

Migrating an on premises VM to the Public Cloud:

Start by installing your preferred migration tool into the VMWare environment. In our case, after evaluating several products, we opted to use Boomerang. But before you do anything else, read the list below.

Step	Task Description
PRE-MIGRATION CHECKS	
1	Identify the type of Application (Web, App or DB), and preferably any interdependencies, network and security constraints. We recommend running vRealize Infrastructure Navigator (VIN) to help identify application interconnects.
2	Determine any special license requirements for applications. Are they going to work in your target location? Some public clouds don't support BYOL so check if you are running a license server on this VM that is bound to a MAC address or other hardware identifier that must necessarily change.
3	Identify application & system owners. You will need to engage with these people, ensure they are readily available to assist.
4	Is the application supported by a Vendor? Are support arrangements in place with vendor for any post migration troubleshooting? Are internal support teams ready?
5	Capture System Services & Sysinfo. You will want this information later should something go awry.
6	Capture any persistent and non-persistent route information from Windows & Linux Servers
7	Check firewall rules & routes to on premises & external networks are in place/configured correctly to ensure there is a clear route from your intended host location back to anything it needs to access (especially on-premises networks / VLANs)
8	Schedule the change. Ensure a proper communication / notification process is applied to notify all stakeholders involved. Note that Dev / Test workloads may not require stringent change control, but changes to underlying hosts / networks may.
9	Pre-migration Application Verification: - Make sure the application works before migration activity. Make sure that verification procedures / checklists exist. - Reboot VM & check for any OS type errors. Often a reboot exposes errors that may not have been previously noted. Migration will involve the system rebooting a number of times, so ensure this is not an issue. - Make sure the instance / VM still works after the reboot.
10	As the IP address will likely change (*unless a stretched Layer 2 network is implemented), you may need to update the DNS records – check and document
11	Check that resources are available for application to function in target location – you may need to migrate other resources at the same time. E.g. does the Server talk to any guest initiated storage present at the guest OS.
12	Check whether your technical resources have full access to the 'cloud console' for troubleshooting purposes. Application teams may require some access as well.
13	Target state for the cloud instance must have been identified prior to migration (e.g. VPC, subnet ids, security groups, EIPs, Tags.) Know what your end state looks like prior to migration.
14	Best practice is to perform a Backup (prior to migration)
15	Select an IAM key pair for EC2. Ensure your tech resources have access to that key pair - always – in case they need to access the EC2 instance later. Otherwise you may create a data rich "brick".
MIGRATION	
16	Launch the Boomerang portal and create new Protection Group (PG). - Choose the correct credential profile created - Input a meaningful name to the PG - Define the replication setting backup retention period, depending on how often you want the replication to run (i.e. forever or delete after X days). Select desired VMs to be included in this protection group. (Note: If you have a lot of VMs, you can switch to Folder View to find the VMs you want more easily).
17	Replicating a Protection Group happens according to the schedule you provide, but you can also trigger it manually by clicking "replicate now".
18	Deploy the replica in the S3 into instances or AMI in EC2 Select the latest snapshot and choose the correct VPC. Select spin up as EC2 running Instances or Convert to Amazon Machine images (AMI) to spin up later. We converted the VM's to AMI's in our case. Record the AMI ID and/or EC2 ID.
POST CHECKS	
19	Validate the cloud instance launches successfully.
20	Validate you can connect to the cloud instance via RDP / SSH
21	Test the OS for any errors (Event Viewer / /var/log/messages)
22	Post migration Application Verification (Log & track any issues identified)
23	Sign-off application verification test with Application owner.
24	Remove VMWare tools from the VM. You won't require these anymore.
25	Remove Backup agents (assuming you have a different solution for cloud backups).

- | | |
|----|---|
| 26 | Setup new cloud backup (e.g. Actifio or similar). You still require backups in the cloud, but your solution may well be different to your on premises solution (agentless backup solutions are usually the norm in Cloud). |
| 27 | Check server monitoring. (Alternatively, ensure Cloudwatch monitoring is enabled) |
| 28 | Once you're satisfied the EC2 instance is running as expected, delete the AMI image as you will incur charges for these (you may choose to wait a period of time before doing this to ensure the application is stable). |
| 28 | As above, once the instance is running in a stable fashion, delete the S3 objects as you will incur charges for these as well. |
| 30 | Delete the old VM in your vSphere environment as you don't want the VM accidentally restarting. You may consider renaming it or moving it in a way that makes it obvious that it has been migrated to Cloud for a short period of time so you can recover it if required. |