Software Vulnerability Manager & Cloud Management Gateway (CMG)

Summary

This document reviews the functionality of Cloud Management Gateway and if it supports third party patches published by vendors like Flexera Software Vulnerability Management.

A recent request by one of our Partners as to whether the scenario of using Software Vulnerability Manager to deploy patches and updates to remote machines via Microsoft's Cloud Management Gateway product for Microsoft Endpoint Configuration Manager (SCCM).

An initial review of the Cloud Management Gateway documentation was undertaken to find out what exactly CMG was and what it did, this led to the opinion of "Yes" and that our SVM product can deploy updates and patches to remote client machines via CMG. But without actually testing it and proving the concept we were not in a position to say "Yes" for definite, but that we believe that it would and that we would test and prove it for ourselves.

Cloud Management Gateway

For those familiar with SCCM and how it works you will also be very familiar with Distribution Points and Management Points, well to put it plain and simple it is a Management Point and Distribution Point in the Microsoft Azure Cloud for deploying software, updates, and patches to remote machines that are part of your enterprise network but are not connected to the network directly or connected via VPN. This takes the headache, the risk, and the cost out of having to try and expose your Enterprises internal SCCM infrastructure to the internet.

Why do I need it?

The requirement for this has become greatly highlighted in the recent situation where employees are having to Work from their home, by deploying CMG Enterprise Administrators can still manage these remote machines, deploy software to them, deploy updates and patches, and also Compliance & Configuration settings without having to provide VPN's or exposure the internal infrastructure as mentioned above.

What we did

In order to prove that CMG would work with Software Vulnerability Manager we created a mini enterprise environment consisting of a DC, CA, SCCM/WSUS/SQL and a selection of Windows 10 clients.

We also required a cloud subscription to Software Vulnerability Manager**, a Microsoft Azure Active Directory account which is free.

To implement CMG we needed to upgrade to Azure Active Directory P2 Premium so we able to configure Device accounts with the Azure Active Directory (AAD) , this is termed as a Hybrid Azure AD Joined account, this means that your machines are both joined to your Windows Domain and to your Azure AD at the same time.

The purpose for this is to give your remote machines an identity in Azure that corresponds to the on-premises computer account, the reason for the auto-enrolment is so that domain-joined machines will do this automatically when you add them to your Windows domain.

We also need a subscription for Azure Services and that the subscription is enabled to purchase other cloud services, as part of the CMG deployment process is the creation of a resource group, a virtual machine which hosts the CMG Web Service, and storage (for Updates to be stored and to host the VM), the two services that need to be enabled within the Azure subscription are Microsoft.ClassicCompute & Microsoft.Storage. The services don't need to be created manually the subscription just needs to have them enabled so that the services can be created in Azure during the CMG deployment process.

The use of an internal PKI Infrastructure is required for the setup, in our test environment we have a Root domain and our root Domain uses PKI and has a certification authority (CA) configured as ROOT CA, A certificate authority server has been created in our child domain and this has been configured as a sub ordinate (intermediate) certificate authority of the Root Domain this means we have a certificate chain to consider.

Part of the configuration process of the CMG requires the use of our Domain Enterprise PKI, as we need to issue a web server certificate which will be applied to the CMG Web Service that the remote clients will connect to and you will also need the Root certificates and the immediate certificates in the chain that apply to your environment, Client Authentication certificates will be required to be issued to the client machines on the domain, this is a requirement of SCCM anyway, so if you are already using SCCM this should already be done, the client machines should already have the Root Certificate and the Intermediaries already deployed to them as part of them being set up for Client Authentication certificates, I would always check to be sure.

We also needed an external public domain name to work with so that we could create some DNS Server entries for the cloud services. For our test domain we purchased a new domain for this purpose the domain is "secuniacmg.co.uk" and we have configured the DNS Servers for this domain to be the Microsoft DNS Servers the reason we used MS DNS is mainly for ease as using Microsoft DNS means that all the domain configuration DNS entries that are needed for the Microsoft Services such as Enterprise Enrolment are created automatically as part of adding the public domain to Azure, and also we can manage the domain within the portal this also means will be only 1 entry that we need to create manually for the CMG Service, which will be a CNAME record that points to the Azure CMG Web Service URL (yourcmg.cloudapp.net) that is automatically created by the CMG service deployment to Azure.

In regard to what changes are required for the configuration for our Software Vulnerability Manager product to support CMG, well the answer to this is nothing, provided your SVM Solution is currently able to publish updates to WSUS/SCCM and is working, there are no changes that need to be made to the configuration of SVM.

*** CMG can work with an on premises SVM Server, but in order for the SVM Agent that is installed on the client machines to communicate scan results back to the on premises SVM server a VPN would be required, or alternatively use the SCCM Inventory Import Function within Software Vulnerability Manager to collect client machine software inventories.*

The Lab Environment

The Domain we have created in our mini enterprise environment, our test environment domain is a child domain of a root Enterprise Domain called “flexdev.com”, our child domain is “secunia.flexdev.com”

This domain consists of:-

svmsup-dc-01.secunia.flexdev.com	• Domain Controller • DNS • Global Catalog
svmsup-ca-01.secunia.flexdev.com	• CA Authority – secunia.flexdev.com
svmsup-sccm-01.secunia.flexdev.com	• SCCM Site Server • WSUS Server • Software Update Point • Distribution Point • Management Point etc.
svmsup-fs-01.secunia.flexdev.com	• To run Azure AD Connect

Microsoft Azure Tennant

For this lab test we also have created a tenancy in Microsoft Azure, with a subscription to Microsoft Azure AD P2 Premium.

Domain Name & DNS Records

If your domain already exists and is hosted on external DNS Servers, and not Microsoft DNS Servers you will need to configure all of the DNS records required for Enterprise Enrolment.

Please see this article: -

https://docs.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide

Once your domain DNS records are configured for Microsoft 365 services and that the domain has been set up correctly within Azure.

This article explains further the configuration to configure your domain name for Azure AD

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain#:~:text=Add%20your%20custom%20domain%20name%20to%20Azure%20AD,-After%20you%20create&text=Search%20for%20and%20select%20Azure,Select%20Add%20domain.

Once the domain is configured in Azure, the next stage is to create a synchronisation between your on-premises enterprise Active Directory and Azure AD

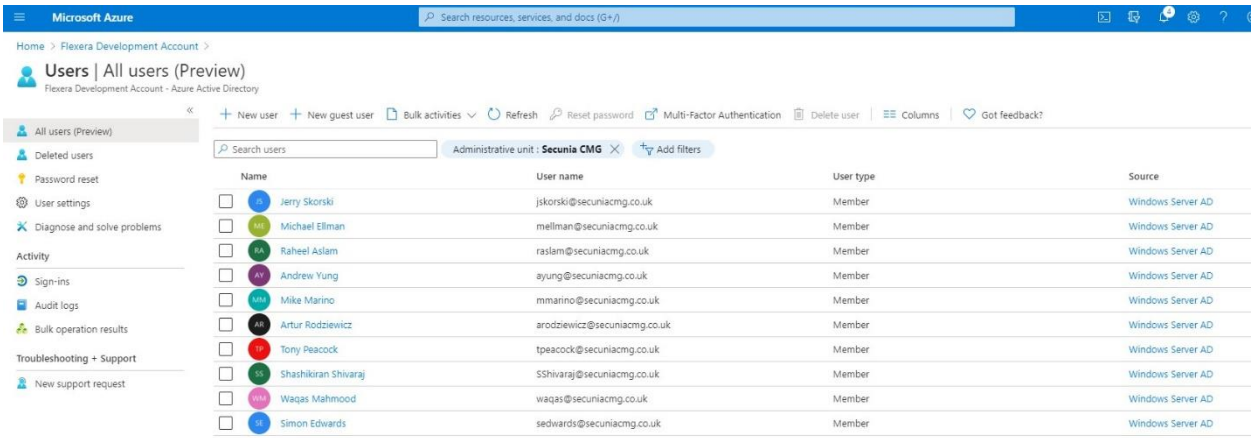
Azure AD Connect

Azure AD Connect tool creates a regular synchronisation of on premises Active Directory Objects to the Azure AD, the first stage is to install the tool on a member server, in our lab environment a server has been created specifically for this purpose, do not install AD connect on a Domain Controller as you will not be able to amend the AD Connect configuration afterwards which you will need to do later to configure Hybrid Domain joins.

The Microsoft article below explains further details for Azure AD Connect along with some “how to’s”, but for the first stage is getting the users sync’d

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect

Once you have configured AD connect and it has done its first synchronisation you will be able to see the synchronised users in the Azure Portal.



Azure AD Connect – Hybrid Domain Join

The next part is to get the machine accounts synchronised, where machine accounts are concerned they are not actually synchronised they are registered (enrolled) within Azure AD as Hybrid Joined. To configure this you will need to revisit the AD Connect configuration as per this article:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-options

Once configured and figured and sync'd (which will take some time) your devices should appear in the Azure AD as below:-

☐	SVMSUP-CLI-01	Yes	Windows	10.0.19041.388	Hybrid Azure AD joined	Simon Edwards
☐	SVMSUP-CLI-02	Yes	Windows	10.0.19041.388	Hybrid Azure AD joined	Simon Edwards
☐	SVMSUP-CLI-03	Yes	Windows	10.0.18363.836	Hybrid Azure AD joined	Artur Rodziewicz
☐	SVMSUP-CLI-04	Yes	Windows	10.0.19041.388	Hybrid Azure AD joined	N/A
☐	SVMSUP-CLI-05	Yes	Windows	10.0.19041.388	Hybrid Azure AD joined	Simon Edwards

To summarise, the Azure Active Directory and Device Hybrid Domain join must be configured correctly and in place before you configure CMG components within SCCM

PKI Pre-requisites.

All machines must have Client Authentication Certificates issued by their enterprise CA

All machines must have the Enterprise CA root certificate, and any intermediate certificates that may apply to your environment deployed to the relevant stores.

A Web Server certificate will need to be generated from the Enterprise CA which will be applied to the CMG Web Service.

https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/certificates-for-cloud-management-gateway

You can use a public certification authority for the CMG Web Service Server certificate, but in our test environment we have used our internal PKI

IMPORTANT NOTE: If you are using your internal PKI it is unlikely that your Certification Revocation Lists will be publicly available. During the setup of CMG there is a checkbox which is checked by default for Verify Certificate Revocation, this must be unticked.

Also during the CMG setup you will be asked for the Enterprise Root Certificate and any intermediate certificates that are applicable.

Azure Subscription

Within your Azure tenant, you will need to create a subscription, this article explains how to create a subscription

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription

Once the subscription is live, you will need to enable two Azure Services within resource providers, the two services that are required are Microsoft.ClassicComputer & Microsoft.Storage

This article gives you some guidance on enabling these resources.

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-providers-and-types

IMPORTANT

For the CMG to deploy successfully, the Azure user account used to create the CMG Service within SCCM must be the same user account that is the owner of the subscription, this user also needs to be a Global Administrator within Azure.

You can add additional owners to the subscription to do this, this article explains how to make changes to the subscription administrator.

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/add-change-subscription-administrator

Setup CMG

This is the main article from Microsoft for setting up Cloud Management Gateway, it does cover several of the points that I have mentioned in this document.

https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/setup-cloud-management-gateway