



Reduce IT overhead by creating virtual environments for applications on IBM Cloud

Deploying VMware Cloud Foundation on IBM Cloud required little time and effort from an admin

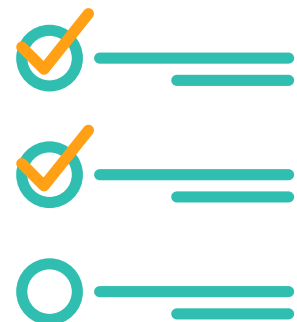
Software-defined datacenter (SDDC) solutions bring the flexibility and scalability of private and hybrid clouds to your organization. Implementing these solutions on-premises requires a knowledge of infrastructure virtualization as well as hardware deployment. Off-premises solutions eliminate the hardware requirement and shift much of the overall solution setup to the vendor.

At Principled Technologies, we looked at how an organization could implement a virtual environment on two different solutions: a VMware Cloud Foundation™ solution running on IBM® Cloud bare-metal servers and an on-premises ad-hoc infrastructure-as-a-service (IaaS) solution based on VMware® virtualization platforms. Procuring the off-premises IBM-VMware infrastructure required less hands-on time and effort from our admin. This truncated hands-on time commitment can create room in your admins' schedules to develop and execute new IT initiatives that will drive business value.

Admins spend a minute on deployment...



...and have to follow just 10 steps.



Let your workloads dictate your IBM Cloud configuration

The IBM-VMware solution we tested was one of many offerings from IBM Cloud. A range of Intel® Xeon® processors power the IBM Cloud configurations so your admins can select their desired number of cores and processors, as well as RAM, processor speed, networking speed, and internal drives based on need. In addition, admins can choose between monthly and hourly pricing options. IBM datacenters around the world feature Cloud Foundation solutions, so your admins can choose to run applications and workloads in a specific location that ensures security and compliance.

Order what you need more easily

Ordering Cloud Foundation on IBM Cloud was much easier than ordering parts for the on-premises solution. With IBM, our admin only had to select the desired configuration and spin up an instance using the web console. For any on-premises solution, it could take several hours or even days to research the required hardware and order necessary software licenses. Ordering an on-premises solution requires at least some knowledge of hardware and understanding of resource needs.

Cloud Foundation solutions require VMware-approved and certified gear, so we couldn't replicate the IBM-VMware solution by reusing older hardware.

How can solution deployment affect your organization?

Your IT admins likely have a full schedule that includes routine tasks such as updating applications and firmware and monitoring the health of servers. Although your datacenter needs new compute, storage, and networking resources for continued growth and development, adding the solutions that deliver those resources could pile onto your admin's full workload. Admins may have to delay their routine tasks, potentially affecting end-user productivity or jeopardizing your digital infrastructure. Here are some other issues to consider if you choose to deploy an SDDC or IaaS solution on-premises:

- If your admin is unfamiliar with new hardware or software, they'll be forced to learn on the fly, which could delay the deployment or routine tasks even further. And if an admin makes a mistake—watch out. That's another potential delay.
- An admin might mis-prioritize deploying a solution over performing necessary routine tasks. This can set a precedent for future scheduling conflicts.
- If an admin feels overburdened, the pressure might cause them to rush and make mistakes.
- If you're planning to run a workload in the cloud for a limited time, IT staff will have to decide how to re-purpose or reuse an on-premises solution after the workload's lifespan. Admins may have to devote more time to reconfiguring the on-premises solution.

Choosing to run an application or workload on an IBM-VMware solution, however, creates an opportunity to introduce new resources to your digital infrastructure while reducing the commitment from your admins. As IBM engineers deploy your solution, your admin can focus on monitoring the health of your other servers, updating firmware, or troubleshooting a problem in the infrastructure.

With an on-premises solution, you can't add resources with simple mouse clicks. Instead you have to ensure compatibility, procure hardware, and install all of your relevant software. This requires time from a team of people. By choosing an off-premises solution, you can skip these time-consuming steps and reduce the manpower you need to get your infrastructure running. The few following sections show some examples of how choosing to deploy a solution on-premises can present more hurdles, take longer, and require more work than choosing an off-premises IBM-VMware solution.

Compatibility

With an on-premises solution like ours, admins must spend time determining what hardware will support the virtual environment. Once they've determined compatibility with the software, they must ensure the hardware components will also work with one another. Then, they often turn their findings into a proposal before they can procure the hardware.

VMware Cloud Foundation runs on approved bare-metal hardware in IBM Cloud datacenters. So when an admin creates a plan for what to procure for an IBM-VMware solution, they need to focus only on sizing and workload considerations.

Procuring hardware

Adding or reconfiguring datacenter infrastructure requires significant planning and potentially some capital expenditure, which could require approval by IT and Accounts Payable decision-makers and take time. If your organization chooses to implement an on-premises IaaS solution like ours by using available hardware from inventory, administrators must still undertake a number of tasks to get the components into a ready state. After checking compatibility requirements, admins must locate, retrieve, and possibly reset the hardware. Even if you're looking to add to an existing infrastructure and know what you need, you still have to wait for the servers to ship and arrive at your location, which could take days or weeks.

With an off-premises IBM-VMware solution, you don't have to wait for the hardware to arrive. After getting approval to acquire the off-premises datacenter resources, your admin orders from the IBM Cloud web console as you would when you purchase something from an online retailer. Your admin can begin setting up workloads as soon as the IBM-VMware solution's ready.

Installing software

For an on-premises solution, once you've acquired hardware and made sure it's compatible with everything you're running, administrators must install updates, patches, and all software that the workloads require. Even after all the planning and procurement hassles and prerequisite software and patch installation, the admin must install and configure the cloud software. With an off-premises bare-metal IBM-VMware solution, IBM engineers handle all of those actions so your admin is free to work on other tasks.

Run applications and workloads on popular VMware virtual platforms in Cloud Foundation

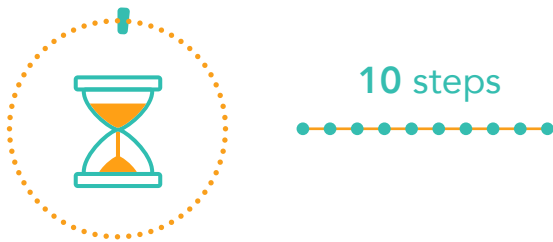
IBM Cloud has partnered with VMware to offer organizations a subscription-based SDDC solution for public clouds. Cloud Foundation on IBM Cloud combines VMware vSphere®, VMware vSAN™, and VMware NSX® to deliver virtual cloud. Organizations can benefit from seamlessly extending their private cloud to Cloud Foundation on IBM Cloud while configuring the solution to meet their specific needs.

Save time for admins deploying an off-premises solution

While we could not measure all the potential pitfalls and comparison points of planning and procurement, we did measure the steps and hands-on admin time required to complete deployment assuming a perfect and ideal case. That hands-on admin time was still much longer and more complex, requiring 269 more steps. See [Appendix B](#) for a detailed comparison between the two. Saving time procuring the solution could have a significant impact on an admin's schedule. In addition, each step in the on-premises deployment presents a possibility for error, which could lengthen the deployment.

Cloud Foundation on IBM Cloud deployment:

1 min 5 sec hands-on time



Conclusion

Creating an on-premises SDDC or IaaS solution can seem like a good idea, but deployment may require a heftier commitment from your admins than simply spinning up your workload on an IBM-VMware solution. Getting a fully functional Cloud Foundation solution on IBM Cloud required less time and effort from our admin than deploying a similar on-premises solution. If your organization is looking at cloud options, consider Cloud Foundation on IBM Cloud to ease the deployment burden on your admins.



On August 15, 2017, we finalized the hardware and software configurations we tested. Updates for current and recently released hardware and software appear often, so unavoidably these configurations may not represent the latest versions available when this report appears. For older systems, we chose configurations representative of typical purchases of those systems. We concluded hands-on testing on August 31, 2017.

Appendix A: System configuration information

On-premises solution

We deployed two of each of the servers in the following table.

Server configuration information	Dell EMC PowerEdge™ R710	Lenovo™ ThinkServer® RD530
BIOS name and version	Dell EMC 6.4.0	Lenovo 8.10
Operating system name and version/ build number	VMware ESXi™ 6.0.0 (build 3620759)	VMware ESXi 6.0.0 (build 3620759)
Date of last OS updates/patches applied	8/31/2017	8/31/2017
Processor		
Number of processors	2	2
Vendor and model	Intel Xeon processors X5670	Intel Xeon processors E5-2640
Core count (per processor)	6	6
Core frequency (GHz)	2.93	2.50
Stepping	B1	C2
Memory module(s)		
Total memory in system (GB)	96	128
Number of memory modules	6	8
Vendor and Model	Hynix HMT42GR7MFR4C-PB	Hynix HMT42GR7MFR4C-PB
Size (GB)	16	16
Type	DDR3	DDR3
Speed (MHz)	1,600	1,333
Storage controller		
Vendor and model	Intel SATA IDE Controller (ICH9)	LSI MegaRAID SAS GEN2 Controller
Local storage		
Drive #1 size (GB)	300	300
Drive #2 size (GB)	300	300
Network adapter		
Vendor and model	Intel 82599EB	Intel 82574L Gigabit
Number and type of ports	1 x 10GbE	2 x 1GbE
Vendor and model #2	QLogic® NetXtreme II Broadcom 5709C	Intel 82599EB 10-Gigabit SFI/SFP+
Number and type of ports #2	4 x 1GbE	2 x 10GbE

IBM Cloud configuration

We selected the following technical specifications to ensure an equitable comparison to the on-premises solution:

Hardware

- Standard size: Dual Intel Xeon processors E5-2690 v4 (28 cores total), 2.60 GHz, 256GB RAM
- 2 x 1TB SATA drives
- 8 x 2TB SATA drives
- 2 x 1.2TB SSD drives
- 1 x RAID disk controller
- 10 Gbps dual public and private network uplinks
- VMware Server Virtualization 6.0

Networking

- Three VLANs (one public and two private)
- Secure VMware NSX® Edge™ Services Gateway

VSIs

- One for CloudBuilder, one for Microsoft® Windows® Active Directory (AD) and Domain Name Server (DNS) services

Appendix B: Results

The table below shows the time and steps to complete the off-premises IBM-VMware solution deployment. It took our admin one minute and five seconds to procure the solution in ten steps. The remainder of the deployment did not require the admin.

VMware Cloud Foundation on IBM Cloud deployment			
Action	Admin time (hh:mm:ss)	Unattended time (hh:mm:ss)	Admin steps
Log onto IBM Cloud and place an order for Cloud Foundation	00:01:05	00:00:00	10
Deploy, configure, and clean up the solution (completed by IBM engineers)	00:00:00	12:16:07	0
TOTAL		12:17:12	10

The table below shows the time and steps to complete the on-premises solution. Our admin played the key role in all the actions. It took our admin two hours and 18 minutes in 279 steps to deploy the solution.

On-premises VMware build		
Action	Admin time (hh:mm:ss)	Steps
Prepare four bare-metal servers and install ESXi 6.0 U2	00:58:04	36
Deploy VMware vCenter Server® 6.0 Appliance	00:51:43	26
Create a datacenter in vCenter Server	00:09:48	23
Configure the VMware vSphere® Distributed Switch™ for the cluster	00:04:48	81
Enable vSAN on the server cluster	00:00:37	8
Deploy the VMware NSX® Manager™ VM	00:07:30	16
Connect NSX Manager to VMware vCenter®	00:00:54	9
Create three NSX controller nodes	00:02:39	36
Deploy high-availability NSX Edges	00:02:20	39
Deploy SpoofGuard	00:00:21	5
TOTAL	02:18:44	279

The table below breaks down the deployment time for the two solutions. For the IBM-VMware solution, hands-on time was a small fraction of what was required by the admin for the on-premises solution.

Deployment comparison				
	Admin time (hh:mm:ss)	Unattended time (hh:mm:ss)	Total time (hh:mm:ss)	Admin steps
VMware Cloud Foundation on IBM Cloud deployment	00:01:05	12:16:07	12:17:12	10
On-premises VMware build	02:18:44	00:00:00	02:18:44	279

Appendix C: How we tested

Setting up an on-premises VMware-based solution in your datacenter could require more time than our results. An admin would probably be interrupted often to research how to do things, spend time downloading software, and complete other tasks. We timed the deployment after we created this methodology, so the on-premises timings reflect a best-case scenario.

Deploying the VMware Cloud Foundation solution on IBM Cloud

Placing an order for VMware Cloud Foundations

1. Navigate to <https://console.bluemix.net>, and click Log in.
2. Enter the email address or IBMid for the account, and click Continue.
3. Enter the password, and click Log in.
4. Click Catalog.
5. Click VMware Solutions.
6. Click Cloud Foundation.
7. Click Primary for a primary site.
8. Enter a domain name, instance name, and datacenter location. Click Next.
9. Review the details and the estimated cost of the order, and click Place Order.
10. To confirm the order, click OK.

Deploying and installing the on-premises solution

We used four servers with ESXi 6.0 U2 that we'd already configured in our datacenter. These servers leveraged Active Directory/DNS services and NFS storage.

Installing ESXi 6.0 U2

1. Attach the installation media.
2. Boot the server.
3. At the VMware Installer screen, press Enter.
4. At the EULA screen, press F11 to Accept and Continue.
5. Under Storage Devices, select the appropriate disk, and press Enter.
6. Select US as the keyboard layout, and press Enter.
7. Enter the root password twice, and press Enter.
8. To start installation, press F11.
9. To reboot the server, press Enter.
10. Complete steps 1 through 9 for the three remaining servers.

Deploying vCenter Server 6.0 Appliance

1. Insert the installation media.
2. Navigate to the appropriate folder for the OS being used, and install the vcsa installation client.
3. In the main folder, open the link to vcsa-setup.html.
4. Click Install.
5. Accept the EULA, and click Next.
6. Enter the FQDN or IP of the target server, root, the password, and click Next.
7. Click Yes.
8. Enter a name for the appliance, an OS password, confirm the OS password, and click Next.
9. Select Install Platform Services Controller, and click Next.
10. Select Create a new SSO domain.
11. Enter a vCenter SSO password, and confirm the password.
12. Enter an SSO Domain name, an SSO Site name, and click Next.
13. Select the appliance size, and click Next.
14. Select a datastore, check to enable Thin Disk Mode, and click Next.
15. Select Use an embedded database (PostgreSQL), and click Next.
16. Enter a network address, system name, subnet mask, gateway, and DNS server(s).
17. Configure time sync by entering NTP server(s), enable SSH, and click Next.
18. Click Finish.

19. After the deployment completes, repeat steps 3 through 8 using the same server information.
20. Select Install vCenter Server, and click Next.
21. Enter the Platform Services Controller FQDN or IP address, the SSO password, and click Next.
22. For the vCenter Server deployment, repeat steps 13 through 18. Use a different network address and system name for the vCenter Server.

Creating a datacenter in vCenter Server

1. Open a web browser, and navigate to the vCenter Server.
2. Enter the user name and password, and click Log in.
3. Click Create Datacenter.
4. Enter a name for the new datacenter, and click OK.
5. Select the new datacenter, and click Create a cluster.
6. Enter a name for the new cluster, and click OK.
7. Select the new cluster, and click Add a host.
8. Enter the host name or IP address of the server to add, and click Next.
9. Enter the credentials, and click Next.
10. Review the host summary, and click Next.
11. Review the summary, and click Finish.
12. For each host, repeat steps 7 through 11.
13. Select the datacenter, and click Add a datastore.
14. Click Next.
15. Select NFS, and click Next.
16. Select NFS 3, and click Next.
17. Name the datastore, enter the folder path, enter the server information, and click Next.
18. Select the hosts that can access the datastore, and click Next.
19. Review the summary, and click Finish.
20. Right-click the cluster, and select New Resource Pool.
21. Name the pool `Compute` and select the maximum compute reservation. Click OK.
22. Right-click the cluster, and select New Resource Pool.
23. Name the pool `Memory` and select the maximum memory reservation. Click OK.

Configuring the VMware vSphere Distributed Switch for the cluster

1. In the vSphere Web Client, navigate to Inventory→Networking.
2. Expand vCenter for the cluster.
3. Right-click the datacenter. Under Distributed Switch, click New Distributed Switch.
4. Enter a name for the vDS, and click Next.
5. Click Next.
6. Set the number of uplinks to two, and enter a vSAN as the new default port group name.
7. Review the settings, and click Finish.
8. Right-click the new vDS, and under settings, click Edit Settings.
9. Under Properties, click Advanced.
10. For the MTU setting, type 9000.
11. Click OK.
12. Right-click the new vSAN port group that you created along with the new vDS.
13. Click Edit Settings.
14. Click VLAN, and enter the VLAN for vSAN traffic.
15. Click OK.
16. Right-click the vDS, and click Distributed Port Group→New Distributed Port Group.
17. Type `VMotion` as the name of the new port group.
18. Under VLAN, set a VLAN for vMotion. Click Next.
19. Review the port group settings, and click Finish.
20. Right-click the vDS, and click Distributed Port Group→New Distributed Port Group.
21. Type `VM_NET` as the name of the new port group, and click Next.
22. Under VLAN, set a VLAN to for VM_NET. Click Next.
23. Review the port group settings, and click Finish.
24. Right-click the vDS, and click Add and Manage Hosts....

25. Select Add hosts, and click Next.
26. Click +New hosts....
27. Select all the compatible hosts in vCenter cluster, and click OK.
28. Click Next.
29. Select Manage physical adapters and Manage VMkernel adapters, and click Next.
30. For each host, select each of the two 10Gb ports, click Assign uplink, and assign them to the two uplink ports.
31. Click Next.
32. Select the first host, and click +New adapter.
33. Click an existing network, and click Browse.
34. Select the vMotion port group, and click OK.
35. Click Next.
36. To enable the vMotion service, check the appropriate box, and click Next.
37. Enter the desired network information for the new VMKernel, and click Next.
38. Click OK.
39. Select the first host, and click +New adapter.
40. Click select an existing network, and click Browse.
41. Select the VSAN port group, and click OK. Click Next.
42. To enable the VSAN server, check it, and click Next.
43. Enter the desired network information for the new VMKernel, and click Next. Click OK.
44. Select each of the remaining hosts individually. Complete steps 33 through 44 for the three remaining servers.
45. Analyze the impact, and click Next.
46. Review the settings, and click Next.

Enabling vSAN on server cluster

1. Log into the vCenter web client, and navigate to Hosts and Clusters.
2. Expand the primary site management vCenter, and select the cluster.
3. Select the Manage tab. Under Virtual SAN, click General.
4. Click Configure.
5. At the vSAN capabilities screen, click Next.
6. At the Network validation screen, click Next.
7. Select which disks should be claimed for cache and which for capacity in the vSAN cluster, and click Next.
8. At the Ready to complete screen, click Finish.

Deploying the NSX Manager VM

1. From the vCenter Server web client, right-click the datacenter, and select Deploy OVF Template.
2. To locate the OVF or OVA file, click Browse.
3. After locating and selecting the file, click Next.
4. Accept the extra configuration options, review the details, and click Next.
5. Accept the EULA, and click Next.
6. Enter a name for the VM, select the location, and click Next.
7. Select the resource pool, and click Next.
8. Select the storage location.
9. Select Thin Provision, and click Next.
10. Select the created port group and click Next.
11. Enter a CLI "admin" user password, and confirm the password.
12. Enter a CLI Privilege mode password, and confirm the password.
13. Enter a hostname for the VM.
14. Enter any desired network information, or leave blank for DHCP.
15. Enter the DNS and NTP server IP information, and click Next.
16. Review the summary, and click Finish.

Connecting NSX Manager to vCenter

1. In the vSphere Web Client, power on the NSX Management VM.
2. Click the Summary tab, and wait for the OS to finish booting.
3. Navigate to the IP listed on the summary tab.

4. Log in using `admin` and the password you set during configuration.
5. Select Manage.
6. Under components, select NSX Management Service.
7. Next to vCenter Service, click Edit.
8. On the vCenter Server window, enter the vCenter Server, vCenter User Name, and Password and click OK.
9. When asked to agree to trust the certificate, click Yes.

Creating NSX controller nodes

1. Log into vCenter.
2. At the home screen, navigate to Networking & Security.
3. On the left pane, click Installation.
4. In the Management tab, under NSX Controller Nodes, click Add Controller.
5. Enter a name for the node.
6. Select the NSX Manager.
7. Select the Datacenter.
8. Select the Cluster/Resource Pool.
9. Select the Datastore.
10. Select the Host.
11. Select the IP Pool.
12. Enter and confirm the password. Click OK.
13. Complete steps 1 through 12 two more times.

Deploying high-availability NSX Edges

1. Log into vCenter
2. In the home screen, navigate to Networking & Security
3. On the left pane, click NSX Edges.
4. Click Add NSX Edges.
5. In the New NSX Edge Window, enter a name for the Edge. Click Enable High Availability, and click Next.
6. On the settings screen, enter the password. Click Enable SSH access, and click Next.
7. For Datacenter, select vCF Test. Click Add NSX Edge Appliance.
8. Select a Cluster/Resource Pool.
9. Select a datastore and click OK.
10. Click Next.
11. Click Add NSX Edge Interface.
12. Enter a name.
13. For Connected To:, click Select.
14. In the Connect NSX Edge to a Network window, click Distributed Portgroup.
15. Select a Distributed Port Group. Click OK.
16. Click Add Primary IP Address.
17. Enter the Primary IP Address Information and Subnet Prefix Length.
18. Click OK.
19. Repeat steps 11 through 18 for the remaining two interfaces.
20. Click Next.
21. Enter the Gate IP, and click Next.
22. Click Configure Firewall default Policy.
23. For Default Traffic Policy, click Accept.
24. For Logging, click Enable, and click Next.

Deploying SpoofGuard

1. Log into vCenter.
2. In the home screen, navigate to Networking & Security.
3. On the left pane, click SpoofGuard.
4. Enter a name for the policy, and click Next.
5. To add the four port groups, click Add, and click Finish.

This project was commissioned by IBM.



Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.

DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:

Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.