cockpit
IT Service Manager

Supervision - Accès aux systèmes Windows

Document FAQ

Table des matières

Introduction 3
Connexion sécurisée (recommandée) 4
I. Service d'accès distant 4
II. Création du certificat 4
III. Configuration de WinRM 4
IV. Vérifier la configuration 5
V. Configuration du pare-feu 7
VI. Tests 8
VII. Configuration complémentaire (optionnelle) 9
A. Forcer l'utilisation d'un mode d'authentification 9
B. Suppression du listener HTTP 9
Connexion non sécurisée (non recommandée) 10
I. Service d'accès distant 10
II. Configuration de WinRM 10
III. Vérifier la configuration 10
IV. Tests 11
Mode d'authentification « SPNEGO » 12
I. Service d'accès distant 12
II. Configuration de WinRM 12
III. Tests 12
Utilisateur système 13
I. Paramètres requis 13
II. Paramètres optionnels 13
Ports 15
Configuration du portail 16

Introduction

L'objectif de ce document est d'indiquer comment configurer un accès sur les systèmes Windows afin de les superviser, de les inventorier et de collecter les métriques via le moteur Cockpit IT Service Manager.

Il est recommandé d'utiliser le protocole WinRM afin de superviser et/ou d'inventorier les systèmes Windows.
Plusieurs modes d'authentification sont possibles, 3 modes sont décrits dans le présent document. Le tableau ci-après indique les modes d'authentification compatibles avec les différentes architectures.

Moteur Cockpit IT Service Manager		**Serveur Windows cible**	**Compatibilité du mode d'authentification**		
			SPNEGO	**Basic Unencrypted**	**Basic encrypted**
Linux		-	Non	Oui	Oui
Windows	Dans le domaine	Dans le domaine	Oui	Oui	Oui
		Hors du domaine	Non	Oui	Oui
	Hors du domaine	Dans le domaine	Non	Oui	Oui
		Hors du domaine	Oui	Oui	Oui

Notes :

- Le mode d'authentification « SPNEGO » est le plus simple à mettre en œuvre mais il ne fonctionne pas dans tous les cas (notamment si le moteur Cockpit IT Service Manager est installé sur un serveur Linux).
- Le mode d'authentification « Basic Unencrypted » fonctionne dans tous les cas mais n'est pas recommandé car les données transitent par le réseau sans être encryptées.
- **Le mode d'authentification « Basic Encrypted » est recommandé car il fonctionne dans tous les cas et est sécurisé.**

Connexion sécurisée (recommandée)

La procédure ci-après indique comment configurer un accès avec un mode d'authentification « Basic Encrypted ».

I. Service d'accès distant

Au niveau de la gestion des services du serveur à superviser, le service « Windows Remote Management (WS-Management) » doit être actif et doit être démarré automatiquement (normalement, il l'est par défaut).

II. Création du certificat

Se connecter au serveur cible avec le compte « administrator » (il faut impérativement utiliser ce compte pour effectuer la configuration).
Créer un certificat en exécutant la commande suivante (remplacer <COMPUTERNAME> par le nom DNS complet du serveur, en respectant la casse).

new-SelfSignedCertificate -DnsName "<COMPUTERNAME>" -CertStoreLocation Cert:\LocalMachine\My

Copier la valeur Thumbprint générée par la commande.

```
Directory: Microsoft.PowerShell.Security\Certificate::LocalMachine\My


Thumbprint                                Subject
----------                                -------
BB30999234AE9CE7D1C631F6052428136CD23333  CN=WIN-UHEPFOLN33D
```

III. Configuration de WinRM

Se connecter au serveur cible avec le compte « administrator » (il faut impérativement utiliser ce compte pour effectuer la configuration).
Ouvrir une fenêtre de commande en tant qu'administrateur.
Contrôler la configuration WinRM en exécutant la commande suivante.

winrm get winrm/config/service

Si la commande retourne la liste des paramètres de configuration (exemple ci-après). Le service WinRM est déjà opérationnel, il faut passer à l'étape suivante.

```
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 15
...
```

Si la commande retourne un message d'erreur, paramétrer et démarrer le service WinRM en exécutant le commande suivante. Cette commande démarre le service « Windows Remote Management (WS-Management) » et le configure afin de le lancer automatiquement. Elle configure également un port d'écoute HTTP (port 5985) et met à jour les règles du pare-feu afin de le rendre accessible.

winrm quickconfig

Afin de configurer l'accès avec un mode d'authentification « Basic Encrypted », exécuter les commandes suivantes (remplacer <COMPUTERNAME> par le nom DNS complet du serveur et <THUMBPRINT> par celui qui a été généré).

winrm create winrm/config/listener?Address=+Transport=HTTPS '@{Hostname="<COMPUTERNAME>";CertificateThumbprint="<THUMBPRINT>"}'*

winrm set winrm/config/service/auth '@{Basic="true"}'
winrm set winrm/config/client '@{TrustedHosts=""}'*

IV. Vérifier la configuration

Exécuter la commande suivante et vérifier les valeurs des paramètres surlignés.

winrm get winrm/config/service

```
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 1500
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = false
    Auth
        Basic = true
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    IPv4Filter = *
    IPv6Filter = *
    EnableCompatibilityHttpListener = false
    EnableCompatibilityHttpsListener = false
    CertificateThumbprint
    AllowRemoteAccess = true
```

Exécuter la commande suivante et vérifier les valeurs des paramètres surlignés.

winrm get winrm/config/client

```
Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
        Basic = true
        Digest = true
        Kerberos = true
        Negotiate = true
        Certificate = true
        CredSSP = false
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    TrustedHosts = *
```

Exécuter la commande suivante et vérifier les valeurs des paramètres surlignés.

winrm e winrm/config/listener

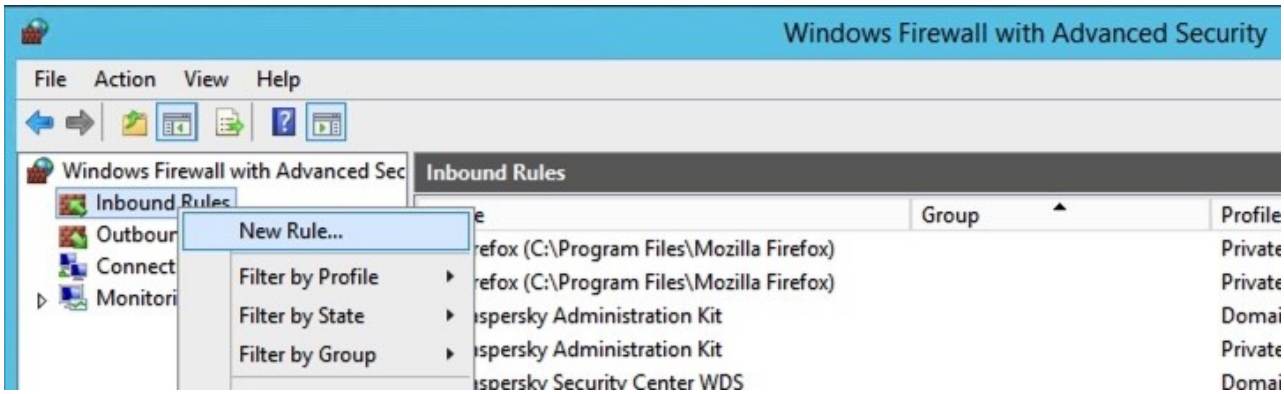
S'assurer que le thumbprint correspond bien au certificat créé.

```
Listener
        Address = *
        Transport = HTTPS
        Port = 5986
        Hostname = WIN-UHEPFOLN33D
        Enabled = true
        URLPrefix = wsman
        CertificateThumbprint = BB30999234AE9CE7D1C631F6052428136CD23333
        ListeningOn = 127.0.0.1, 172.16.42.226, ::1, 2001:0:5ef5:73b8:142c:140:53ef:d51d,fe80::5efe:172.1
        6.42.226%13, fe80::142c:140:53ef:d51d%11#
```

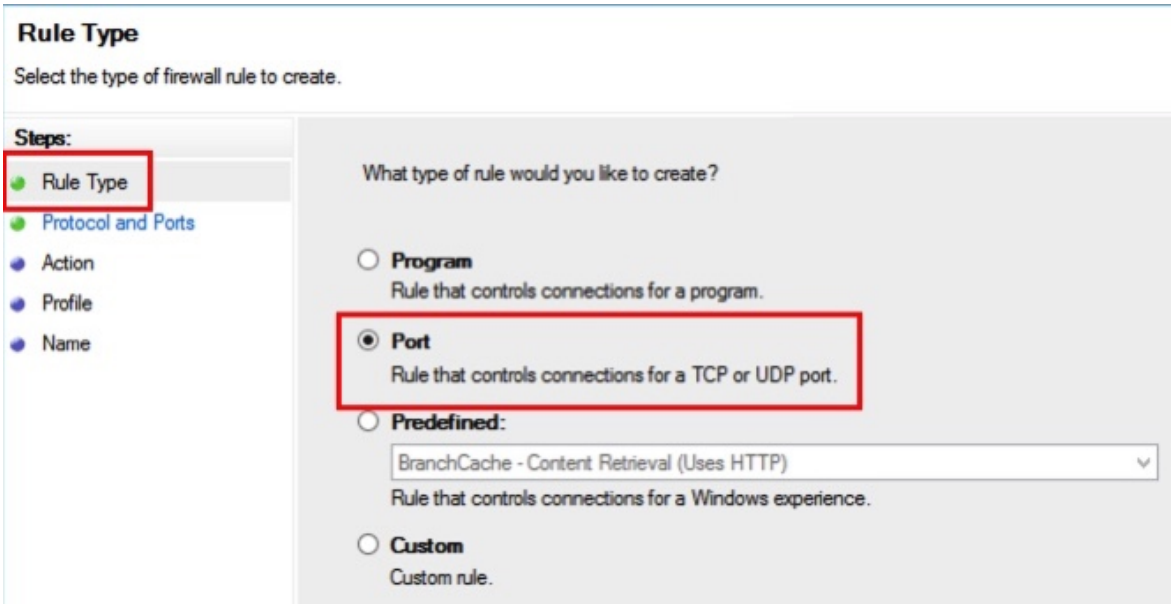
V. Configuration du pare-feu

Ouvrir le gestionnaire de pare-feu Windows (Control Panel → System and Security → Windows Firewall → Advanced Settings).

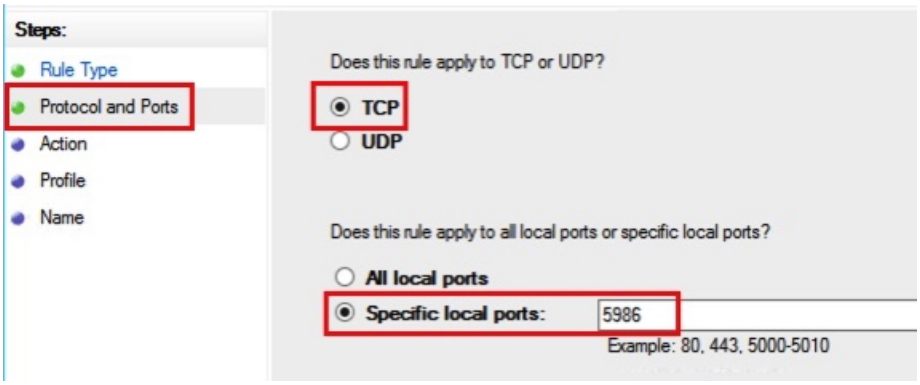
Créer une nouvelle règle d'autorisation entrante.



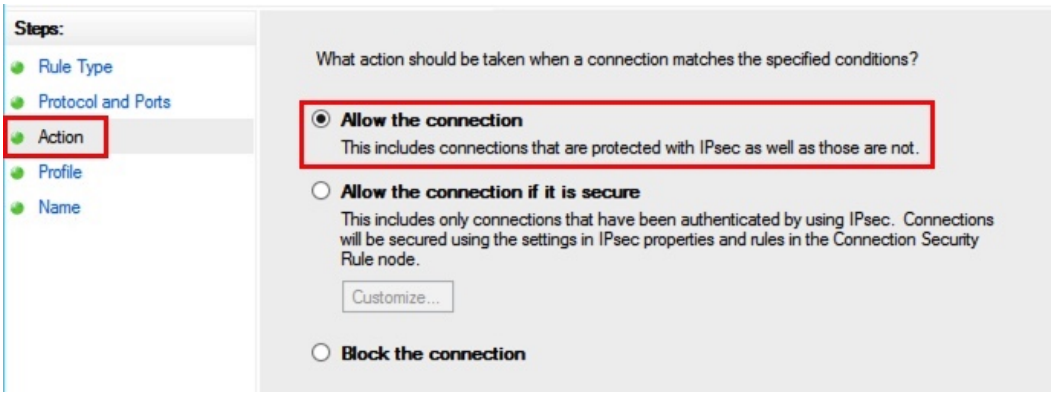
Sélectionner le type « Port ».



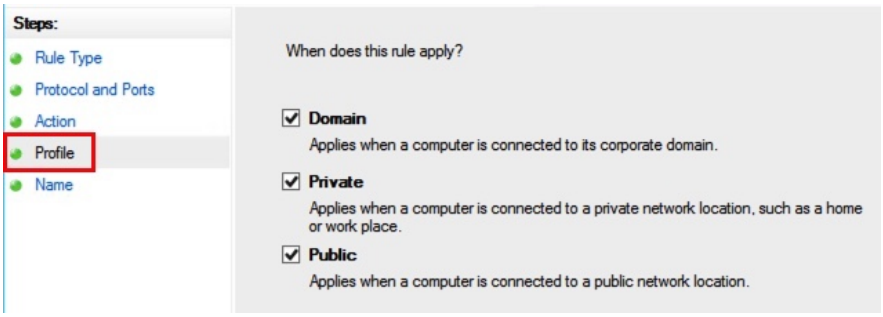
Sélectionner le protocole « TCP » et spécifier le port « 5986 »



Autoriser les connexions.

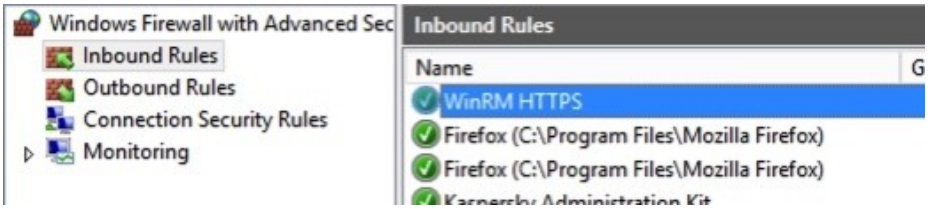


Autoriser tous les réseaux.



Nommer la règle.

Editer la règle.



VI. Tests

Depuis un poste Windows distant (qui accède au serveur à superviser), ouvrir une fenêtre de commande en tant qu'administrateur.

Exécuter la commande suivante, le mot de passe de l'utilisateur doit être demandé par le serveur cible.

winrm g winrm/config/service -r:https://<serveur cible>:5986 -u:<utilisateur> -skipCAcheck

VII. Configuration complémentaire (optionnelle)

A. Forcer l'utilisation d'un mode d'authentification

Le paramètre d'authentification « Negociate = true » permet au système d'exploitation Windows de sélectionner automatiquement le bon mode de connexion.

Toutefois si vous rencontrez des problèmes de connexion, vous pouvez tester un mode de connexion en forçant son utilisation.

Par exemple passer le mode « Basic » en « false » pour forcer l'utilisation du mode « Kerberos » avec la commande suivante :

winrm set winrm/config/service/auth '@{Basic="fase"}'

Exécuter la commande suivante afin de vérifier la configuration.

winrm get winrm/config/service

Contrôler les valeurs des paramètres surlignés, dans cet exemple le mode d'authentification « Kerberos » est utilisé.

```
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
    ...
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = false
    Auth
        Basic = false
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
```

B. Suppression du listener HTTP

Si vous souhaitez supprimer le listener HTTP (car vous utilisez le listener HTTPS), il faut utiliser la commande suivante.

winrm delete winrm/config/listener?Address=+Transport=HTTP*

Afin d'obtenir la liste des listeners exécuter la commande winr/config/ suivante.

winrm e winrm/config/listener

Connexion non sécurisée (non recommandée)

La procédure ci-après indique comment configurer un accès avec un mode d'authentification « Basic Unencrypted ».

I. Service d'accès distant

Au niveau de la gestion des services du serveur à superviser, le service « Windows Remote Management (WS-Management) » doit être actif et doit être démarré automatiquement (normalement, il l'est par défaut).

II. Configuration de WinRM

Se connecter au serveur cible avec le compte « administrator » (il faut impérativement utiliser ce compte pour effectuer la configuration).
Ouvrir une fenêtre de commande en tant qu'administrateur.
Contrôler la configuration WinRM en exécutant la commande suivante.

winrm get winrm/config/service

Si la commande retourne la liste des paramètres de configuration (exemple ci-après). Le service WinRM est déjà opérationnel, il faut passer à l'étape suivante.

```
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 15
...
```

Si la commande retourne un message d'erreur, paramétrer et démarrer le service WinRM en exécutant le commande suivante. Cette commande démarre le service « Windows Remote Management (WS-Management) » et le configure afin de le lancer automatiquement. Elle configure également un port d'écoute HTTP (port 5985) et met à jour les règles du pare-feu afin de le rendre accessible.

winrm quickconfig

Afin de configurer l'accès avec un mode d'authentification « Basic Unencrypted », exécuter les commandes suivantes.

winrm set winrm/config/service/auth '@{Basic="true"}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
winrm set winrm/config/client '@{TrustedHosts=""}'*

III. Vérifier la configuration

Exécuter la commande suivante et vérifier les valeurs des paramètres surlignés.

winrm get winrm/config/service

```
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = true
    Auth
        Basic = true
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    IPv4Filter = *
    IPv6Filter = *
    EnableCompatibilityHttpListener = false
    EnableCompatibilityHttpsListener = false
    CertificateThumbprint
    AllowRemoteAccess = true
```

Exécuter la commande suivante et vérifier les valeurs des paramètres surlignés.

winrm get winrm/config/client

```
Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
        Basic = true
        Digest = true
        Kerberos = true
        Negotiate = true
        Certificate = true
        CredSSP = false
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    TrustedHosts = *
```

IV. Tests

Depuis un poste Windows distant (qui accède au serveur à superviser), ouvrir une fenêtre de commande en tant qu'administrateur.

Exécuter la commande suivante, le mot de passe de l'utilisateur doit être demandé par le serveur cible.

winrm g winrm/config/service -r:http://<serveur cible>:5985 -u:<utilisateur>

Mode d'authentification « SPNEGO »

La procédure ci-après indique comment configurer un accès avec un mode d'authentification « SPNEGO ».

I. Service d'accès distant

Au niveau de la gestion des services du serveur à superviser, le service « Windows Remote Management (WS-Management) » doit être actif et doit être démarré automatiquement (normalement, il l'est par défaut).

II. Configuration de WinRM

Aucune configuration n'est nécessaire, ce mode d'authentification à WinRM fonctionne avec la configuration par défaut.

Exécuter la commande suivante afin de vérifier la configuration.

winrm get winrm/config/service/auth

Contrôler le paramètre « Kerberos », sa valeur doit être « true ».

```
Auth
    Basic = false
    Kerberos = true
    Negotiate = true
    Certificate = false
    CredSSP = false
    CbtHardeningLevel = Relaxed
```

Si cette valeur n'est pas « true », exécuter la commande suivante.

winrm set winrm/config/service/auth '@{Kerberos="true"}'

III. Tests

Depuis un poste Windows distant (qui accède au serveur à superviser), ouvrir une fenêtre de commande en tant qu'administrateur.

Exécuter la commande suivante, le mot de passe de l'utilisateur doit être demandé par le serveur cible.

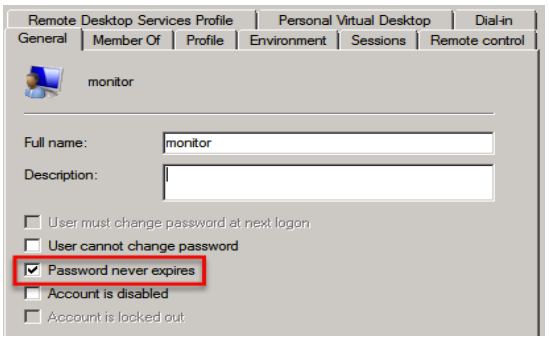
winrm g winrm/config/service -r:http://<serveur cible>:5985 -u:<utilisateur>

Utilisateur système

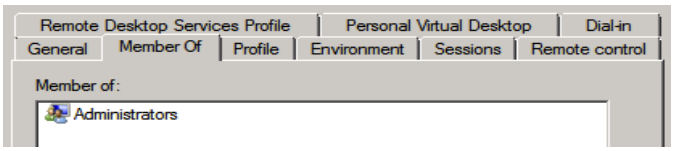
> Note : l'utilisateur peut être un utilisateur local ou de domaine.

I. Paramètres requis

Au niveau du serveur à superviser, créer un utilisateur système protégé par un mot de passe n'expirant jamais.

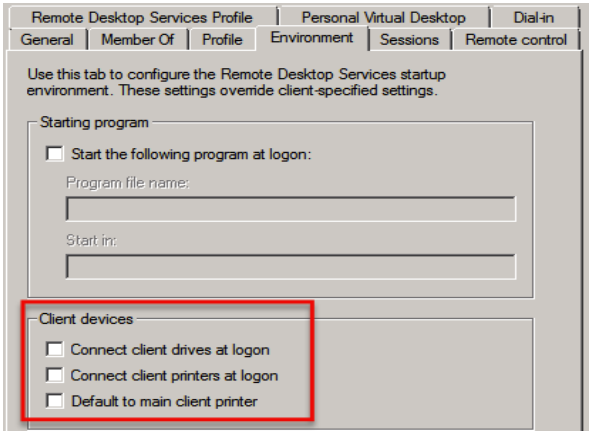


L'utilisateur doit être membre du groupe « Administrators »

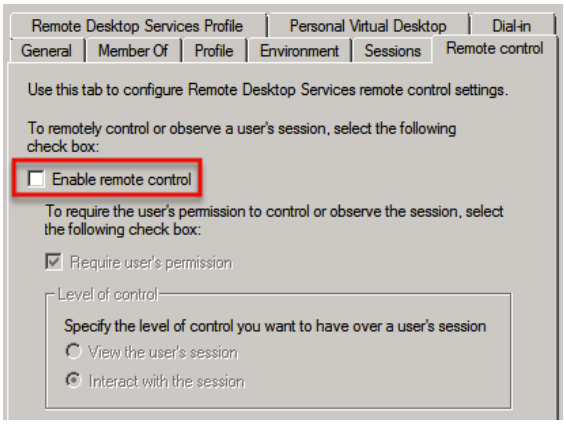


II. Paramètres optionnels

Ne pas connecter les périphériques



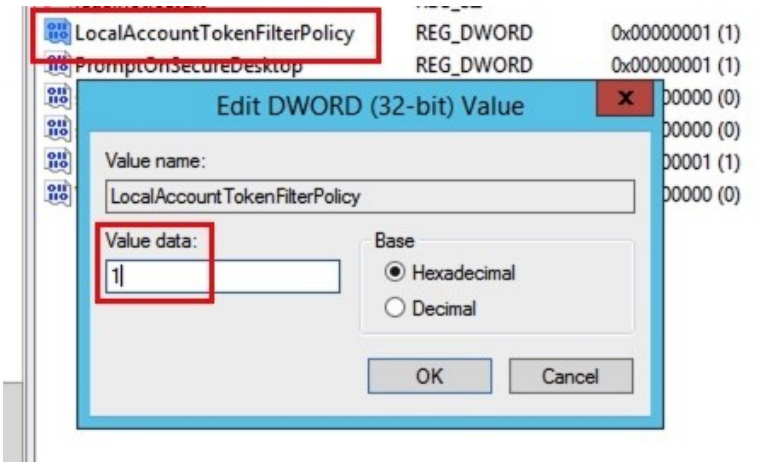
Désactiver la prise de contrôle à distance via « Remote Desktop Services ».



Dans le cas où le moteur de supervision n'est pas dans le même domaine que l'équipement supervisé, il peut être nécessaire de paramétrer l'entrée suivante dans la base de registre :

Chemin : [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

Entrée : LocalAccountTokenFilterPolicy = 1 (REG_DWORD)



Ports

Le port à ouvrir dépend du mode d'authentification :

Mode d'authentification	Port
SPNEGO	5985
Basic Unencrypted	5985
Basic Encrypted	5986

Attention : Assurez-vous que le port utilisé par WinRM est bien disponible (pour certaines versions de Windows, les ports par défaut sont 80 ou 443). Nous recommandons d'utiliser les ports 5985 (mode non SSL) et 5986 (mode SSL). Afin de vérifier le port d'écoute, lancer la commande suivante.

winrm e winrm/config/listener

```
Listener
    Address = *
    Transport = HTTP
    Port = 5985
```

Ou

```
Listener
    Address = *
    Transport = HTTPS
    Port = 5986
```

Configuration du portail

Au niveau du portail Cockpit IT Service Manager, afin de saisir les informations de connexion au serveur, suivre la procédure ci-après.

1. Se rendre dans le menu « Infrastructure / Equipements / Gestion »
2. Ouvrir (mode modification) le serveur cible
3. Au niveau de l'onglet « Paramètres », renseigner les champs suivants

Champ	Remarques
Nom DNS	Nom de l'équipement tel qu'il est identifié sur le réseau et utilisé pour les connexions Pour les connexions sécurisées, il faut utiliser le nom du serveur qui a été indiqué pour générer le certificat.
Cluster	Cocher cette case si le serveur est le noeud logique d'un cluster Si cette case est cochée le superviseur n'utilisera pas les connexions persistantes
Identifiant	Utilisateur de domaine : renseigner « Domain\user ». Utilisateur local : renseigner « user ». Dans le cas où l'équipement supervisé n'est pas dans le domaine où se trouve le moteur de supervision, il peut être nécessaire d'indiquer le nom de l'équipement monitoré en domaine : « Hostname\user ».
Mot de passe	
Type de connexion	WinRM
Port	5985 (mode d'authentification SPNEGO) 5985 (mode d'authentification Basic Unencrypted) 5986 (mode d'authentification Basic Encrypted)
SSL	Cocher cette case pour le mode « Basic Encrypted »
Délai de connexion	10 secondes par défaut, augmenter ce délai si la connexion au serveur est lente

4. Sauvegarder

Fin du document