admins

Certificate: Click to create a user certificate

3-Création d'un serveur OpenVPN

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

General Information

Description
A description of this VPN for administrative reference.

Disabled Disable this server
Set this option to disable this server without removing it from the list.

Mode Configuration

Server mode Remote Access (SSL/TLS + User Auth)

Backend for authentication Local Database

Device mode tun - Layer 3 Tunnel Mode
tun mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
tap mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol UDP on IPv4 only

Interface WAN
The interface or Virtual IP address where OpenVPN will receive client connections.

Local port 1195
The port used by OpenVPN to receive client connections.

Cryptographic Settings

TLS Configuration Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key.

Peer Certificate Authority ASM-CERTIF

Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check Check client certificates with OCSP

Server certificate ASM-VPN (Server: Yes, CA: ASM-CERTIF, In Use)

DH Parameter Length 2048 bit
Diffie-Hellman (DH) parameter set used for key exchange. [i](#)

ECDH Curve Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Negotiation Enable Data Encryption Negotiation
This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

Data Encryption Algorithms

AES-128-CFB8 (128 bit key, 128 bit block)	AES-256-GCM
AES-128-GCM (128 bit key, 128 bit block)	AES-128-GCM
AES-128-OFB (128 bit key, 128 bit block)	CHACHA20-POLY1305
AES-192-CBC (192 bit key, 128 bit block)	
AES-192-CFB (192 bit key, 128 bit block)	
AES-192-CFB1 (192 bit key, 128 bit block)	
AES-192-CFB128 (192 bit key, 128 bit block)	

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.0.0.0/8"/> <small>This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.</small>
IPv6 Tunnel Network	<input type="text"/> <small>This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.</small>
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	<input type="text" value="192.168.200.0/24"/> <input type="button" value="x"/> <small>IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
IPv6 Local network(s)	<input type="text"/> <small>IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
Concurrent connections	<input type="text"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>
Allow Compression	<input type="button" value="Refuse any non-stub compression (Most secure)"/> <input type="button" value="v"/> <small>Allow compression to be used with this VPN instance.</small>
Dynamic IP	<input type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Topology	<input type="button" value="net30 - Isolated /30 network per client"/> <input type="button" value="v"/> <small>Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".</small>
Ping settings	
Inactive	<input type="text" value="300"/> <small>Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.</small>
Ping method	<input type="button" value="keepalive - Use keepalive helper to define ping configuration"/> <input type="button" value="v"/> <small>keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows: ping = interval ping-restart = timeout*2 push ping = interval push ping-restart = timeout</small>
Interval	<input type="text" value="10"/>
Timeout	<input type="text" value="60"/>
Advanced Client Settings	
DNS Default Domain	<input checked="" type="checkbox"/> Provide a default domain name to clients
DNS Default Domain	<input type="text" value="assurmer.fr"/>
DNS Server enable	<input checked="" type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	<input type="text" value="172.16.0.1"/> <input type="button" value="x"/>

4-Installation du package « openvpn-client-export »

System / Package Manager / Installed Packages

Installed Packages Available Packages

Name	Category	Version	Description	Actions
✓ openvpn-client-export	security	1.6_9	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	

Package Dependencies:
[openvpn-client-export-2.5.8](#) [openvpn-2.5.4_1](#) [zip-3.0_1](#) [p7zip-16.02_3](#)

= Update = Current
 = Remove = Information = Reinstall

Newer version available

Package is configured but not (fully) installed or deprecated

5-Mise en place des règles de pare-feu, afin d'accéder à la DMZ depuis le VPN

Firewall / Rules / WAN

Floating **WAN** LAN DMZ OpenVPN

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input type="checkbox"/> ✓ 0/240 B	IPv4 *	*	*	WAN address	*	*	none		accès distant open vpn	

Firewall / Rules / OpenVPN

Floating WAN LAN DMZ **OpenVPN**

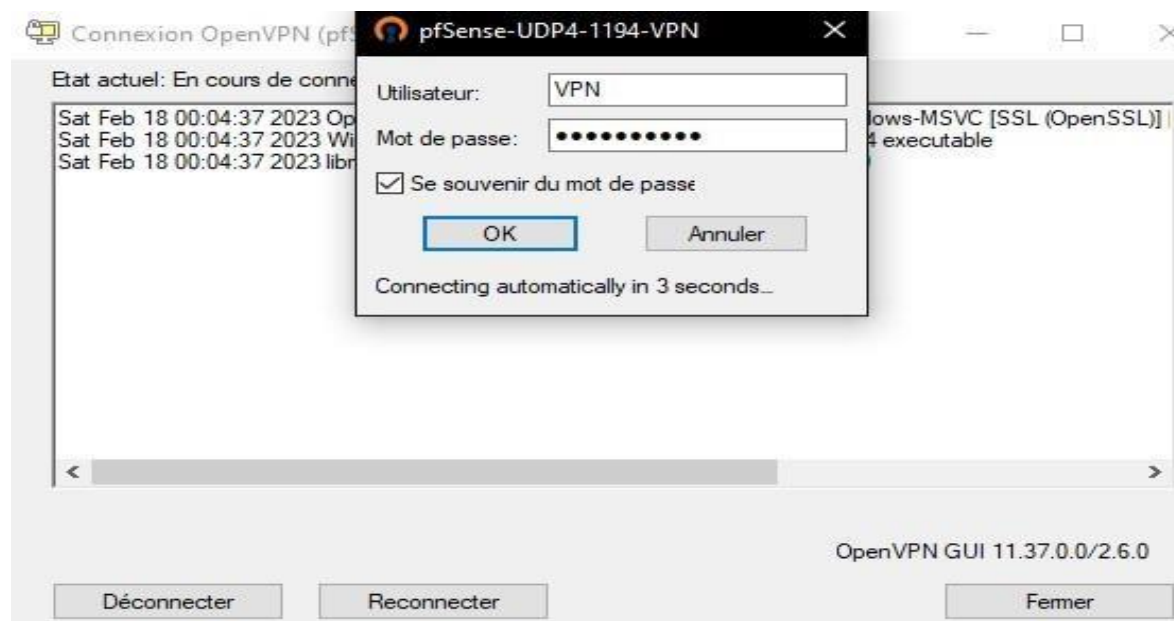
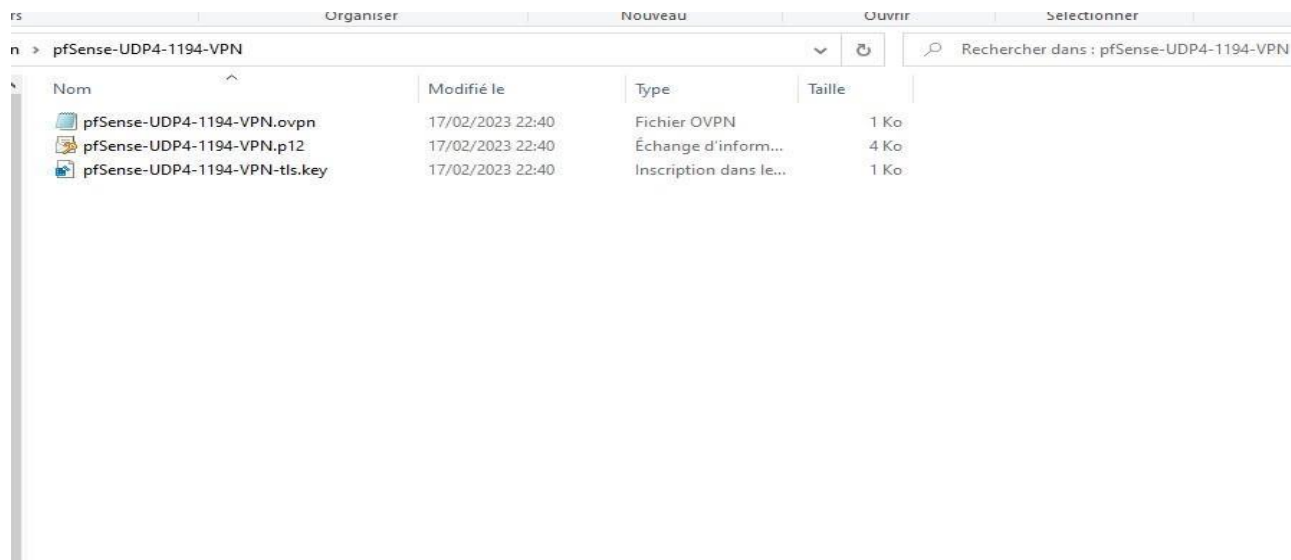
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 0/0 B	IPv4 TCP	*	*	192.168.200.2	80 (HTTP)	*	none		accès wintranet	

6-Exportation et installation du client sur l'utilisateur distant.

OpenVPN Clients

User	Certificate Name	Export
VPN	VPN-CERTIF-USER	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none"> Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none"> Archive Config File Only - Current Windows Installers (2.5.8-ix04): <ul style="list-style-type: none"> 64-bit 32-bit - Legacy Windows Installers (2.4.12-ix01): <ul style="list-style-type: none"> 10/2016/2019 7/8.1/2012:2 - Viscosity (Mac OS X and Windows): <ul style="list-style-type: none"> Viscosity Bundle Viscosity Inline Config

Only OpenVPN-compatible user certificates are shown



B- Veeam Backup

Prérequis :

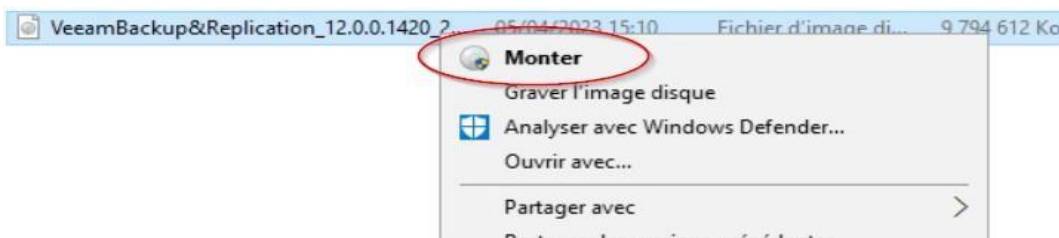
- Nombre de mémoire RAM conséquent pour assurer les sauvegardes : 8Go
- Un disque dur possédant l'espace nécessaire afin d'accueillir les sauvegardes des différentes VM
- L'ISO d'installation de Veeam Backup & Réplication

(<https://www.veeam.com/fr/virtual-machine-backup-solution-free.html>)



Procédure d'installation :

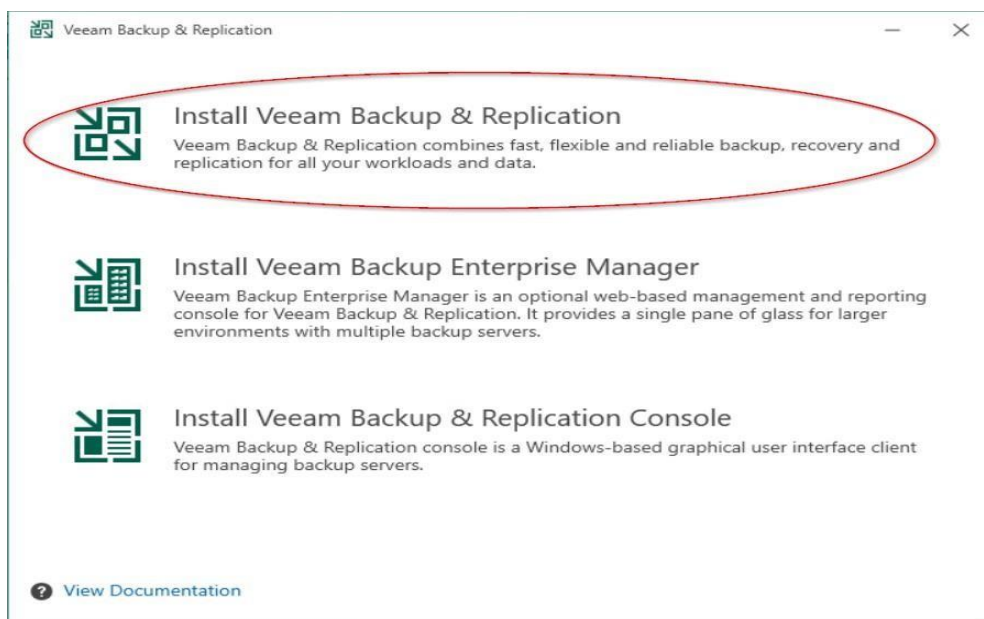
1. Après avoir installé le fichier ISO de Veeam Backup & Réplication, il suffit de faire un clic-droit, et sélectionner l'option « Monter ».



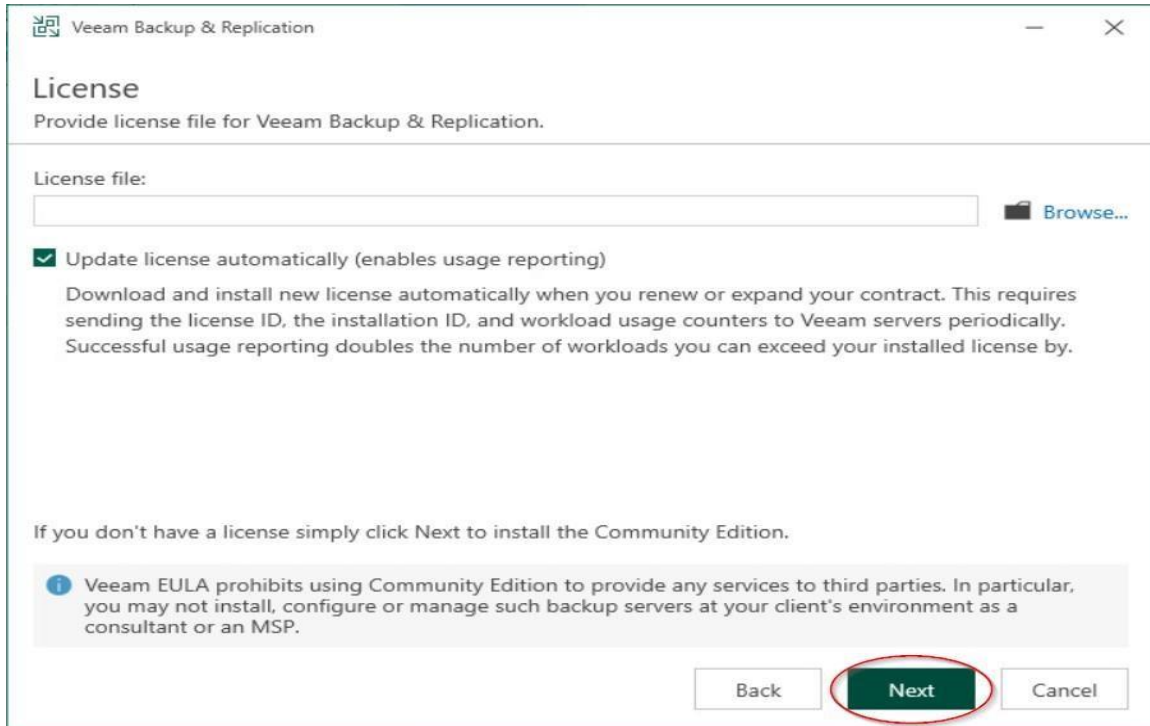
2. Ouvrez ensuite le fichier exécutable « setup ».



3. Vous pourrez alors procéder à l'installation de l'utilitaire Veeam ; sélectionnez « Install Veeam Backup & Réplication »



4. Il nous sera alors demandé de sélectionner une licence. Dans notre cas nous utilisons la version Gratuite, on cliquera alors simplement sur « Next ».



Veeam Backup & Replication

License

Provide license file for Veeam Backup & Replication.

License file:

 [Browse...](#)

Update license automatically (enables usage reporting)

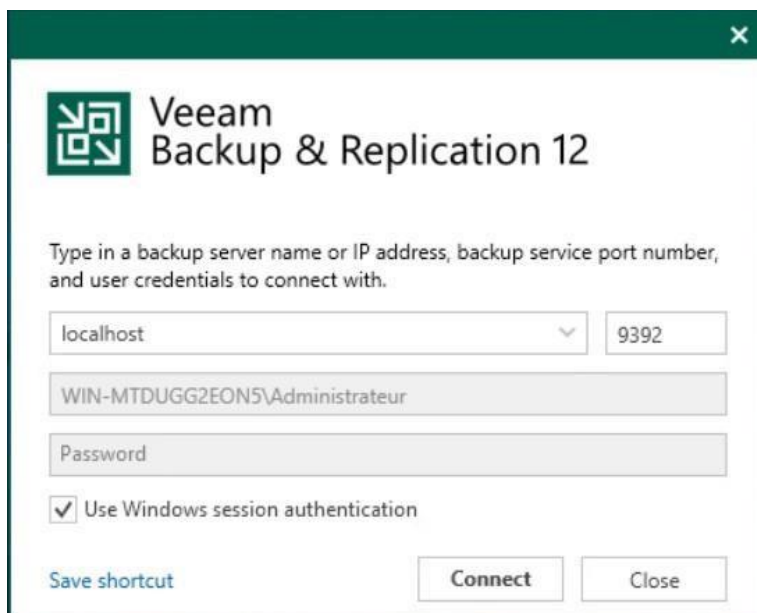
Download and install new license automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to Veeam servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.

If you don't have a license simply click Next to install the Community Edition.

i Veeam EULA prohibits using Community Edition to provide any services to third parties. In particular, you may not install, configure or manage such backup servers at your client's environment as a consultant or an MSP.

[Back](#) **Next** [Cancel](#)

5. À la suite de l'installation, vous devrez lancer « Veeam Backup & Réplication Console ».



Veeam Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

localhost 9392

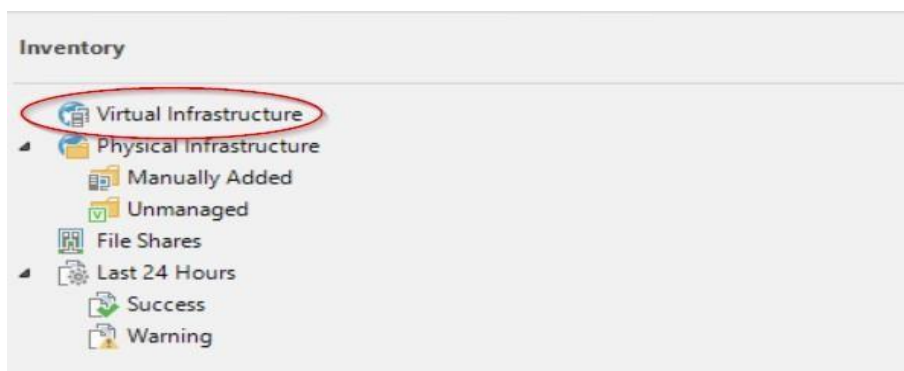
WIN-MTDUGG2EON5\Administrateur

Password

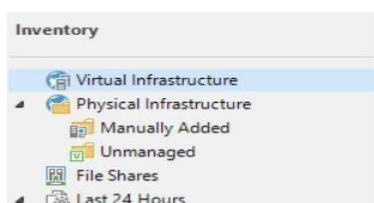
Use Windows session authentication

[Save shortcut](#) [Connect](#) [Close](#)

7. Après vous être authentifié, vous aurez accès à l'interface de Veeam. Pour lier notre serveur de sauvegarde à l'hyperviseur que l'on souhaite backuper, on doit se rendre dans « inventory » puis « Virtual infrastructure ».



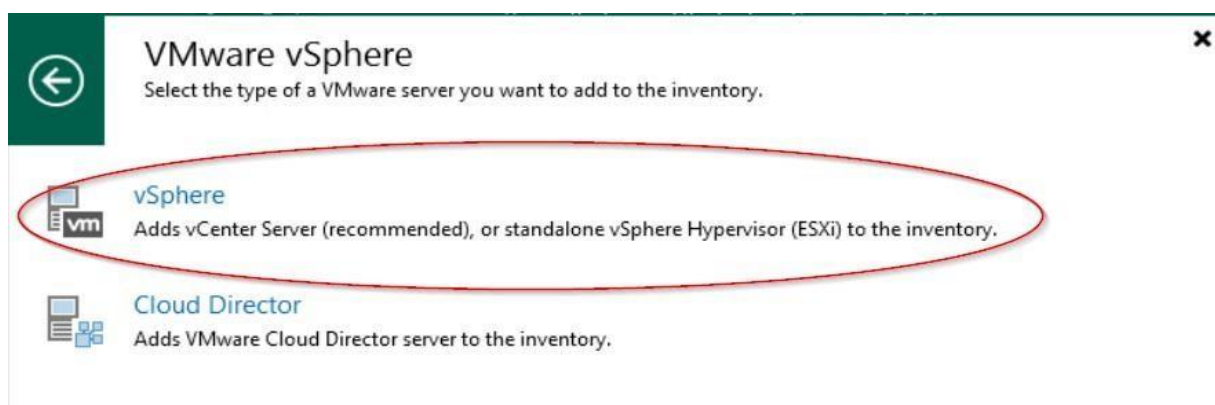
8. On se rendra alors dans « Add-Server »


Add Server

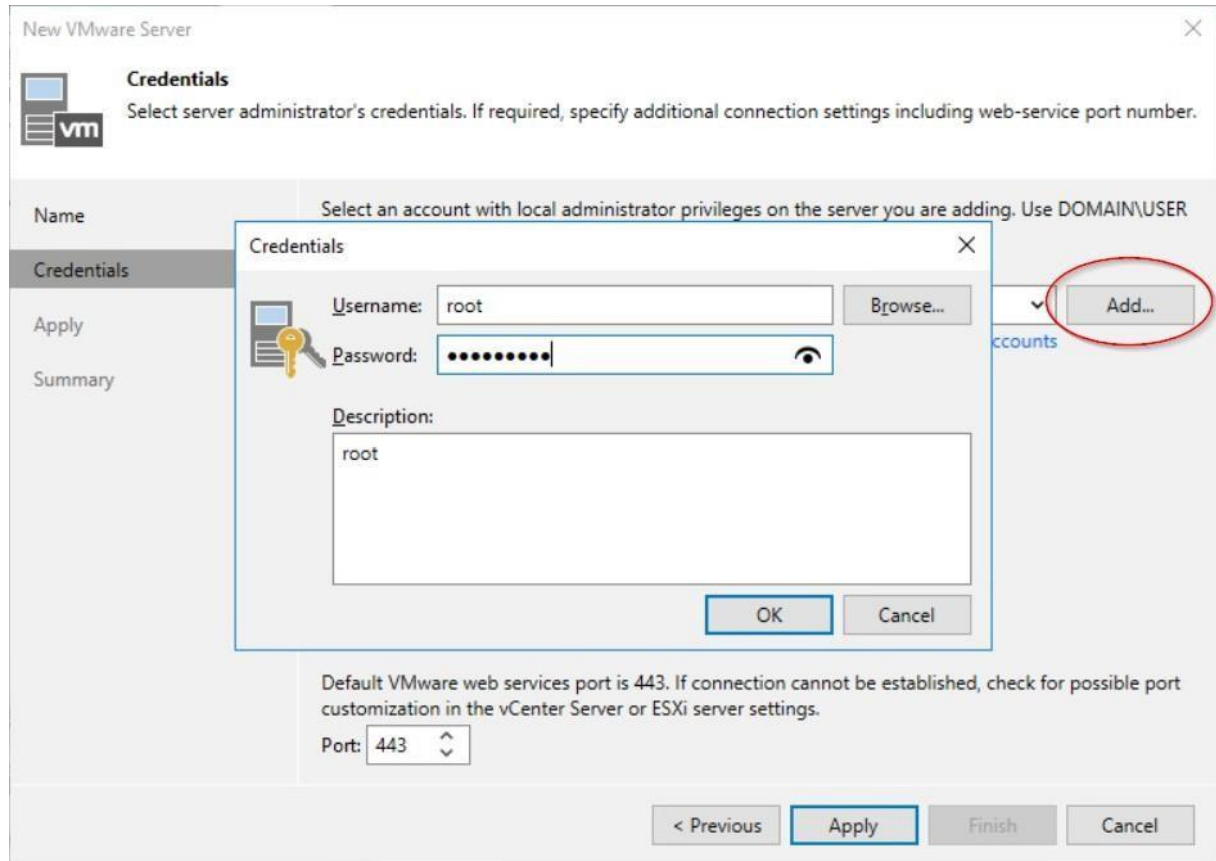
Before using Veeam Backup & Replication, you must register your protected data sources in the inventory. To start this process, click the Add Server button in the ribbon (or just click this text).

For VMware vSphere protection, add a vCenter Server. You can also add ESXi hosts individually. Adding vCenter Server is preferred, because it makes Veeam Backup & Replication

Dans notre cas, on choisit de backuper un ESXI, on se rendra donc dans « VMware vSphere », puis vSphere.

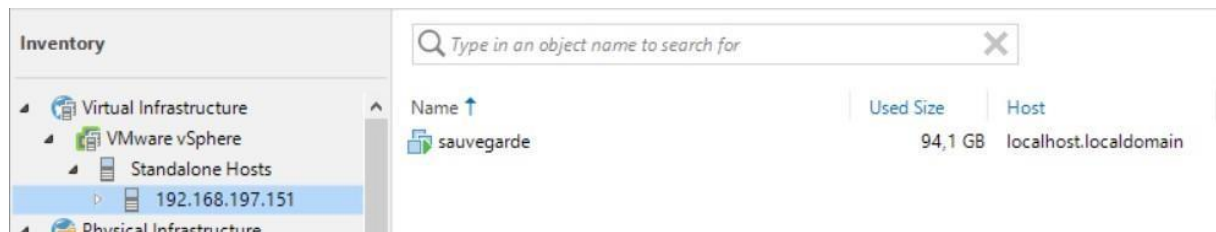


Après avoir renseigné l'adresse IP de notre hôte ESXI, on passera à l'étape suivante pour ajouter les identifiants servant à établir une connexion à l'ESXI, dans notre cas on utilise le compte root. (Si le port d'accès à l'hôte est autre que le port https par défaut, vous devrez le modifier dans cette même rubrique.)



À la suite de cela, vous pourrez cliquer sur « Apply », il vous sera alors demandé d'accepter le certificat auto-généré de l'ESXi lors de la première connexion, puis si vos identifiants sont corrects, Veeam récupérera les informations propres à l'ESXi.

Vous pourrez désormais consulter la liste des machines virtuelles dans la rubrique « Virtual infrastructure » en cliquant sur l'IP ou le nom de votre Hyperviseur.



Afin de connaître comment créer ou restaurer des backups de machines virtuelles, merci de vous rendre sur la procédure dédiée.

III. Quelles sont les impacts

A- OpenVPN

Avec la multiplication des équipements mobile et le développement du télétravail depuis 2020, il est nécessaire de disposer d'outils et service sécurisé, afin d'accéder aux ressources de l'entreprise à distance. Il est nécessaire de disposer d'un VPN. En effet, il permet d'accéder au SI depuis un site distant et de disposer d'un canal sécurisé depuis l'extérieur de l'entreprise.

Dans une entreprise, quelle que soit sa taille, les aspects liés à la sécurité informatique sont fondamentaux. L'entreprise doit pouvoir échanger des données sensibles avec ses filiales ou partenaires, en toute sérénité. De plus, les processus d'interconnexion répondent parfaitement aux nouveaux usages, comme la mobilité, le multi-site ou encore le télétravail.

La mise en place d'un VPN pour l'accès distant est recommandée par la CNIL avec une solution de chiffrement suffisante. De plus le logiciel OpenVPN est certifié par l'ANSSI.

B- Veeam Backup

Les solutions de sauvegarde permettent de sauver de manière intègre les données (fichiers, logiciels, systèmes d'information) de l'entreprise pour assurer une reprise d'activité rapide notamment après une attaque de type ransomware ou un sinistre. Ces sauvegardes proposent en effet une restauration facilitée des données devenues inaccessibles. Elles peuvent être faites localement sur les infrastructures d'une organisation.

Les sauvegardes maîtrisées et protégées, associées à un plan de reprise d'activité, constituent un élément essentiel face aux menaces telles que les ransomware ou autres sinistres. Il est nécessaire de définir un plan de sauvegarde (types de sauvegardes, fréquence, espace de stockage, etc.) Ainsi que de réaliser des tests d'intégrité des sauvegardes et des tests de restauration réguliers.

Il est important de suivre les recommandations de la CNIL, prévoir des sauvegardes incrémentales quotidiennes et des sauvegardes complètes à intervalles réguliers. Et ne pas conserver les sauvegardes de donnée au même endroit que les machines les hébergeant.

Le serveur Veeam Backup & Réplication permet de sauvegarder et de restaurer des serveurs critiques tel que l'Active Directory, Mail et de stockage.