Cloud On-Premise installation: Summary & Prerequisites

Scott Kircher - 2021-02-11 - in Cloud

There are some things that need to be done before launching the Cloud On-Premise installer. Here is a summary of installation steps, and recommendations to make the process go smoother. Be aware of and plan for one or more PC/server reboots during the installation process.

If possible, install on a PC that is dedicated to the On-Premise product. This will avoid port conflicts between the OP components and other products, and ensure all resources can be utilized by OP, and OP isn't taking resources away from some other product.

If using Windows 10, only the Pro or Enterprise editions should be used; the Home/Standard edition of Windows 10 does not contain necessary components. Even if the OP product installs with no errors on Windows 10 Home/Standard, the product will not work correctly and Wasp will not support the OP product in that environment.

If using Windows Server, do not install on a Domain Controller. SQL Server, the Rabbit component, and IIS will expand to consume resources that will negatively impact the DC's performance.

A well run webserver should not have a commercial anti-virus (AV) package installed. The kind of Office macro viruses and mass-market trojans that AV packages are optimized for are a poor match to your Wasp web server.

What you should do is:

- Absolutely obsess over single purpose. Installing your Wasp web server on a platform already hosting other services like active directory, Database or file sharing just opens up additional avenues thru which users can upload malicious content to your site.

- Keep your server patched up with the latest security updates, and configured according to best-practices. Look at things like Microsoft's security toolkit.
- Have a separate firewall. Doesn't help you much with regards to intrusions, but it adds another layer of defense against misconfigured network services, and helps with simple DOS attacks. It also helps a lot with locking down remote management possibilities etc.
- Install a host intrusion detection system (H-IDS) on your server.

There is a lot of confusion about the terms, the words are often used in many different ways here. To be clear, what we mean by an H-IDS here is:

- a service on a computer
- which continuously check-sums all executable files on the computer
- and throws an alert whenever a executable file has been added or modified (without authorization).

Actually a good H-IDS will do a bit more than this, such as monitoring file permissions, Registry access etc, but the above gets the gist of it.

A host intrusion detection system takes some configuration, since it can give a lot of false errors if not set up properly. But once it's up and running, it will catch more intrusions than AV packages. Especially H-IDS should detect a one-of-a-kind hacker backdoor, which a commercial AV package probably will not detect.

H-IDS also lighter on the server load, but that's a secondary benefit -- the main benefit is a better detection rate.

Now, if the resources are limited; if choice is between a commercial AV package and doing nothing, then some AV products are better than nothing.

So if you must install AV software you are responsible for making sure the that the product is properly administered so that installing your new wasp server will go smoothly.

Please also make sure the platform is up to the additional load the AV software is putting on it.

1. Note: This is a requirement, not merely a recommendation. Do not use a Domain account to perform the Cloud OP installation. If necessary, create a local user, add that user to the local Administrators group (not the Users group), then log on as this new local admin. This will ensure that the software is installed in a manner that does not depend on a domain account.

2. If you will need to change the PC/server name to something else, perform the name change before starting the installation process. Consult your IT department for guidance if necessary.

3. Rather than installing on a temporary server, then moving the database to the final server, perform the installation on the Cloud OP's destination server.

Points 2 and 3 will avoid tedious and complicated reconfiguration steps.

4. Configure IIS as described in the article "Cloud On-Premise installation: IIS Settings Prerequisites" linked below in Related Pages.

5. Configure Powershell as described in the article "Cloud On-Premise installation: PowerShell permission configuration" linked below in Related Pages.

6. If you downloaded the installation file, right click on it and go to Properties. If there is a message stating that it came from a different machine and an Unblock check box, check that box and click Apply and OK before extracting. The file should be extracted somewhere else on the local drive outside of the Downloads folder. e.g. the Desktop, root of C: drive, etc. (This folder should be on a local drive (not a network location), and not in the Downloads folder.)

7. While logged into the PC/server as a local administrator, right-click setup.exe, Run as Administrator. See Notes below. If you receive an installation error, reboot the PC/server, then do this step again. If you get repeated errors, take screenshots and notes on the steps you took, and contact Wasp Tech Support.

8. After successful installation, restore your initial Powershell setting (as described in the Powershell article).

9. Configure IIS performance settings as described in the article "Cloud On-Premise: IIS Settings to improve performance" linked below in Related Pages.

10. (optional) Set user-defined sa password in SQL Studio Management Studio.

Notes:

a. If a PowerShell window appears with a Security warning, asking if you want to run certain files with .ps1 extension, type R, Enter to allow that. You may need to do this multiple times before the automated process continues.

b. The setup.exe installer is designed to recognize what components have already been installed, so it should be able to pick up where it left off, if the installation is interrupted or the PC is rebooted.

c. When browsing the site, you may get a an Internet Explorer security notification about https://kendo.cdn.telerik.com. This is the website for a third-party component used by the Cloud OP system and should be safe to add to Trusted Sites.

d. We recommend keeping the extracted installation files intact on the server in case they're needed during the course of support later.

Related Pages

- Cloud On-Premise: How to backup and restore the database
- Cloud On-Premise: Overview of what gets installed, procedures performed (Express installation type)

- Cloud On-Premise: mobile device connection troubleshooting
- Cloud On-Premise: Adding an additional binding to an IIS site
- Cloud On-Premise: After changing computer hostname, new user invitation emails are still pointing to the old PC name
- Cloud On-Premise installation: IIS Settings Prerequisites
- Cloud On-Premise: IIS Settings to improve performance
- Cloud On-Premise installation: PowerShell permission configuration
- Cloud On-Premise installation: hang/stuck on SQL Server Management Studio (SSMS) setup