Technical Requirements

Overview

The VSM collector contains one or more probe services appropriate to the type of environment to be monitored. The collector uses these probe services to collect service management data.

Depending on the nature of the UC environment, the collector may also use remote probe services such as the Machine Proxy Agent (MPA) running directly on the UC servers or work stations being managed.

In all cases, the VSM collector acts as an aggregator and compresses, encrypts then forwards data from all sources to the Virsae cloud computing service.
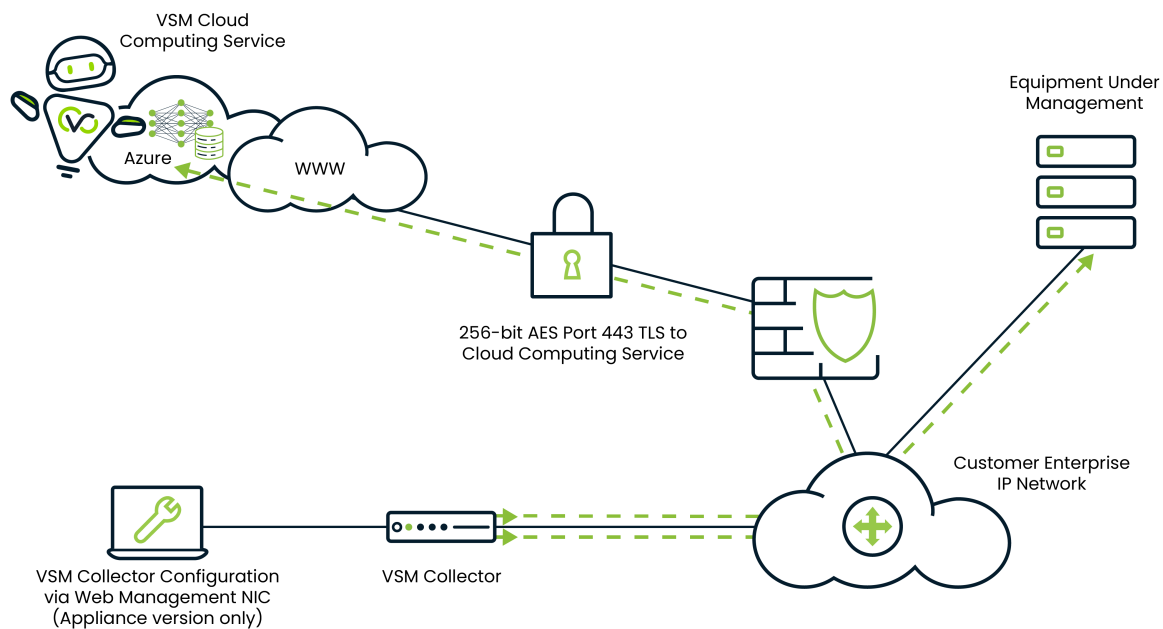
The VSM collector requires outbound access to the Virsae cloud computing service and your Business Partner's Access Concentrator (if required), on TCP Port 443.

Once installed, the VSM collector will automatically connect to the Virsae cloud computing service to retrieve its configuration. It will then open a connection to the configured UC and/or Application Servers and begin the interrogation process using a number of different protocols to collect information. The resulting information is compressed and transmitted over a secure connection, using 256-bit AES encryption, and is stored in the cloud for reporting purposes.

For continuity reasons, the VSM collector requires a static IP address.

VSM Collector

VSM supports three types of collector depending on the specific needs of your customer:

- Windows Software Client: Designed to work in a customer or partner provided physical or virtualised environment.
  - Virsae provides the collector software, the partner or customer provides the physical or virtualised instance and the operating system.

- Linux Virtual Machines: Designed to be deployed within the customer or BP's virtual environment

- - Hyper-V
  - VMWare OVA
- RaspberryPi: To be deployed where the scale is appropriate, or in SMB environments.

Further information and technical requirements for each collector type is available in the Configure the Collector section