Powering Business Worldwide

Eaton Intelligent Power® Manager

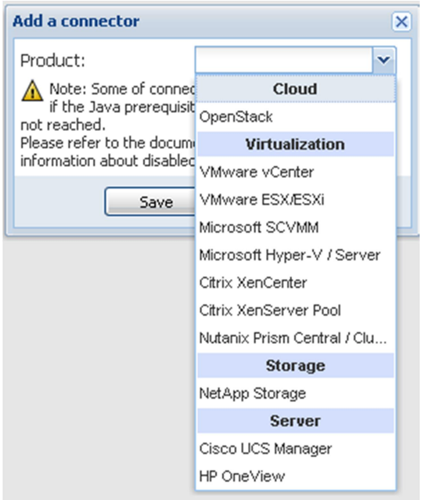
Microsoft Hyper-V

March 14, 2018

Adding a Microsoft Hyper-V/Server connector

Create Microsoft connector

1. Select the Infrastructure connector and click on add



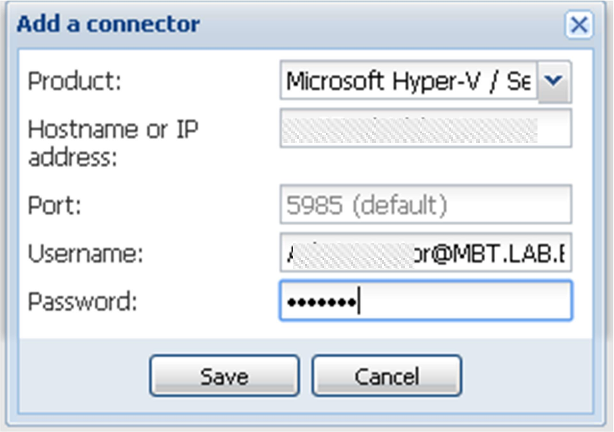
Add a connector

Product:

Note: Some of connec
if the Java prerequisit
not reached.
Please refer to the docum
information about disabled

(figure Add Connector Microsoft Hyper-V 01)

2. Select Microsoft Hyper-V/Server
3. Configure it properly (for details, check the section Configure Microsoft Server authentication)

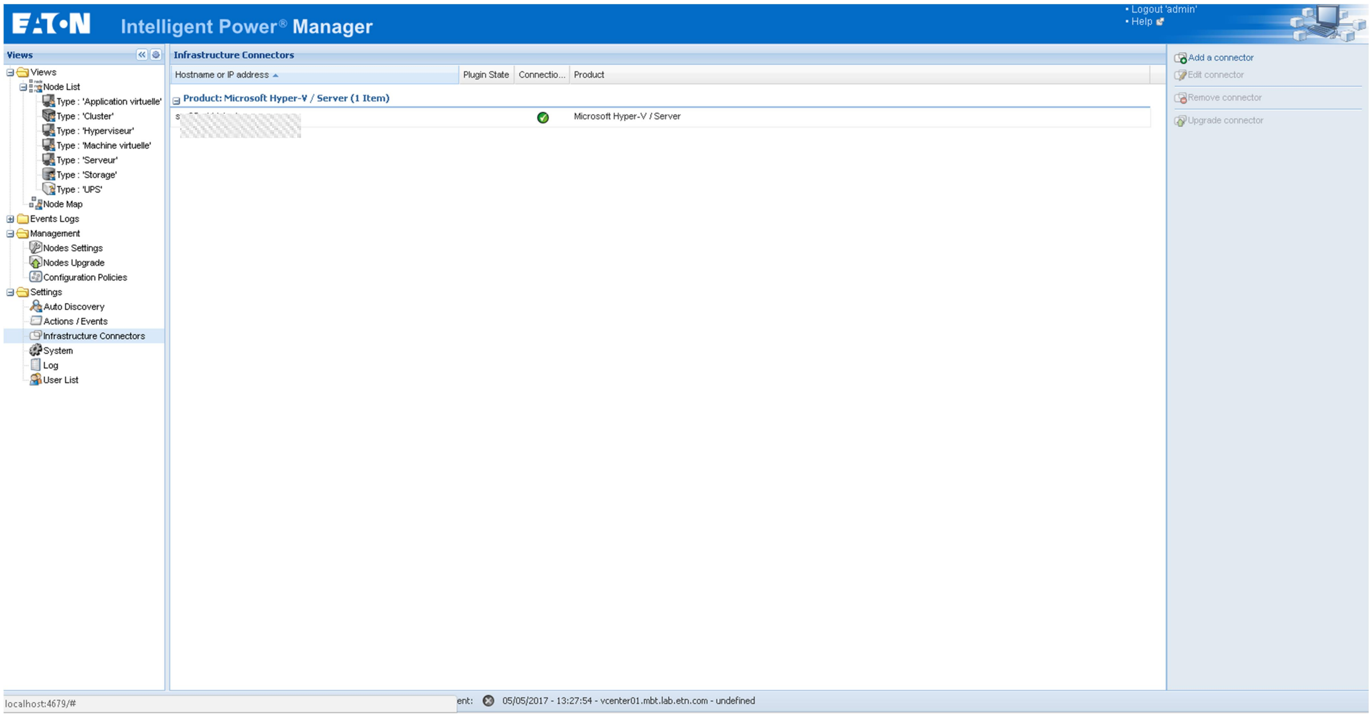


Add a connector

Product:	Microsoft Hyper-V / Se
Hostname or IP address:	[redacted]
Port:	5985 (default)
Username:	A[redacted]or@MBT.LAB.I
Password:	•••••••

(figure AddConnector Microsoft Hyper-V 02)

4. Check that the communication is Ok

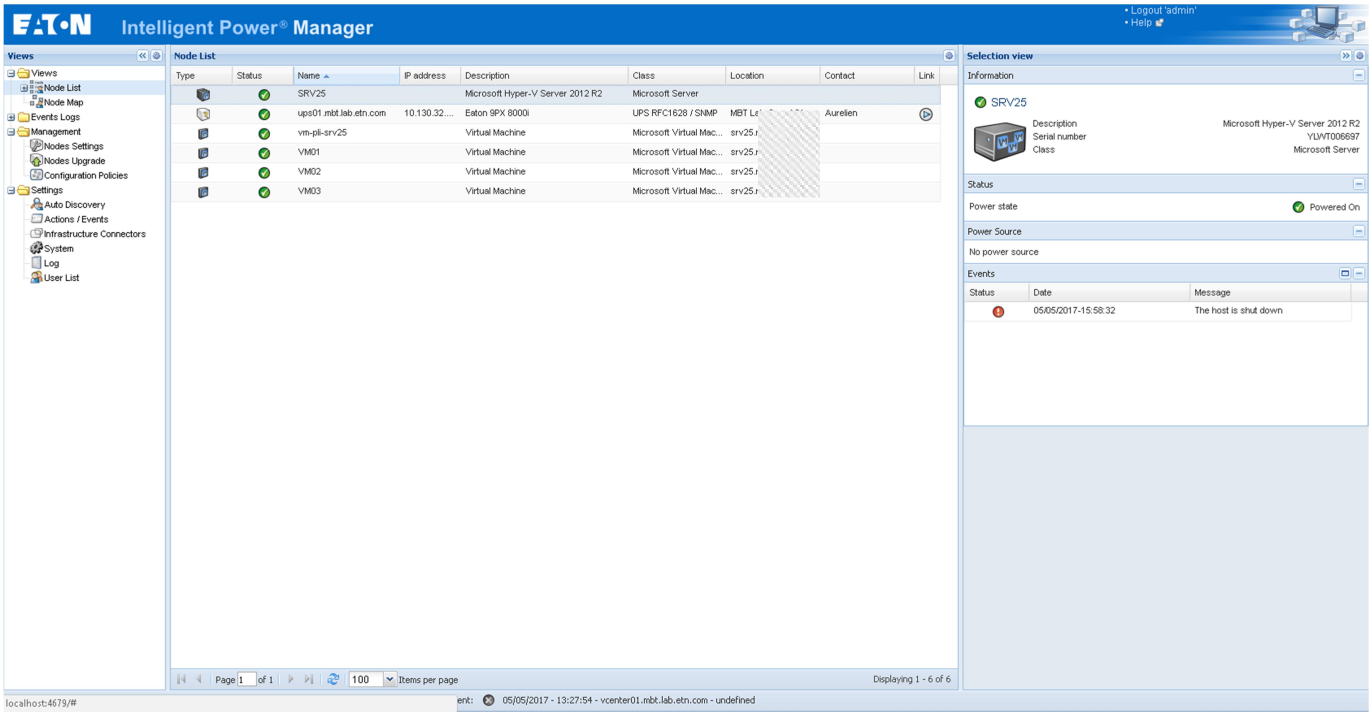


Hostname or IP address	Plugin State	Connectio...	Product
Product: Microsoft Hyper-V / Server (1 Item)			
[redacted]		✓	Microsoft Hyper-V / Server

ent: ⊗ 05/05/2017 - 13:27:54 - vcenter01.mbt.lab.etn.com - undefined

(figure AddConnector Microsoft Hyper-V 03)

Display Data



Type	Status	Name ▲	IP address	Description	Class	Location	Contact	Link
	✓	SRV25		Microsoft Hyper-V Server 2012 R2	Microsoft Server			
	✓	ups01.mbt.lab.etn.com	10.130.32....	Eaton 9PX 8000i	UPS RFC1628 / SNMP	MBT La[redacted]	Aurelien	▷
	✓	vm-pli-srv25		Virtual Machine	Microsoft Virtual Mac...	srv25.r[redacted]		
	✓	VM01		Virtual Machine	Microsoft Virtual Mac...	srv25.r[redacted]		
	✓	VM02		Virtual Machine	Microsoft Virtual Mac...	srv25.r[redacted]		
	✓	VM03		Virtual Machine	Microsoft Virtual Mac...	srv25.r[redacted]		

Page 1 of 1 — 100 Items per page — Displaying 1 - 6 of 6

Information

✓ SRV25

Description	Microsoft Hyper-V Server 2012 R2
Serial number	YLWT006697
Class	Microsoft Server

Status

Power state — ✓ Powered On

Power Source

No power source

Events

Status	Date	Message
!	05/05/2017-15:58:32	The host is shut down

localhost:4679/#

ent: ⊗ 05/05/2017 - 13:27:54 - vcenter01.mbt.lab.etn.com - undefined

(*MSNodeList Hyper v 01*)

Configure Microsoft server authentication

Server side

Configure prerequisites

IPM is able to connect on Microsoft server with two authentication configuration but need somes prerequisites.

WinRM service need to be enable

```
winrm quickconfig
```

WinRM service AllowUnencrypted need to be "true"

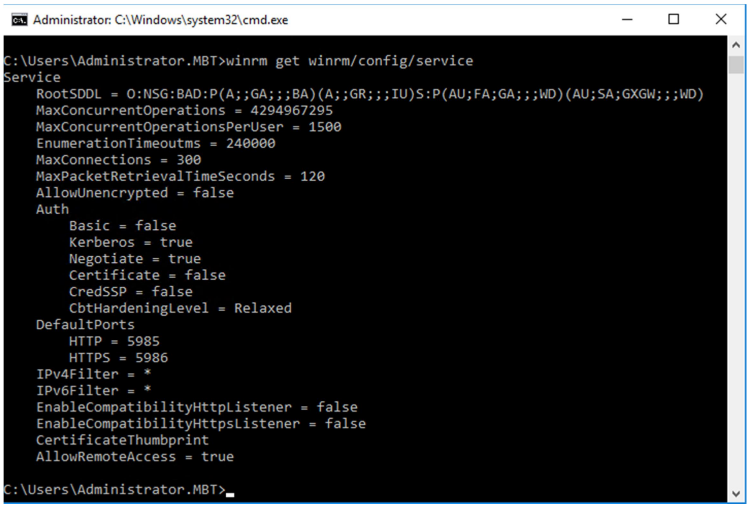
```
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

Or remotely

```
winrm set winrm/config/service @{AllowUnencrypted="true"} -r:microsoftServer01
```

Kerberos Authentication

This is the default configuration, it should be no need to modify it.



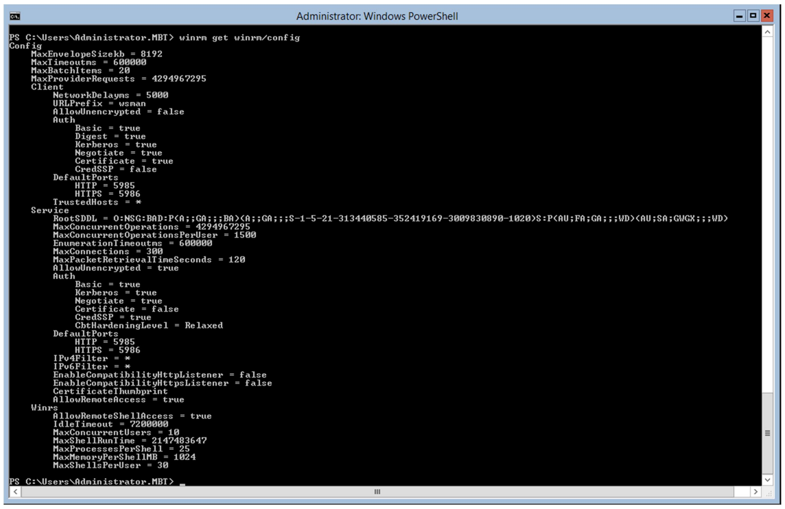
```
C:\Users\Administrator.MBT>winrm get winrm/config/service
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 1500
    EnumerationTimeoutms = 240000
    MaxConnections = 300
  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

C:\Users\Administrator.MBT>
```

(figure AuthConf01)

Basic Authentication

To allow the basic authentication you need to change the “auth” parameters:

```
winrm set winrm/config/service/auth @{Basic="true"}
```



```
PS C:\Users\Administrator.MBT> winrm get winrm/config
Config
    MaxEnvelopeSizekb = 8192
    MaxTimeoutms = 600000
    MaxBatchItems = 20
    MaxProviderRequests = 4294967295
    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 = *
    Service
        RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GA;;;S-1-5-21-313440585-352419169-3009830890-1020)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
        MaxConcurrentOperations = 4294967295
        MaxConcurrentOperationsPerUser = 1500
        EnumerationTimeoutms = 600000
        MaxConnections = 300
        MaxPacketRetrievalTimeSeconds = 120
        AllowUnencrypted = true
        Auth
            Basic = true
            Kerberos = true
            Negotiate = true
            Certificate = false
            CredSSP = true
            CbtHardeningLevel = Relaxed
        DefaultPorts
            HTTP = 5985
            HTTPS = 5986
        IPv4Filter = *
        IPv6Filter = *
        EnableCompatibilityHttpListener = false
        EnableCompatibilityHttpsListener = false
        CertificateThumbprint
        AllowRemoteAccess = true
    Winrs
        AllowRemoteShellAccess = true
        IdleTimeout = 7200000
        MaxConcurrentUsers = 10
        MaxShellRunTime = 2147483647
        MaxProcessesPerShell = 25
        MaxMemoryPerShellMB = 1024
        MaxShellsPerUser = 30

PS C:\Users\Administrator.MBT> _
```

(figure AuthConf02)

Client side (IPM hosted server)

Kerberos Authentication

Windows server

You need to configure the connector with the domain name like "Administrator@DOMAIN.COM"

The domain need to be in uppercase.

IPM should create a file named "krb5.conf" in "%%/IntelligentPowerManager/emc4j/etc/"

Virtual appliance

You need to modify the file "/etc/krb5.conf" as below

INFO : Domain name need to be in Uppercase

vi /etc/krb5.conf

```
[libdefaults]

    default_realm = DOMAIN.COM

[realms]

    DOMAIN.COM = {

        kdc = kerberos.DOMAIN.COM

        admin_server = kerberos.DOMAIN.COM
```

DOMAIN.COM is the Domain where the user is.

kerberos.DOMAIN.COM is the domain name of the Active Directory server

Server time

NOTE : Date need to be the same as the Kerberos server, check ntp services