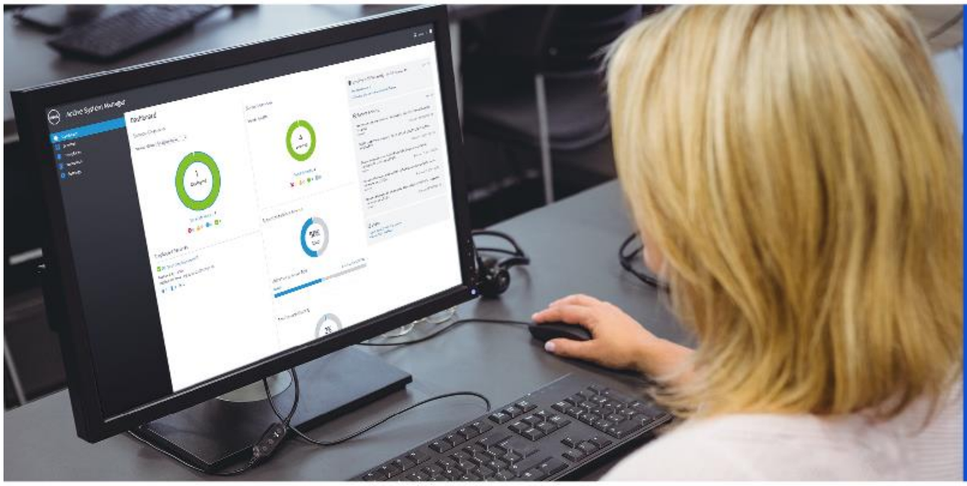
MANAGE INFRASTRUCTURE AND DEPLOY SERVICES WITH EASE USING DELL ACTIVE SYSTEM MANAGER

SIMPLIFY DEPLOYMENT, SAVE TIME

Dell Active System Manager



FASTER & MORE EFFICIENT
80% faster, with 71% fewer steps

EASIER TO USE
Wizard-driven approach for any level of IT experience

REDUCED COMPLEXITY
Template-based automation and pre-built templates

vs. Cisco® solution

Automated systems management solutions can free up administrators to innovate in the datacenter rather than tie them up with routine management tasks.

A systems administrator has plenty to worry about when keeping an organization’s infrastructure running efficiently. The right tools can make infrastructure deployment and configuration simpler and faster.

With its intuitive, wizard-driven automation, we found that Dell Active System Manager (ASM) was easier to use than a Cisco UCS® solution, and required less time and effort to deploy enterprise solutions. With Dell ASM, gone are the days of manually scripting every aspect of your own deployment tasks. Dell ASM contains wizards that guided us through deploying a ready-to-host VMware® vSphere® cluster, including the process of discovering hardware, defining networks, configuring resources, and deploying services.

Once we configured our environment, Dell ASM let us deploy a new service in just ten steps. We found deploying the equivalent service with Cisco UCS Director was more difficult because it required extensive experience with its workflow designer. Dell ASM makes routine deployment tasks easier and gives administrators more time to focus on innovation, bringing real value to the datacenter.

APRIL 2015
A PRINCIPLED TECHNOLOGIES TEST REPORT
Commissioned by Dell Inc.

DELL ASM AUTOMATES TASKS TO FREE UP ADMINISTRATORS

Organizations want to get new hardware up and running with services deployed as quickly as possible. With ASM automation, not only do your customers benefit from quick service delivery, administrators can spend less time completing routine tasks and more time innovating elsewhere in the datacenter.

Dell ASM is infrastructure and workload automation software that provides a single interface for managing infrastructure hardware and automating service deployments. This unified, converged approach can cut down on time wasted with different consoles when you discover, deploy, update, or repair your hardware. Dell ASM uses intuitive wizards to guide you every step of the way with valuable features:

- Simple resource discovery and fast onboarding, which enables you to go from an open box to a running service in a small amount of time
- Template-based provisioning, which easily defines IT services and comprehensive infrastructure requirements
- Service lifecycle management, which enables infrastructure scaling, updating, and compliance tracking

To learn more about Dell ASM, visit www.dell.com/asm.

LESS TIME, FEWER STEPS, MORE INTUITIVE

In our hands-on tests, we found we could install Dell ASM and deploy a ready-to-host VMware vSphere cluster in 15 minutes and 57 seconds of administrator time. That's 80 percent[1] less time than the Cisco solution, which took 1 hour, 19 minutes, and 5 seconds of administrator time (see Figure 1).

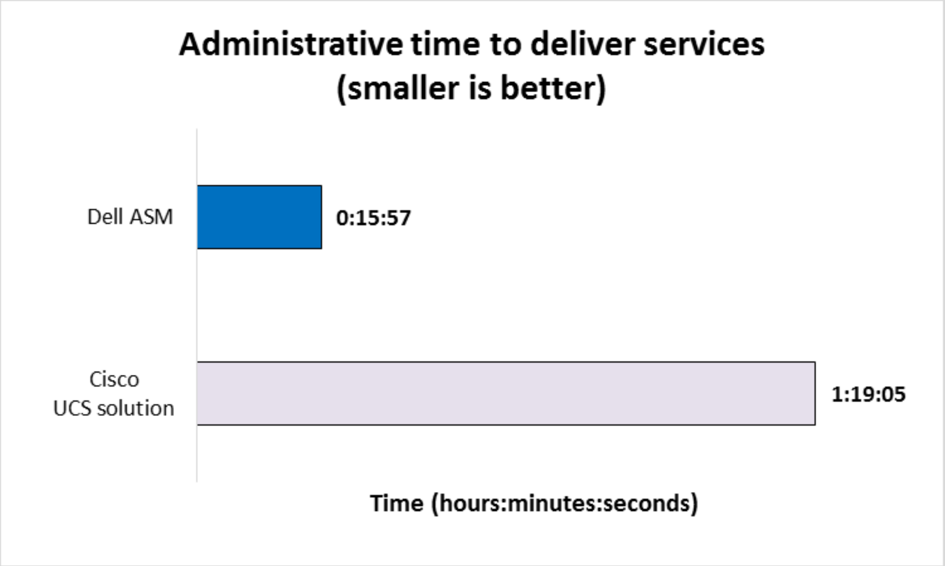


Figure 1: Dell ASM simplified the cluster deployment process to save 80 percent of hands-on administrator time compared to Cisco solution.

[1] Rounded from calculated 79.8%.

For Cisco UCS, the total administrative time included the time to build the execution wizard in UCS Director from a documented procedure, but not the actual development and testing time required to design that procedure. Building your own wizard with the Cisco solution requires in-depth knowledge of Cisco UCS service profiles, hardware components, and add-in components necessary to perform bare-metal deployments. Due to errors, resets, and restarts, your administrators could need substantially more time to create a properly functioning wizard and get repeatable results.

The easy-to-use interface of Dell ASM reduced complexity when deploying a ready-to-deliver-services cluster compared to the Cisco solution. It reduced the necessary manual steps by 315 – a 71 percent[2] reduction, which can speed up the process, reduce chances of delays related to human error, and let administrators move on to the next important task.

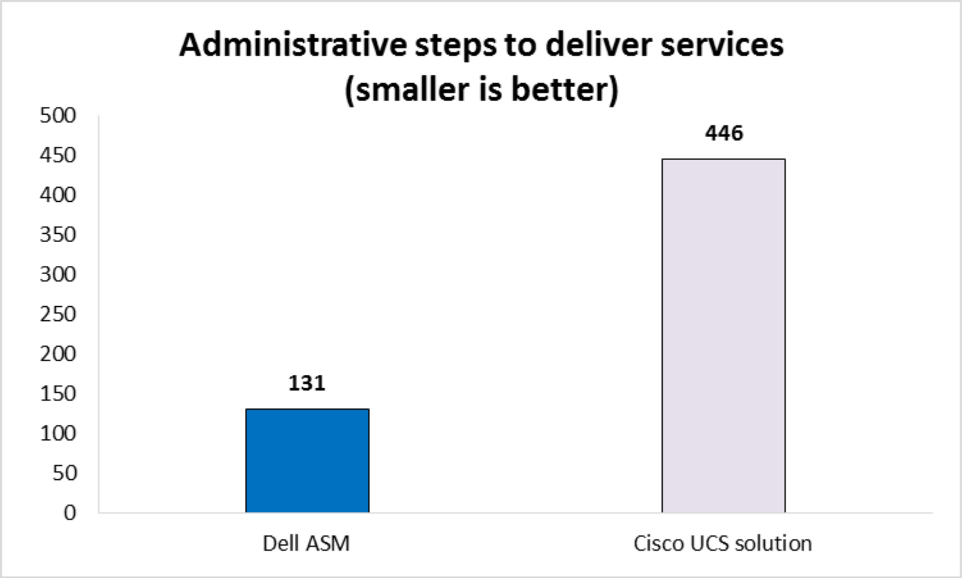


Figure 2: Dell ASM cut the number of steps to deploy a cluster and deliver services by 315 steps compared to the Cisco solution.

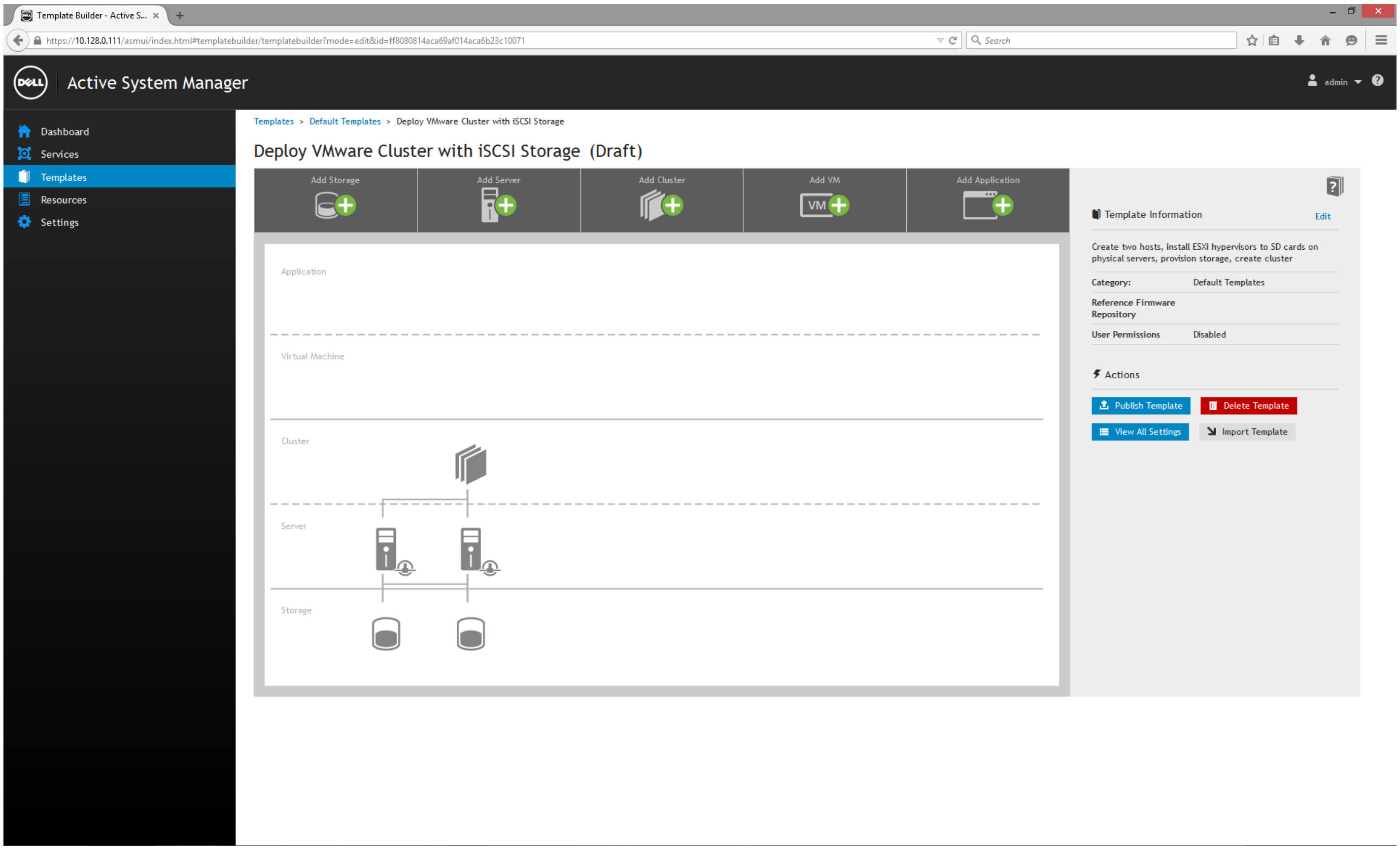
A look inside the tools

For starters, Dell ASM let us do everything to deploy a ready-to-host vSphere cluster (see Appendix A for hardware details) from a single interface. We found that the best approach with Cisco UCS required using both Cisco UCS Manager and UCS Director.[3]

When it comes to user experience, the most noticeable difference between Dell ASM and the Cisco UCS solution is in the template creation process. Dell ASM includes

[2] Rounded from calculated 70.6%.
[3] http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-manager/whitepaper_c11-697337.html

15 service templates to help administrators get started with designing services, and its template editor (see Figure 3) creates a clear hierarchy for adding physical and virtual components to a deployment. From the Dell ASM template editor, you can easily add storage, compute nodes, VMs, clusters, operating systems, and applications to a service template. In addition, administrators can deploy bare-metal operating systems or a complete Microsoft® SQL Server® 2012 instance right out of the box. Administrators can publish templates in a matter of clicks from the Templates tab, and monitor health status and availability from the Dell ASM Dashboard.



https://10.128.0.111/asmui/index.html#templatebuilder/templatebuilder?mode=edit&id=ff8080814aca69af014aca6b23c10071

Templates > Default Templates > Deploy VMware Cluster with iSCSI Storage

Deploy VMware Cluster with iSCSI Storage (Draft)

Template Information

Create two hosts, install ESXi hypervisors to SD cards on physical servers, provision storage, create cluster

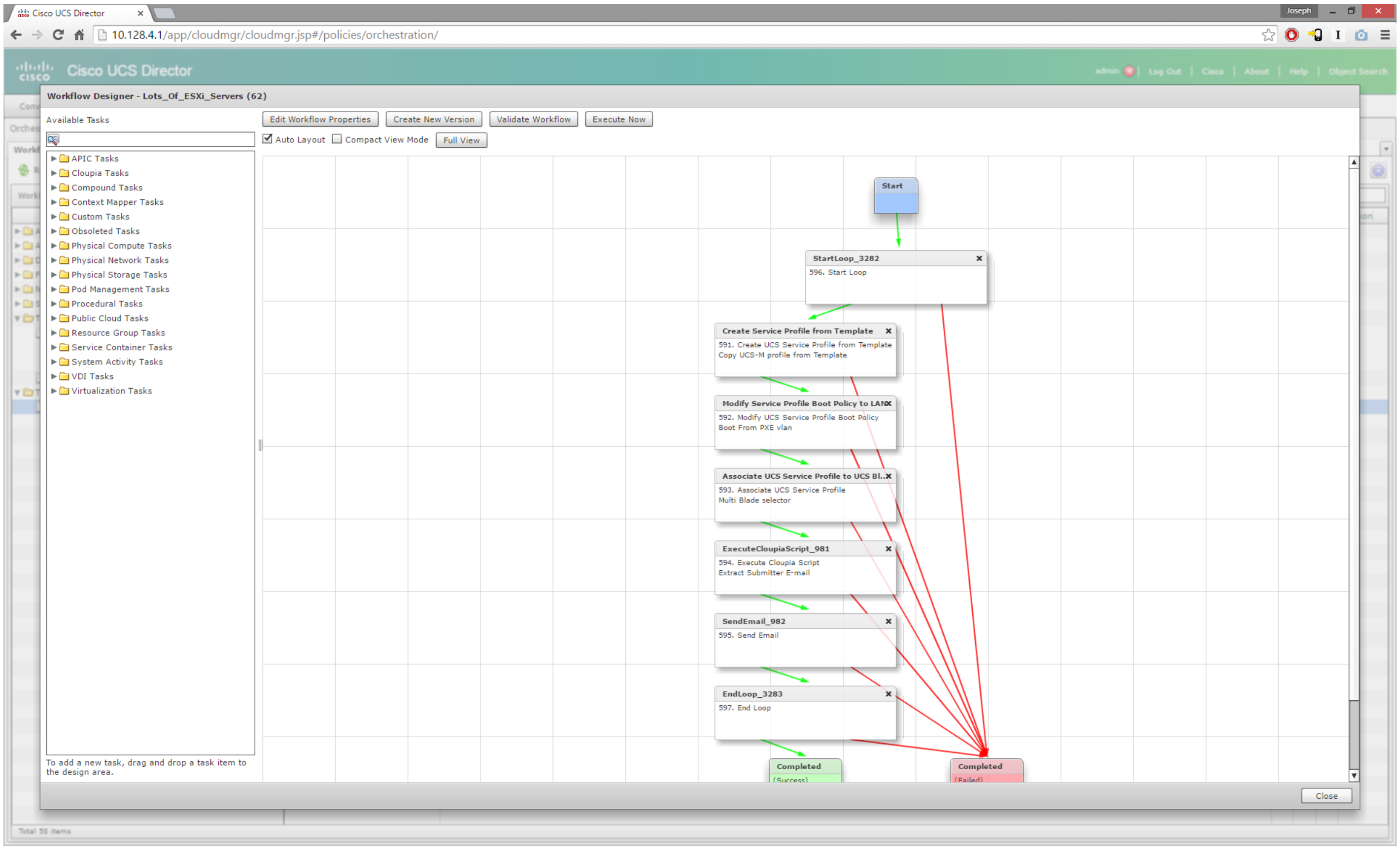
Category:	Default Templates
Reference Firmware Repository	
User Permissions	Disabled

Figure 3: Creating and editing a template with the template editor in Dell ASM.

Creating similar services in UCS Director proved to be more difficult than using the template editor in Dell ASM. UCS Director's automation capabilities rely on creating workflows in the workflow designer (see Figure 4). Before you can use a wizard in UCS Director, you must use the workflow designer to custom-build a service wizard from scratch. We found that because Cisco UCS Director provided only five workflow templates, designing a workflow for a simple service, such as deploying a vSphere cluster with iSCSI storage, required researching community workflows and developing our own workflow template to align with our environment. The actual process of modifying workflows and adding tasks required an understanding of workflow user inputs and outputs.

The template editor in Dell ASM simplified the individual configuration of virtual and physical components. While ASM logged every step in the process, we did not have to design the process needed to deploy a service in order to automate it.

Cisco UCS Director, on the other hand, required us to understand the details of the entire process, and add every necessary step. Cisco UCS enumerates every task so that later steps can refer back to the output from previously executed tasks, but this can be difficult to manage when adding workflow components out of the normal workflow order. For example, when the wizard generates an error due to a missing but necessary step, you must add the step and reference it out of sequence in the workflow.



To add a new task, drag and drop a task item to the design area.

Figure 4: Creating and editing a workflow with the workflow designer in Cisco UCS Director.

During our testing, our administrators required several business days to create and document a wizard-driven workflow that produced repeatable results for just a single service with Cisco UCS Director. Dell ASM's templates are ready to use, so you can skip the time-consuming process of building a workflow that Cisco UCS requires. If creating a wizard in UCS Director required two days per service, using Dell ASM to deploy the same services could save a month of development time, which administrators could use on more strategic tasks.

SAVE TIME AND MONEY

Managing your IT environment can be costly. IT budgets aren't expanding as rapidly as user demand and expectations are. A comprehensive, intuitive tool that lets IT deliver services rapidly and simplify datacenter management might seem like it would break the bank, but our analysis showed otherwise.

The simplicity of Dell ASM means that technicians of any level can use it, while the Cisco solution requires administrators to have extensive expertise with a variety of technologies and infrastructure components. With Dell ASM, your existing IT administrators can take advantage of infrastructure automation without expensive additional training or expensive additions to the staff.

Dell ASM also offers big savings in licensing costs (see Figure 5). Based on the list/MSRP costs for each solution, Dell ASM offers data center automation features for only $165 per node,[4] 95 percent less per node than the Cisco solution, which costs $4,000 per node.[5]

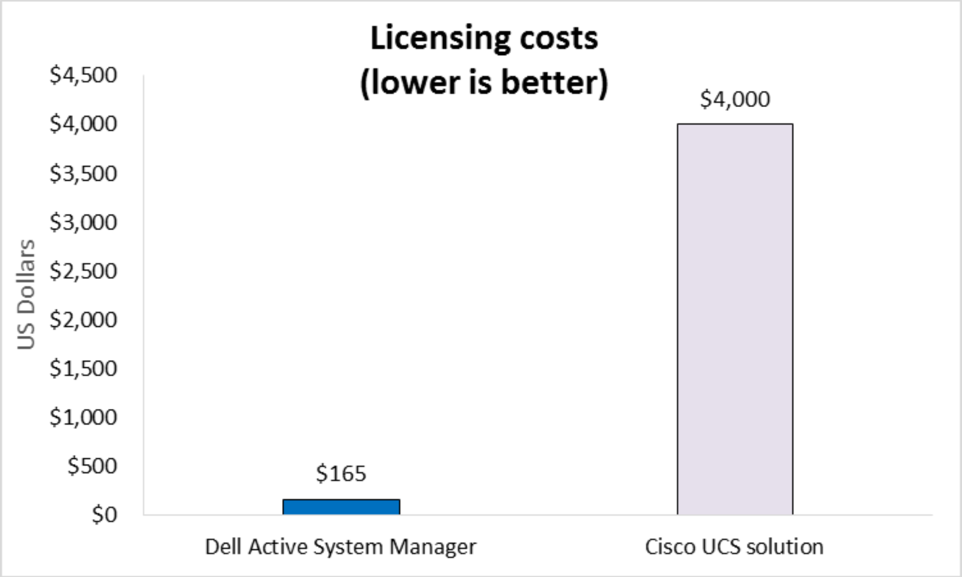


Figure 5: The license for a single instance of Dell ASM cost 95 percent less compared to the Cisco solution.

[4] http://en.community.dell.com/techcenter/converged-infrastructure/w/wiki/7725.asm-8-0-new-pricing, 4/15/15

[5] https://apps.cisco.com/Commerce/guest , 4/15/2015

CONCLUSION

There are better ways to use your time in the datacenter than going through the tedious process of deploying infrastructure and applications with a solution that requires unnecessary hands-on time. By automating many processes and using a friendly, intuitive wizard, we found that Dell ASM simplified the process of setting up a cluster to deliver IT services.

It took 80 percent less time and 71 percent fewer steps to get our services up and running, compared to doing the same thing with a Cisco solution including UCS Director and UCS Manager. Not only did Dell ASM have a VMware vSphere cluster up and running more easily and in less time, it cost less to license than the Cisco solution. With superior ease of use and 95 percent lower licensing costs, Dell ASM can make life easier for administrators while freeing them up for strategic tasks, saving you time and money for more efficient management of your datacenter.

APPENDIX A – SYSTEM CONFIGURATION INFORMATION

Figures 6 through 9 provide detailed configuration information for the hardware we used in our tests.

System	Dell PowerEdge M1000e blade enclosure
Power supplies	
Number of power supplies	6
Vendor and model number	Dell E2700P-00
Wattage of each (W)	2,700
Cooling fans	
Total number of fan modules	9
Vendor and model number	Dell X46YM Rev. A00
Volts	12
Amps	5
Midplane	
Chassis midplane	1.1
Chassis firmware	
Chassis Management Controller firmware	4.31
iKVM firmware and hardware	01.00.01.01 A03
IOM firmware	11
IOM software	8.3.17.2
I/O modules	
Switch	Dell Force10 MXL 10/40GbE
Occupied bay	A1, A2
Management modules	
Chassis Management Controller slot 1	Chassis Management Controller Hardware
iKVM slot	Avocent iKVM Switch (0K036D)
Chassis Management Controller slot 2	Chassis Management Controller Hardware

Figure 6: Configuration information for the Dell blade server chassis.

System	Dell PowerEdge M620 blade server
Enclosure	
Blade enclosure	Dell PowerEdge M1000e
General	
Number of processor packages	2
Number of cores per processor	6
Number of hardware threads per core	2
System power management policy	Default
CPU	
Vendor	Intel
Name	Xeon
Model number	E5-2640
Stepping	C2
Socket type	FCLGA2011
Core frequency (GHz)	2.5
Bus frequency (GHz)	3.6
L1 cache	32KB + 32KB (per core)
L2 cache	256 KB (per core)
L3 cache	15 MB
Platform	
Vendor and model number	Dell PowerEdge M620
Motherboard model number	0VHRN7A03
BIOS version	1.6.0
BIOS settings	Default
Memory module(s)	
Total RAM in system (GB)	32
Vendor and model number	Micron MT18KSF51272PDZ
Type	PC3L-10600R
Speed (MHz)	1,333
Speed running in the system (MHz)	1,333
Size (GB)	4
Number of RAM module(s)	8
Chip organization	Double-sided
Rank	Dual
RAID controller	
Vendor and model number	Dell PERC S110 Embedded
Firmware version	3.0.0-0139
Cache size (MB)	0
Ethernet adapters	
Vendor and model number	Broadcom® BCM57810 NetXtreme® II 10 GigE
Type	LOM

System	Dell PowerEdge M620 blade server
USB ports	
Number	2 external
Type	2.0
Firmware	
Integrated Dell Remote Access Controller	1.40.40
Broadcom NetXtreme II 10 Gb Ethernet BCM57810	7.4.8
BIOS	1.6.0
Lifecycle Controller, 1.1.5.165, A00	1.1.5.165
Enterprise UEFI Diagnostics	4217A4
OS Drivers Pack	7.2.1.4 7.2.1.4
System CPLD	1.0.2
PERC H310 Mini	3.0.0-0139

Figure 7: Configuration information for the Dell blade server we used in our tests.

System	Cisco UCS 5108 blade server chassis
Power supplies	
Number of power supplies	4
Vendor and model number	Cisco Systems Inc. N20-PAC5-2500W
Wattage of each (W)	2,500
Cooling fans	
Total number of fan modules	8
Vendor and model number	Cisco Systems Inc. N20-FAN5
Chassis firmware	
Board Controller	11.0
CIMC Controller	2.2(1d)
IOM firmware	2.2(1d)
I/O modules	
Switch	Cisco UCS 2208XP
Occupied bay	1, 2

Figure 8: Configuration information for the Cisco blade server chassis.

System	Cisco UCS B200 M3 blade server
Enclosure	
Blade enclosure	Cisco UCS 5108
General	
Number of processor packages	2
Number of cores per processor	10
Number of hardware threads per core	2
System power management policy	Default

System	Cisco UCS B200 M3 blade server
CPU	
Vendor	Intel
Name	Xeon
Model number	E5-2680 v2
Stepping	M1
Socket type	FCLGA2011
Core frequency (GHz)	2.8
Bus frequency (GHz)	4
8	10 x 32 KB instruction caches, 10 x 32 KB data caches
L2 cache	10 x 256 KB
L3 cache	25 MB
Platform	
Vendor and model number	Cisco UCS B200 M3
Motherboard model number	UCSB-B200-M3
BIOS version	B200M3.2.2.1a.0.111220131105
Memory module(s)	
Total RAM in system (GB)	384
Vendor and model number	SK Hynix HMT42GR7AFR4C-RD
Type	PC3-14900R
Speed (MHz)	1,866
Speed running in the system (MHz)	1,866
Size (GB)	16
Number of RAM module(s)	24
Chip organization	Double-sided
Rank	Dual
RAID controller	
Vendor and model number	LSI MegaRAID SAS 2004 ROMB RB2
Firmware version	20.11.1-0135
Cache size (MB)	0
Firmware	
CIMC	1.40.40
Board Controller	2.2(1d)
BIOS	B200M3.2.2.1a.0.111.220131105
Cisco UCS VIC 1240	2.2(1d)

Figure 9: Configuration information for the Cisco blade servers we used in our tests.

APPENDIX B – HOW WE TESTED

Deploying the Dell ASM Appliance

Deploying the ASM OVF Appliance

1. Before testing, extract the Dell ASM zip file (Dell-ActiveSystemManager-8.0.0-3233_VMware.zip) to a location accessible by VMware vSphere Client.
2. Simultaneously start the timer and open vSphere Client, and connect to the vCenter server that will host the Dell ASM appliance.
3. In vSphere Client, click File, and Deploy OVF Template. The Deploy OVF Template wizard will open.
4. On the Source page, click Browse, and select the OVF package.
5. Click Next.
6. To continue, click Next.
7. Accept the License Agreement, and click Next.
8. Enter a name (Active System Manager), and select the Inventory Location.
9. Click Next.
10. Assuming a resource pool has been configured, select the storage volume to host the appliance virtual machine. For our tests, we used an EqualLogic array.
11. To continue, click Next.
12. On the Disk Format page, select Thin Provision.
13. Click Next.
14. Verify the Destination Network for Network 1 is set to the management VLAN (mgmt vlan128).
15. Click Next.
16. Click Finish, and stop the timer.

Configuring VM network adapter

1. Simultaneously start the timer and select the newly created VM (Active System Manager) from the host.
2. In the Getting Started subtab, click Edit virtual machine settings.
3. Select Network adapter 1.
4. Verify the Network label is set to the management network (management vlan128).
5. Click Add…
6. Select Ethernet Adapter, and click Next.
7. Under the Network Connection section, select the PXE network label (PXE vlan1076).
8. Click Next.
9. Click Finish.
10. Click OK. Stop the timer when the Recent Tasks list reports that Reconfiguring virtual machine has completed.

Adding appliance network definitions

1. In the vSphere Client, simultaneously start the timer and right-click the Active System Manager virtual machine, and select Power On.
2. Click the Console tab.
3. Log in with the default ASM credentials (delladmin, delladmin).
4. Type `sudo su –`, and then press enter.

5. Type the current admin password (delladmin), and press enter.
6. Accept the License Agreement, and click Forward.
7. Click Network Configuration.
8. Select Auto eth0, and click Edit.
9. Change the connection name to management-0.
10. Select the IPv4 Settings tab.
11. Change Method to Manual.
12. Click Add, and click the text field to enter the IPv4 address, the Netmask, and the Gateway (for our management network, we used 10.128.0.111, 255.255.0.0, and 10.128.0.1).
13. Enter 10.128.0.10 as the DNS Servers.
14. Click Apply…
15. Select Auto eth1, and click Edit.
16. Change the connection name to PXE-1.
17. Select the IPv4 Settings tab.
18. Change Method to Manual.
19. Click Add, and click the text field to enter the IPv4 address, the Netmask, and the Gateway (for our PXE network, we used 192.168.76.1, 255.255.255.0, and 0.0.0.0).
20. Click Apply…
21. Click Close.
22. Click Close again, and stop the timer.

Using the initial setup wizard

1. Simultaneously start the timer and open a browser from the workstation, and navigate to the ASM appliance IP (10.128.0.111).
2. Log in with the default credentials (admin, admin).
3. At the welcome screen, click Initial Setup.
4. Click Next.
5. Click Choose File, navigate to the license file location, and upload the license file.
6. Click Save and Continue.
7. Set the Time Zone ((UT-05:00) Eastern Time (US & Canada)), and Preferred NTP Server.
8. Click Save and Continue.
9. Leave Use a proxy server unchecked, and click Save and Continue.
10. Check Enable DHCP/PXE Server.
11. Enter the subnet (192.168.76.0).
12. Enter the netmask (255.255.255.0).
13. Enter the DHCP Scope Starting IP Address (192.168.76.100).
14. Enter the DHCP Scope Ending IP Address (192.168.76.200).
15. Enter the Default Gateway (192.168.76.1).
16. Click Save and Continue.
17. Review the summary, and click Finish.
18. Click Yes to confirm, and stop the timer.

Configuring Dell ASM chassis and blade

Adding network definitions

1. Simultaneously start the timer, and click Define Networks.
2. We used six networks in our setup: a hypervisor management network, a hypervisor migration network, a storage network, a PXE network, a data network, and a hardware management network. Click + Define.
3. Name the hypervisor management network (Hypervisor Management).
4. Change Network Type to Hypervisor Management.
5. Enter the hypervisor management VLAN ID (128).
6. Check Configure static IP address ranges.
7. Enter the hypervisor management network Gateway (10.128.0.1).
8. Enter the hypervisor management network Subnet Mask (255.255.0.0).
9. Enter the hypervisor management network Primary DNS (10.128.0.10).
10. Click Add IP Address Range.
11. Enter the Starting IP Address (10.128.30.1).
12. Enter the Ending IP Address (10.128.30.254).
13. Click Save IP Address Range.
14. Click Save.
15. Click +Define.
16. Name the hypervisor migration network (Hypervisor Migration).
17. Change Network Type to Hypervisor Migration.
18. Enter the hypervisor migration VLAN ID (200).
19. Check Configure static IP address ranges.
20. Enter the hypervisor migration network Subnet Mask (255.255.255.0).
21. Click Add IP Address Range.
22. Enter the Starting IP Address (192.168.200.150).
23. Enter the Ending IP Address (192.168.200.199).
24. Click Save IP Address Range.
25. Click Save.
26. Click +Define.
27. Name the storage network (Storage).
28. Change Network Type to SAN [Software iSCSI].
29. Enter the storage VLAN ID (201).
30. Check Configure static IP address ranges.
31. Enter the storage network Subnet Mask (255.255.255.0).
32. Click Add IP Address Range.
33. Enter the Starting IP Address (192.168.201.150).
34. Enter the Ending IP Address (192.168.201.199).
35. Click Save IP Address Range.
36. Click Save.
37. Click +Define.
38. Name the PXE network (PXE deployment).

39. Change Network Type to PXE.
40. Enter the PXE VLAN ID (1076).
41. Click Save.
42. Click +Define.
43. Name the Data network (Data).
44. Change the Network Type to Private LAN.
45. Enter the data network VLAN ID (1080).
46. Click Save.
47. Click +Define.
48. Name the hardware management network (Hardware Management).
49. Change Network Type to Hardware Management.
50. Check Configure static IP address ranges.
51. Enter the hardware management network Gateway (10.128.0.1).
52. Enter the hardware management network Subnet Mask (255.255.0.0).
53. Enter the hardware management network Primary DNS (10.128.0.10).
54. Click Add IP Address Range.
55. Enter the Starting IP Address (10.128.3.1).
56. Enter the Ending IP Address (10.128.3.254).
57. Click Save IP Address Range.
58. Click Save.
59. Click Close, and stop the timer.

Discovering the chassis and blade

Note: These steps continue from the Getting Started wizard.

1. Simultaneously start the timer and click Discover Resources to launch the discovery wizard.
2. Click Next.
3. Click Add Resource Type.
4. Change Select to Chassis.
5. Enter the CMC IP address in the Starting IP Address field. If the IP address is unknown, include an Ending IP Address.
6. Click Save.
7. Click Next.
8. Click Finish.
9. Click Yes when the warning dialog appears and stop the timer. Automation time completes when all servers report Available from the Resources dashboard.

Checking firmware compliance

1. Simultaneously start the timer and click Configure Resources to launch the resource configuration wizard.
2. Click Next.
3. Check that the Chassis resource, the blades, and interconnects will all be selected.
4. Click Next.
5. Check the Embedded ASM Minimum Required Default Firmware Repository.
6. Click Next.

7. When the Firmware Compliance check completes successfully, click Next and stop the timer.

Configuring resources

1. Continued from the Configure Resources wizard above.
2. At the Chassis Configuration page, simultaneously start the timer and click the NTP dropdown, and change Time Zone to EST (UTC -5:00).
3. Click Next.
4. If you wish to customize the Chassis Name, CMC DNS Name, System Input Power Cap, or Location Details, check Configure Unique Chassis Settings; otherwise, click Next.
5. If you wish to customize the blade iDRAC DNS names, check Configure Unique Server Settings; otherwise, click Next.
6. If you wish to customize the I/O Module host names, check configure Unique I/O Module Settings and enter the names; otherwise, click next.
7. If you wish to configure the Uplinks, check Configure Uplinks; otherwise, click Next.
8. Click Finish.
9. Click Yes when the warning dialog appears and stop the timer.

Discovering storage, vCenter, and TOR switch

1. Simultaneously start the timer and click the Resources tab.
2. Click Discover.
3. At the Discover Resources Welcome screen, click Next.
4. Click Add Resource Type.
5. Change Select to Switch.
6. Enter the top of rack switch management IP address in the Starting IP Address field (10.128.1.5). If the IP address is unknown, include an Ending IP Address.
7. Click the + icon next to Select Switch Credential.
8. Enter a Credential Name.
9. Enter the top of rack username and password, and confirm the password.
10. Click Save.
11. Click Add Resource Type.
12. Change Select to vCenter.
13. Enter the vCenter Host IP in the Starting IP Address field (10.128.0.60). If the IP address is not known, include an Ending IP Address.
14. Click the + icon next to Select vCenter Credential.
15. Enter a Credential Name.
16. Enter the vCenter username and password, and confirm the password.
17. Click Save.
18. Click Add Resource Type.
19. Change Select to Storage.
20. Enter the storage Group Mgmt IP in the Starting IP Address field (10.128.0.86). If the IP address is not known, include an Ending IP Address.
21. Click the + icon next to Select Storage Credential.
22. Enter a Credential Name.

23. Enter the storage username and password, and confirm the password.
24. Click Next.
25. Click Finish.
26. Click Yes when the warning dialog appears and stop the timer. Automation time completes when the Discovery Job Running dialog closes and all items are as Available in the Resources pane.

Deploying a Dell ASM service

Creating the template

1. Simultaneously start the timer and click the Templates tab.
2. Click the Default Templates category to expand the default templates, and select Deploy VMware Cluster with iSCSI Storage.
3. Click Clone.
4. Enter a Template Name (Test Deployment).
5. Select Create a New Category and enter the New Category Name (Test Templates).
6. Click Save.
7. From the Template Designer, select the Cluster and click Edit.
8. Change Target Virtual Machine Manager to vcenter.
9. Change Data Center Name to Create New Datacenter… and enter the New datacenter name (ASMDC).
10. Change Cluster Name to Create New Cluster… and enter the New cluster name (ASMCluster).
11. Check Cluster HA Enabled.
12. Check Cluster DRS Enabled.
13. Click Save.
14. Select the first Server and click Edit.
15. Scroll down to the NIC Partition section. For the first Partition, check the Hypervisor Management and PXE networks.
16. For the second Partition, check the Hypervisor Migration network.
17. For the third Partition, check the Data network.
18. For the fourth Partition, check the Storage network.
19. Click Save.
20. Select the second Server and click Edit.
21. Scroll down to the NIC Partition section. For the first Partition, check the Hypervisor Management and PXE networks.
22. For the second Partition, check the Hypervisor Migration network.
23. For the third Partition, check the Data network.
24. For the fourth Partition, check the Storage network.
25. Click Save.
26. Select the first Storage Component and click Edit.
27. Change Target EqualLogic to group-0.
28. Change Storage Volume Name to Create New Volume… and enter the New Volume Name (ASMClusterVolumeOne).
29. Change Storage Size to 1000GB.
30. Click Save.

31. Select the second Storage Component and click Edit.
32. Change Storage Volume Name to Create New Volume… and enter the New Volume Name (ASMClusterVolumeTwo).
33. Change Target EqualLogic to group-0.
34. Change Storage Size to 1000GB.
35. Click Save.
36. Click Publish Template.
37. Click Yes when the warning dialog appears and stop the timer.

Deploying a service from template

1. Simultaneously start the timer and click the Services tab.
2. Click Deploy New Service.
3. Change Select Template to the newly created template (Test Deployment).
4. Enter a service name (Test Service 1).
5. Click Next.
6. Name the first Server's OS Host Name.
7. Name Server 2's OS Host Name.
8. Click Next.
9. Click Finish.
10. Click Yes when the warning dialog appears and stop the timer. Automation time completes when the service is fully deployed.

Deploying the Cisco UCS Director Appliance

Deploying UCSD OVF appliance

1. Before testing, extract the Cisco UCS Director .zip file (CUCSD_5_2_0_0_VMWARE_GA.zip) to a location accessible by VMware vSphere Client.
2. Simultaneously start the timer and open vSphere Client and connect to the vCenter server that will be used to host the Cisco UCSD appliance.
3. In vSphere Client, click File, Deploy OVF Template. The Deploy OVF Template wizard will open.
4. On the Source page, click Browse, and then select the OVF package.
5. Click Next to continue.
6. Click Next again to continue.
7. Accept the License Agreement and click Next to continue.
8. Enter a name (Cisco UCSD), and select the Inventory Location.
9. Click Next to continue.
10. Assuming a resource pool has been configure, select the storage volume to host the appliance virtual machine. For our tests, we used an EqualLogic array.
11. Click Next to continue.
12. On the Disk Format page, select Thin Provision.
13. Click Next to continue.
14. Verify the Destination Network for Network 1 is set to the management VLAN (mgmt vlan128).
15. Click Next.

16. Click Finish to run the deployment job and stop the timer.

Configuring UCSD VM Network Adapter

1. Simultaneously start the timer and select the newly created VM (Cisco UCSD) from the host.
2. In the Getting Started subtab, click Edit virtual machine settings.
3. Select Network adapter 1.
4. Verify the Network label is set to the management network (management vlan128).
5. Click Add…
6. Select Ethernet Adapter and click Next.
7. Under the Network Connection section, select the PXE network label (PXE vlan1076).
8. Click Next.
9. Click Finish.
10. Click OK. Stop the timer when the Recent Tasks list reports that Reconfiguring virtual machine has Completed.

Applying UCSD appliance network definitions

1. In the vSphere Client, simultaneously start the timer and right click the Cisco UCSD virtual machine, and select Power On.
2. Click the Console tab.
3. Use the spacebar to scroll through the license agreement.
4. Type yes and press enter to accept the license agreement.
5. Type yes and press enter to Configure static IP.
6. Type v4 and press enter to configure IPv4.
7. Type the IP address of the appliance and press enter (for our test we used 10.128.4.1).
8. Type the Netmask and press enter (for our test we used 255.255.0.0).
9. Type the Gateway and press enter (for our test we used 10.128.0.1).
10. Type yes and press enter to continue.
11. Type 1 and press enter to use the default Cisco UCS Director personality and top the timer. Automation time completes when the server finishes rebooting.

Setting up Cisco UCSD with the initial setup wizard

1. Simultaneously start the timer and navigate to the UCSD appliance IP (10.128.4.1). Accept any certificate warnings.
2. Log in with the default credentials (admin, admin).
3. At the Guided Setup screen, check Initial System Configuration and Device Discovery.
4. Click Submit.
5. In the Selected Tasks pane, uncheck Mail Setup, Configured Email, and DNS Server.
6. Click Submit.
7. Click Next.
8. Click Browse, navigate to the license file location, and upload the license file.
9. Click Upload.
10. Click OK.
11. Click Next.
12. Leave the default language and click Next.

13. Check Modify NTP Servers and enter the preferred NTP servers.
14. At the summary screen click Next and stop the timer.

Configuring Cisco UCS Manager chassis and blade

Logging in to UCSM

1. Simultaneously start the timer and navigate to the Cluster IPv4 Address (10.128.100.50). For our test, we used Google Chrome. Java was previously installed on the workstation.
2. Click Launch UCS Manager.
3. A .jnlp file will prompt for download; click Keep.
4. When the download completes, click the download to open it (ucsm.jnlp).
5. Check I accept the risk and want to run this application.
6. Click run.
7. Log in with the admin credentials (username: admin, password: Password11). Stop the timer when the UCSM window is fully loaded.

Discovering UCSM Chassis/Blade

1. Assuming USCM launches in the default tab (Equipment), simultaneously start the timer, select the Equipment tree item, and click the Policies subtab.
2. In Global Policies, verify the Chassis/FEX Discovery Policy matches the physical configuration (our test used two 10Gb connections between each Fabric interconnect and IOM, so we selected 2 Link).
3. Configure the power policy to match the chassis' configuration (for our test, we selected Grid).
4. Click Save Changes.
5. Click OK.
6. Click the Fabric Interconnects subtab.
7. In the Fabric Interconnects subtab pane, click the topmost + icon to extend all available ports.
8. For Fabric Interconnect A, select the server ports, right click, and select Configure as Server Port (for our test, we used ports 1 and 2 as our server ports for Fabric Interconnect A).
9. Click Yes.
10. Click OK.
11. For Fabric Interconnect A, select the uplink port, right click, and select Configure as Uplink Port (for our test, we used port 3 as our uplink port on Fabric Interconnect A).
12. Click Yes.
13. Click OK.
14. Scroll down to Fabric Interconnect B, select the server ports, right click, and select Configure as Server Port (for our test, we used Ports 1 and 2 as our server ports for Fabric Interconnect B).
15. Click Yes.
16. Click OK.
17. For Fabric Interconnect B, select the uplink port, right click, and select Configure as Uplink Port (for our test, we used port 3 as our uplink port on Fabric Interconnect B).
18. Click Yes.
19. Click OK.

20. Verify that the Overall Status changes to Up for all configured ports, and the Administrative State changes to Enabled.
21. Click the + icon in the Equipment tree to expand all items; stop the timer when Chassis 1 appears.

Assigning management pool addresses to UCSM

1. Simultaneously start the timer and click the LAN tab.
2. Under the Pools tree, expand the root organization and select IP Pools.
3. In the IP Pools pane, right click IP Pool ext-mgmt and select Create a Block of IPv4 Addresses.
4. Enter the beginning IP address range (for our test we used 10.128.173.1).
5. Enter the size (for our test we used 16).
6. Enter the Subnet Mask (for our test we used 255.255.0.0).
7. Enter the Default Gateway (for our test we used 10.128.0.1).
8. Enter the Primary DNS (for our test we used 10.128.0.10).
9. Click OK.
10. Click OK again and stop the timer.

Assigning WWNN and WWPN pool addresses to UCSM

1. Simultaneously start the timer and click the SAN tab.
2. Under the Pools tree, expand the root organization and select WWNN Pools.
3. In the WWNN Pools pane, right click WWNN Pool node-default and select Create WWN Block.
4. Enter the first WWN Block (for our test we used 20:00:00:25:B5:00:00:00).
5. Enter the size (for our test we used 64).
6. Click OK.
7. Click OK again.
8. Under the root organization, select WWPN Pools.
9. In the WWPN Pools pane, right click WWPN Pool default and select Create WWN Block.
10. Enter the first WWN Block (for our test we used 20:00:00:25:b5:00:00:00).
11. Enter the size (for our test we used 64).
12. Click OK.
13. Click OK again and stop the timer.

Assigning MAC pool addresses to UCSM

1. Simultaneously start the timer and click the LAN tab.
2. Under the Pools tree, expand the root organization and select MAC Pools.
3. Right click MAC Pool default and select Create a Block of MAC Addresses.
4. Enter the first MAC Address (for our test we used 00:25:B5:12:00:00).
5. Enter the size (for our test we used 64).
6. Click OK.
7. Click OK again and stop the timer.

Assigning UUID pool addresses to UCSM

1. Simultaneously start the timer and click the Servers tab.
2. Under the Pools tree, expand the root organization and select UUID Suffix Pools.
3. Right click Pool default, and select Create a Block of UUID Suffixes.

4. Leave the default UUID Suffix and enter the size (for our test we used 10).
5. Click OK.
6. Click OK again and stop the timer.

Creating a vNIC template and adding VLAN definitions in UCSM

1. Simultaneously start the timer and click the LAN tab.
2. Under the Policies tree, expand the root organization, right click vNIC Templates and select Create vNIC Template.
3. Name the vNIC Template to match Fabric A (for our test we used vNIC Template A).
4. Check Enable Failover.
5. In the VLANs section, click Create VLAN.
6. Name the management VLAN (for our test we used management).
7. Enter the management VLAN IDs (for our test, we used 128 as our management VLAN ID).
8. Click OK.
9. Click OK again.
10. Click Create VLAN.
11. Name the vMotion VLAN (for our test we used vMotion).
12. Enter the vMotion VLAN ID (for our test, we used 200 as our hypervisor migration VLAN ID).
13. Click OK.
14. Click OK again.
15. Click Create VLAN.
16. Name the storage VLAN (for our test we used storage).
17. Enter the storage VLAN ID (for our test, we used 201 as our storage VLAN ID).
18. Click OK.
19. Click OK again.
20. Click Create VLAN.
21. Name the data VLAN (for our test we used data).
22. Enter the data VLAN ID (for our test, we used 1080 as our storage VLAN ID).
23. Click OK.
24. Click OK again.
25. In the VLANs section, check the default, data, management, storage, and vMotion VLANs.
26. Select default as the Native VLAN.
27. Change MTU to 9000.
28. Change MAC Pool to the default pool.
29. Click OK.
30. Click OK again.
31. Right click vNIC Templates and select Create vNIC Template.
32. Name the vNIC Template to match Fabric B (for our test we used vNIC Template B).
33. Change Fabric ID to Fabric B and check Enable Failover.
34. In the VLANs section, check the default, data, management, storage, and vMotion VLANs.
35. Select default as the Native VLAN.
36. Change MTU to 9000.

37. Change MAC Pool to the default pool.
38. Click OK.
39. Click OK again and stop the timer.

Creating a vHBA template and adding VSAN Definitions in UCSM

1. Simultaneously start the timer and click the SAN tab.
2. Under the Policies tree, expand the root organization, right click vHBA Templates and select Create vHBA Template.
3. Enter the vHBA Template Name (F-A).
4. Ensure Select VSAN is set to the default VSAN and WWPN Pool is set to the default pool.
5. Click OK.
6. Click OK again.
7. Right click vHBA Templates again and select Create vHBA Template.
8. Enter the vHBA Template Name (F-B).
9. Change Fabric ID to B.
10. Ensure Select VSAN is set to the default VSAN and WWPN Pool is set to the default pool.
11. Click OK.
12. Click OK again, and stop the timer.

Configuring UCSM blade firmware (baseline)

1. Simultaneously start the timer and click the Equipment tab.
2. Ensure the topmost tree item is selected (Equipment) and click on the Firmware Management subtab.
3. From Installed Firmware, ensure UCS Manager is selected, and click Update Firmware.
4. Change Version to Bundle.
5. Change Set Bundle to the most updated version available (for our test we used 2.2(1d)A).
6. Click Apply.
7. Click OK.
8. Click OK again, and stop the timer. Automation time completes when all Update Statuses change to Ready.

Creating a UCSM service profile template

1. Simultaneously start the timer and click the Servers Tab.
2. Expand the Servers tree, right click Service Profile Templates and select Create Service Profile Template.
3. Name the template (for our test we used b200-template).
4. Change UUID Assisgnment to the default pool.
5. Click Next.
6. Change the configuration mode from Simple to Expert.
7. Click Add.
8. Name the vNIC for Fabric A (for our test we used 0).
9. Check Use vNIC Template.
10. Change vNIC Template to nic-a.
11. Change Adapter Policy to VMWare.
12. Click OK.
13. Click Add.

14. Name the vNIC for Fabric B (for our test we used 1).
15. Check Use vNIC Template.
16. Change vNIC Template to nic-b.
17. Change Adapter Policy to VMWare.
18. Click OK.
19. Click Next.
20. Change Local Storage to default Storage Policy.
21. Change SAN connectivity to No vHBAs.
22. Click Next.
23. Click Next to skip the Zoning configuration screen.
24. Click Next to skip the vNIC/vHBA Placement screen.
25. Change Boot Policy to default.
26. Click Next.
27. Click Next to skip the Maintenance Policy screen.
28. At the Server Assignment screen, change the selected power state to Down.
29. Click Next.
30. At the Operational Policies screen, click the Management IP Address dropdown field.
31. Change Outband IPv4 Management IP Address Policy to ext-mgmt(X/16).
32. Click Finish.
33. Click OK, and stop the timer.

Creating UCSM service profiles

These steps continue from the Servers tab from the Service Profile Template creation instructions above.

1. Simultaneously start the timer and select the newly created template (Service Template b200-template), right click, and select Create Service Profiles From Template.
2. Enter the Naming Prefix (for our test we used server).
3. Enter the Name Suffix Starting Number (for our test we used 1).
4. Enter the Number of Instances (for our test we used 4).
5. Click OK.
6. Click OK again, and stop the timer.

Adding servers to the default server pool in UCSM

These steps continue from the Servers tab from the instructions above.

1. Simultaneously start the timer and expand the Pools tree, expand the Server Pools tree, right click Server Pool default and select Add Servers to Server Pool.
2. Click the first server, shift click the last server to select all servers, and click the >> arrow to move all servers into the Pooled Servers section.
3. Click OK.
4. Click OK again, and stop the timer.

UCSD UCSM and NetApp Account Discovery

1. Click the Administration dropdown menu, and select Physical Accounts.
2. Click the Physical Accounts subtab.

3. Click Device Discovery.
4. At the Overview screen, click Next.
5. Enter the IP Address for the UCSM and NetApp account (10.128.100.50, 10.128.60.51).
6. Under Credential Policy, click the + icon.
7. In the Add Credential Policy screen, select UCSM as the Account Type.
8. Enter the Policy Name (UCSM-Credentials), UCSM Username (admin), and the UCSM Password (Password1). Accept the default Protocol, Port, Authentication Type, and Server Management settings, and click Submit.
9. Click OK.
10. Under Credential Policy, click the + icon.
11. In the Add Credential Policy screen, select NetApp ONTAP as the Account Type, enter the Policy Name (NetApp-Credentials), the NetApp ONTAP Username (admin) and NetApp ONTAP Password (Password1). Accept the default Protocol and Port settings, and click Submit.
12. Click OK.
13. Click Next.
14. Click Discover.
15. Click the topmost checkbox to select both discovered accounts. Click Add.
16. Click Close.

UCSD Virtual Account Discovery

1. Click the Administration dropdown menu and select Virtual Accounts.
2. Under the Virtual Accounts subtab, click +Add.
3. Change Cloud Type to VMware, enter the Cloud Name (VDC01), the Server Address (10.128.0.60), the Server User ID (root), and the Server Password (vmware). Accept the default Server Access Port and Server Access URL and click Add.
4. Click OK.

UCSD Workflow Variable Definition

1. Click the Policies dropdown menu and select Orchestration.
2. Click + Add Workflow, Enter Workflow Name and Select Folder. Click Next.
3. Click + button. Enter Input label (Cluster Name), click Select, check Generic Text Input, click Select, check Admin Input value, enter (Cluster Name) in box then click Submit. Click Ok.
4. Click + button. Enter Input label (Static IP Pool), click Select, check Static IP Pool Address Input, click Select, check Admin Input value, enter (IP Pool Range) in box then click Submit. Click Ok.
5. Click + button. Enter Input label (Gateway IP), click Select, check Generic Text Input, click Select, check Admin Input value, enter (10.128.0.1) in box then click Submit. Click Ok.
6. Click + button. Enter Input label (Netmask 24 Bit), click Select, check Subnet Mask, click Select, check Admin Input value, enter (255.255.255.0) in box then click Submit. Click Ok.
7. Click + button. Enter Input label (Netmask 16 Bit), click Select, check Subnet Mask, click Select, check Admin Input value, enter (255.255.0.0) in box then click Submit. Click Ok.
8. Click + button. Enter Input label (Name Server), click Select, check Generic Text Input, click Select, check Admin Input value, enter (10.128.0.10) in box, and click Submit. Click Ok.
9. Click + button. Enter Input label (User Name), click Select, check Generic Text Input, click Select, check Admin Input value, enter (root) in box, and click Submit. Click Ok.

10. Click + button. Enter Input label (Root Password), click Select, check Password, click Select, check Admin Input value, enter (Password1) in box then click Submit. Click Ok.
11. Click + button. Enter Input label (Server Pool), click select, check UCS Multi Server Pool Identity, click Select, check Admin Input List, select all Server Pools then click Submit. Click Ok.
12. Click + button. Enter Input label (Select Server Blade 1)), click select, check, check UCS Server Identity, click Select, check Admin Input List, select all blades then click Submit. Click Ok.
13. Click + button. Enter Input label (Select Server Blade 2)), click select, check, check UCS Server Identity, click Select, check Admin Input List, select all blades then click Submit. Click Ok.
14. Click + button. Enter Input label (Select Profile 1)), click select, check, check UCS Service Profile Identity, click Select, check Admin Input List, select all profiles then click Submit. Click Ok.
15. Click + button. Enter Input label (Select Profile 2)), click select, check, check UCS Service Profile Identity, click Select, check Admin Input List, select all profiles then click Submit. Click Ok.
16. Click + button. Enter Input label (Default Boot Policy), click select, check, check UCS Boot Policy Identity, click Select, check Admin Input List, select all boot policies then click Submit. Click Ok.
17. Click + button. Enter Input label (PXE Boot Policy), click select, check, check UCS Boot Policy Identity, click Select, check Admin Input List, select all boot policies then click Submit. Click Ok.
18. Click + button. Enter Input label (IP Range), click Select, check Generic Text Input, click Select, check Admin Input value, enter (10.128.4.101 – 10.128.4.200) in box then click Submit. Click Ok.
19. Click Next. Click Submit. Click Ok.

UCSD Workflow Creation

1. Expand the folder that contains newly created workflow, and double-click workflow.
2. From left column, expand Physical Compute Tasks, and expand Cisco UCS Tasks.
3. Drag and drop Associate UCS Service Profile task onto work area.
4. Accept the defaults, and click Next.
5. Check Map to User Input for Service Profile, and from the pull-down menu, select Service Profile 1.
6. Check Map to User Input for Server, and from the pull-down menu, select Select Server 1.
7. Check Map to User Input for Server Pool, and from the pull-down menu, select Server Pool.
8. Click Next.
9. From the pull-down menu, select Include Servers.
10. Click Next. Click Submit. Click Ok.
11. From left column, expand Physical Compute Tasks, and expand Cisco UCS Tasks.
12. Drag and drop Modify UCS Service Profile Boot Policy into the work area.
13. Accept the defaults for Task Information, and click next.
14. Check Map to User Input for Service Profile, and from the pull-down menu, select Service Profile 1.
15. Check Map to User Input for Boot Policy, and from the pull-down menu, select PXE Boot Policy.
16. Click Next. Click Next.
17. Click Submit. Click Ok.
18. From left column expand Cloupia Tasks, expand Network Services tasks, and drag and drop Setup PXE Boot task on to work area.
19. Accept the defaults for Task Information, and click Next.
20. Click Next.

21. Check Map to User Input for Server MAC Address, and from the pull-down menu, select AssociateUCSServiceProfile_###.OUTPUT_UCS_BLADE_MAC_ADDRESS.
22. Check Map to User Input for Server Address, and from the pull-down menu, select IP Range.
23. Check Map to User Input for Server Pool, and from the pull-down menu, select Server Pool.
24. Check Map to User Input for Server Netmask, and from the pull-down menu, select Netmask 16 Bit.
25. Check Map to User Input for Server Name Server, and from the pull-down menu, select Name Server.
26. Check Map to User Input for Root Password, and from the pull-down menu, select Root Password.
27. Click Next.
28. Select ESXi_Cisco_5.5 from the OS Type pull-down menu.
29. Enter Server Host Name.
30. Select Timezone.
31. Click Next.
32. Click Submit. Click Ok.
33. From the left column, expand Physical Compute Tasks, and expand Cisco UCS Tasks.
34. Drag and drop Associate UCS Service Profile task onto work area.
35. Accept the defaults and click Next.
36. Check Map to User Input for Service Profile, and from the pull-down menu, select Service Profile 2.
37. Check Map to User Input for Server and from the pull-down menu, select Server 2.
38. Check Map to User Input for Server Pool, and from the pull-down menu, select Server Pool.
39. Click Next.
40. From the pull-Down menu, select Include Servers.
41. Click Next.
42. Click Submit. Click Ok.
43. From the left column, expand Physical Compute Tasks, and expand Cisco UCS Tasks.
44. Drag and drop Modify UCS Service Profile Boot Policy into the work area.
45. Accept the defaults for Task Information, and click Next.
46. Check Map to User Input for Service Profile, and from the pull-down menu, select Service Profile 2.
47. Check Map to User Input for Boot Policy, and from the pull-down menu, select PXE Boot Policy.
48. Click Next.
49. Click Next.
50. Click Submit. Click Ok.
51. From the left column, expand Cloupia Tasks, expand Network Services tasks, and drag and drop Setup PXE Boot task onto the work area.
52. Accept the defaults for Task Information, and click Next.
53. Click Next.
54. Check Map to User Input for Server MAC Address, and from the pull-down menu, select AssociateUCSServiceProfile_###.OUTPUT_UCS_BLADE_MAC_ADDRESS.
55. Check Map to User Input for Server Address, and from the pull-down menu, select IP Range.
56. Check Map to User Input for Server Pool, and from the pull-down menu, select Server Pool.
57. Check Map to User Input for Server Netmask, and from the pull-down menu, select Netmask 16 Bit.
58. Check Map to User Input for Server Name Server, and from the pull-down menu, select Name Server.
59. Check Map to User Input for Root Password, and from the pull-down menu, select Root Password.

60. Click Next.
61. Select ESXi_Cisco_5.5 from the OS Type pull-down menu.
62. Enter Server Host Name.
63. Select Timezone.
64. Click Next.
65. Click Submit. Click Ok.
66. From the left column, expand Cloupia Tasks, expand general tasks, and drag and drop Wait for Specified Duration task onto the work area.
67. Click Next.
68. Click Next.
69. Set Duration for 10 min, and click Next.
70. Click Submit. Click Ok.
71. From the left column, expand Physical Compute Tasks, and expand Cisco UCS Tasks.
72. Drag and drop Modify UCS Service Profile Boot Policy into the work area.
73. Accept the defaults for Task Information, and click Next.
74. Check Map to User Input for Service Profile, and from the pull-down menu, select Service Profile 1.
75. Check Map to User Input for Boot Policy, and from the pull-down menu, select Default Boot Policy.
76. Click Next.
77. Click Submit. Click Ok.
78. From the left column, expand Physical Compute Tasks, and expand Cisco UCS Tasks.
79. Drag and drop Modify UCS Service Profile Boot Policy into the work area.
80. Accept the defaults for Task Information, and click Next.
81. Check Map to User Input for Service Profile, and from the pull-down menu, select Service Profile 2.
82. Check Map to User Input for Boot Policy, and from the pull-down menu, select Default Boot Policy.
83. Click Next.
84. Click Submit. Click Ok.
85. From the left column, expand Physical Storage Tasks, and expand NetApp ONTAP Tasks.
86. Drag and drop Create Flexible Volume.
87. Accept the defaults for Task Information, and click Next.
88. Accept the defaults for User Input Mapping, and click Next.
89. Click Select for Aggregate Name, and select desired Aggregate.
90. Enter volume name, volume size, and volume size units. In the pull-down for Space Guarantee, select none. Enter 5 for Snapshot Size. Click Next.
91. Click Submit, and click OK.
92. Drag and drop Create LUN.
93. Click Next.
94. Select the check box for NetApp Volume Identity, select CreateNetAppFlexibleVolume, and click Next.
95. Select VMware as OS Type, enter LUN Size, select GB for LUN Size Units, select Reserve Space, and click Next.
96. Click Submit, and click OK.
97. Drag and drop Create Initiator Group.
98. Accept the defaults for Task Information, and click Next.
99. Accept the defaults for User Input Mapping, and click Next.

100. Click Select.
101. Check the box beside the target array, and click Select.
102. Accept the remaining defaults, and click Next.
103. Click Submit, and click Ok.
104. Drag and drop Map LUN to Initiator Group.
105. Click Next.
106. Click Next, select the check box for NetApp Filer Identity, Netapp Initiator Group Name, Netapp LUN Path. Accept the default selections, and click Next.
107. Accept the defaults for Task Inputs, and click Next.
108. Click Submit, and click OK.
109. From the left column, expand Cloupia Tasks, expand General Tasks, and drag and drop Wait for Specified Duration task onto the work area.
110. Accept the defaults for Task Information, and click Next.
111. Accept the defaults for User Input Mapping, and click Next.
112. Set Duration for 5 min, and click Next.
113. Click Submit, and click OK.
114. From the left column, expand Virtualization Tasks→VMware Tasks→VMware Host Tasks, and drag and drop Create Cluster into the work area.
115. Accept the defaults for Task Information, and click Next.
116. Accept the defaults for User Input Mapping, and click Next.
117. Select the Datacenter Name from the pull-down list, and provide a Cluster Name for the new cluster. Click Next.
118. Click Submit, and click OK.
119. From the left column, expand Virtualization Tasks→VMware Tasks→VMware Host Tasks, and drag and drop Register Host with vCenter into the work area.
120. Accept the defaults for Task Information, and click Next.
121. Check Map to User Input for Server Netmask, and from the pull-down menu, select PXEBOOT_###.OUTPUT_PXE_BOOT_ID.
122. Check Map to User Input for Host Node, and from the pull-down menu, select PXEBOOT_###.OUTPUT_HOST_IP_ADDRESS.
123. Check Map to User Input for User ID, and from the pull-down menu, select User Name.
124. Check Map to User Input for Password, and from the pull-down menu, select Root Password.
125. Check Map to User Input for Cluster/Data Center, and from the pull-down menu, select CreateVMwareCluster_###.OUTPUT_CLUSTER_NAME.
126. Click Next.
127. From the pull-down menu, select Account Name.
128. Select Cluster from the Associate with pull-down menu.
129. Click Next.
130. Click Submit, and click OK
131. From the left column expand Virtualization Tasks→VMware Tasks→VMware Host Tasks, and drag and drop Register Host with vCenter into the work area.
132. Accept the defaults for Task Information, and click Next.

133. Check Map to User Input for Server Netmask, and from the pull-down menu, select PXEBOOT_###.OUTPUT_PXE_BOOT_ID.
134. Check Map to User Input for Host Node, and from the pull-down menu, select PXEBOOT_###.OUTPUT_HOST_IP_ADDRESS.
135. Check Map to User Input for User ID, and from the pull-down menu, select User Name.
136. Check Map to User Input for Password, and from the pull-down menu, select Root Password.
137. Check Map to User Input for Cluster/Data Center, and from the pull-down menu, select CreateVMwareCluster_###.OUTPUT_CLUSTER_NAME.
138. Click Next.
139. From the pull-down menu, select Account Name.
140. Select Cluster from the Associate with pull-down menu.
141. Click Next.
142. Click Submit, and click OK.
143. From the left column, expand Virtualization Tasks→VMware Tasks→VMware Network Tasks, and drag and drop vSwitch into the work area.
144. Accept the defaults for Task Information, and click Next.
145. Check Map to User Input for PXE Boot Id, and from the pull-down menu, select PXEBOOT_###.OUTPUT_PXE_HOST_IP_ADDRESS.
146. Click Next.
147. Select Account Name from the pull-down menu.
148. Accept Number of Switch Ports default.
149. Enter the vSwitch Name.
150. Click Next.
151. Click Submit, and click OK.
152. From the left column, expand Virtualization Tasks→VMware Tasks→VMware Network Tasks, and drag and drop Create vSwitch into the work area.
153. Accept the defaults for Task Information, and click Next.
154. Check Map to User Input for Server PXE Boot Id, and from the pull-down menu, select PXEBOOT_###.OUTPUT_PXE_HOST_IP_ADDRESS.
155. Click Next.
156. Select Account Name from the pull-down menu.
157. Accept Number of Switch Ports default.
158. Enter vSwitch Name.
159. Click Next.
160. Click Submit, and click OK.
161. From the left column, expand Virtualization Tasks→VMware Tasks→VMware Network Tasks, and drag and drop Create VMKernel Port Group into the work area.
162. Accept the defaults for Task Information, and click Next.
163. Check Map to User Input for Cluster/Data Center, and from the pull-down menu, select CreateVMwareCluster_###.OUTPUT_CLUSTER_NAME.
164. Check Map to User Input for Datacenter Name, and from the pull-down menu, select CreateVMwareCluster_###.OUTPUT_DATACENTER_NAME.

165. Check Map to User Input for Cluster Name, and from the pull-down menu, select Cluster Name.
166. Check Map to User Input for vSwitch Name, and from the pull-down menu, select CreatevSwitch_###.OUTPUT_VMWARE_VSWITCH_IDENTITY.
167. Check Map to User Input for Static IP Pool, and from the pull-down menu, select Static IP Pool.
168. Check Map to User Input for Gateway IP, and from the pull-down menu, select Gateway IP.
169. Click Next.
170. Select Account name from the pull-down menu, select (Vm Kernel Portgroup), enter (iSCSI0) for Network Label, Enter (201) for VLAN ID, select IPv4 from the Network Type pull-down menu, enter (255.255.255.0) for Subnet mask, and click Next.
171. Click Submit, and click OK.
172. From the left column, expand Cloupia Tasks, expand Network Services tasks, and drag and drop Remove PXE Boot Setup task onto the work area.
173. Accept the defaults for Task Information, and click Next.
174. Click Next.
175. Check Map to User Input for Server PXE Boot Id, and from the pull-down menu, select PXEBOOT_###.OUTPUT_PXE_BOOT_ID.
176. Click Next. Click Next. Click Ok.
177. From the left column, expand Cloupia Tasks, expand Network Services tasks, and drag and drop Remove PXE Boot Setup task onto the work area.
178. Accept the defaults for Task Information, and click Next.
179. Click Next.
180. Check Map to User Input for Server PXE Boot Id, and from the pull-down menu, select PXEBOOT_###.OUTPUT_PXE_BOOT_ID.
181. Click Next. Click Submit. Click Ok.

Executing the UCS Director workflow

1. Log into Cisco UCS Director.
2. Select Policies Tab→Orchestration.
3. Expand Addinsell_Verify Folder.
4. Right-click the workflow, and select Execute Now.
    a. Enter Cluster Name.
    b. Select Default Boot Policy Default.
    c. Enter Cluster Name `UCSD001`
    d. Select Server Pool Server Pool Addinsell.
    e. Select Server Blade 1.
    f. Select PXE Boot Policy “PXE.”
    g. Select Server Blade 2.
    h. Select Service Profile 2.
5. Click Submit.
6. Click Monitor task.

Post-workflow tasks

1. Log into vSphere Client. Enter IPaddress/Name, User name, and Password. Click Login.

2. Click Ignore.
3. Expand Datacenter→Cluster.
4. Select the first server. On the Configuration tab, click the Networking menu item.
5. Click Add Networking, and select VMKernel. Click Next.
6. Accept defaults, and click Next.
7. Change Network Label to desired name (vSwitch3).
8. Enter VLAN (201). Click Next.
9. Enter IP Address and Subnet Mask. Click Next. Click Finish.
10. From the hardware section on the left, select Storage adapter.
11. Click add. Select Add Software iSCSI Adapter. Click OK. Click OK.
12. Select the iSCSI Software Adapter, and click Properties.
13. On the General tab, highlight the iSCSI name, right-click, and select Copy.
14. Click Close.
15. Open the NetApp OnCommand Application.
16. Double-click the entry for the array you want to modify.
17. Expand Storage→LUNs, and select the Initiator Group tab.
18. Select the IGroup you created during the service deployment, and click Edit.
19. Click the Initiators tab, and click Add.
20. Right-click and paste the iSCSI name copied from the first host, and click OK.
21. Switch to the vSphere Client.
22. Select second server→Configuration.
23. Click Add Networking, and select VMKernel. Click Next.
24. Accept defaults, and click Next.
25. Change Network Label to desired name (vSwitch3).
26. Enter VLAN (201). Click Next.
27. Enter IP Address and Subnet Mask. Click Next. Click Finish.
28. From the hardware section on the left, select Storage adapter.
29. Click add. Select Add Software iSCSI Adapter. Click OK. Click OK.
30. Select the iSCSI Software Adapter, and click Properties.
31. On the General tab, highlight the iSCSI name, right-click, and select Copy.
32. Switch to the NetApp OnCommand Application.
33. On the Edit Initiators window, click Add.
34. Right-click and paste the iSCSI name copied from the first host, and click OK.
35. Click Save and Close.
36. Switch to the vSphere Client.
37. On the open iSCSI Initiator panel, select the Dynamic Discovery tab, and click Add.
38. Enter the IP address of the iSCSI target. Click OK.
39. Click Close, and click Yes to initiate a rescan of the host adapters.
40. In the hardware menu, select Storage, and click Add Storage…
41. Click Next.
42. Select the newly available LUN, and click Next.

43. To accept the default disk format, click Next.
44. To accept the default layout, click Next.
45. Enter a datastore name, and click Next.
46. To accept the default size, click Next.
47. Click Finish to add the datastore.
48. Select the first host from the left menu.
49. Select the iSCSI software adapter, and click Properties.
50. Select the Dynamic Discovery tab, and click Add.
51. Enter the IP address of the iSCSI target. Click OK.
52. Click Close, and click Yes to initiate a rescan of the host adapters. The datastore is automatically added.

ABOUT PRINCIPLED TECHNOLOGIES

Principled Technologies, Inc.
1007 Slater Road, Suite 300
Durham, NC, 27703
www.principledtechnologies.com

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help our clients assess how it will fare against its competition, its performance, its market readiness, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.

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.