Setting Up SSH and Administrator Access

Introduction

This lab concerns creating a cluster; the cluster you are going to use throughout the rest of the San Volume Controller training. In simple terms, clusters are multiple servers running in concert. It is a collection of servers that, together, provide a set of resources to clients. Clusters provide high availability, optimum utilization of resources and scalability. The client is not aware of the underlying physical hardware of the cluster. This means that the client is isolated and protected from changes to the physical hardware.

The cluster has many benefits, perhaps the most important of these is high availability. Resources on clustered servers act as highly available versions of un-clustered resources. If a node (an individual server) in the cluster is down or too busy to respond to a request for a resource, the request is transparently passed to another node capable of processing it. Clients, therefore, are able to access resources even if a node has failed. The user gains access to the application in a timely and reliable manner. Another benefit is scalability. If you need to add users or applications to your system and want performance to be maintained at existing levels, you simply add servers to the cluster.

The IBM TotalStorage SAN Volume Controller is a collection of up to four cluster nodes - added in pairs. (In future releases the cluster size will be increased to permit further performance scalability.) These four nodes are managed as a set (cluster) and present a single point of control to the administrator for configuration and service activity. Within each cluster, one node will be defined as the configuration node. This node will be assigned the cluster IP address and will be responsible for transitioning additional nodes into the cluster. During normal operation of the cluster the nodes keep in touch with each other. If a node is idle for a while (a few seconds) then a heartbeat signal is sent to assure connectivity with the cluster. Should a node fail for any reason, the workload intended for that node will be taken over by another node until the failed node has been restarted and re-admitted to the cluster (which happens automatically).

In this lab, you will setup the Secure Shell (SSH) utility PuTTY and create the cluster. Secure shell (SSH) is the communication vehicle between the management system (usually the master console) and the SVC cluster. Secure shell is used to secure data flow between the SVC cluster and a client. The connection is secured by the means of a public and private key pair. The Public Key is uploaded to the SSH server. The Private Key identifies the client and is checked against the Public Key during the connection. PuTTY is pre-installed in the SVC master console. You will begin by using the PuTTY Key generator to create Public and Private encryption keys to make the cluster secure. You will then create the actual cluster within the SAN Volume Controller using the password generated by the configuration node (from the LCD screen of the node). Once the cluster is created, you will input the public and private encryption keys generated by the PuTTY Key Generator. You will then use PuTTY to identify candidate nodes that are available to be added to the cluster

and add a second node to the cluster. The lab will conclude by confirming the cluster attributes and showing you where you can modify IP addresses and set the time and date for the new cluster.

Instructions

Begin by generating the public and private encryption keys by accessing the PuTTY Key Generator.

1. Click 'Start' button.
2. Click 'Programs'.
3. Click 'PuTTY'.
4. Click 'PuTTYgen'.

Follow the directions to generate the encryption keys. The PuTTY Key generator creates public and private encryption keys to make the cluster secure. The public and private keys are compared and must match. This provides authentication to allow secure access to the management of the cluster.

5. Select 'SSH2RSA' radio button.
6. Click the 'Generate' button and move the cursor within the Key field while the key is generated. Go to 'Options', and click show me to see this done.

Follow the directions to save the newly generated Public Key.

7. Click the 'Save Public Key' button.
8. Type 'svctest.pub' in the File Name field.
9. Click the 'Save' button.

Follow the directions to save the newly generated Private Key. NOTE: The PuTTYgen warning window asks you if you want to save the key without a passphrase. In this lab, we will not use a passphrase but you should consider using a passphrase on the client that stores your private keys.

10. Click the 'Save Private Key' button.
11. Click the 'Yes' button on the PuTTYgen Warning window.
12. Save the file as 'svctest.ppk'
13. Close the PuTTY Key generator screen by clicking the X in the upper right corner.

It is now time to create the cluster and add the encryption keys to the SVC.

14. Click the 'Internet Explorer icon' in the task bar at the bottom of the screen or double click the 'Internet Explorer icon' on the desktop.

To access the SVC Console using a Web browser, use the following address: **'https://<SVC Cluster IP>/create'** . In this simulation, the IP address is 9.42.164.123.

14. Click 'File' from the menu bar.
16. Select 'Open'
17. Type 'https://9.42.164.123/create' and click 'OK'.

18. Click the 'Yes' button to accept the security certificates.

19. Type 'uKHrWPcT' in the password field. This is the password that was generated and displayed on the front panel LCD screen of the configuration node when you set up the hardware. It is CASE SENSITIVE.

20. Click the 'OK' button.

The Create New Cluster wizard will guide you through the steps to configure the new cluster.

21. Click the 'Continue' button.

This screen allows you to enter a new administrator password to replace the password that was randomly generated by the configuration node. It also allows you to create a service password. The new passwords are case sensitive and can consist of A - Z, a - z, 0 - 9, and the underscore, but cannot start with a number (minimum 1 character, maximum 15 characters). The service IP address is used to access the configuration node for service operations.
Please Note: The Administrator Password Policy check box, if selected, enables you to reset the password from the service panel if you forget it. This check box is optional. However the SVC should be in a secure room if you enable this function as anyone who knows the correct key sequence will be able to reset the administrator password.

22. Type 'password' in the Administrator Password field.
23. Tab to the Retype the Administrator Password field and re-type 'password'.
24. Tab to the Service Password field and type 'password'.
25. Press the Tab key.
26. In the Retype the Service Password field type 'password'.
27. Tab to the Cluster Name field and enter 'SVC2'.
28. Tab and type the Service IP number: '9.42.164.134'.
29. Leave the Fabric Speed at 2 Gb/s and click 'Create New Cluster' button.

The Create New Cluster screen acknowledges that the cluster has been created. You are then directed to click **Continue** to modify the administrator password you entered on the prior screen.

30. Click the 'Continue' button.

You receive verification that the password has been modified. You can now move on to set the Error Notification Settings.

31. Click the 'Continue' button.
32. In the password field, type 'password'.
33. Click the 'OK' button.

Follow the directions to configure the error notification settings. The SNMP Manager IP address is not the IP address of the SVC cluster you are creating, but the IP address of the system that will receive the error notification from the SVC cluster.

34. Click the radio button to the right of All.
35. In the SNMP Manager IP Address, field type '9.42.164.175'.
36. Tab to the SNMP Community field and type 'public'.
37. Click the 'Update Settings' button.

The Error Notification screen acknowledges that the error notification settings have been updated.

38. Click the 'Continue' button.

The Featurization Settings screen allows you to enable the FlashCopy and Remote Copy features and set the Virtualization Limit. You will learn more about these features in a later section.

39. Click the Enabled radio button for the FlashCopy parameter.
40. Click the Enabled radio button for the Remote Copy parameter.
41. Type '1000' in the Virtualization Limit field.
42. Click the 'Set Features' button.

The Featurization Settings screen acknowledges that the featurization settings have been set. It is now time to upload the SSH Public key to the cluster.

43. Click the 'Continue' button.

44. Click the 'Browse' button.
45. Click the file 'svctest.pub'.
46. Click 'Open'.

47. In the ID field, type 'SVC2'. This field is case sensitive.
48. Click the 'Add Key' button.

The Add SSH Public Key screen acknowledges that it has added a new SSH administrator key associated with ID **SVC2**.

49. Click the 'Continue' button.

You have now completed the cluster configuration, with only 1 node (the configuration node) in the cluster. To be a fully functional SVC cluster, a second node needs to be added to the configuration. Adding the second node requires you to access the SVC cluster using the PuTTY application. However, before you can access the cluster, you must first upload the Private SSH key. Once the private key has been added, you will have command line access to the cluster and can add the second node (or any additional nodes).

50. Click the 'Start Menu'.
51. Click 'Programs'.
52. Click 'PuTTY'.
53. Click 'PuTTY'.

In order to be able to login to the SVC cluster via the PuTTY application, you will need to upload the Private SSH key. This screen will allow you to upload the private key and save your session. You will then be able to use the PuTTY SSH shell to add the other nodes to the cluster.

54. In the Host Name field, type '9.42.164.123'.
55. Tab to the Saved Session field, and type 'svctest'.
56. Click 'Auth' from the Category list on the left.
57. Click the 'Browse' button.
58. Click the 'svctest.ppk' file.
59. Click 'Open'.
60. Click 'Session' from the Category list.
61. Click the 'Save' button.
62. Click the 'Open' button.

The PuTTY SSH shell window is displayed. Login as admin to access the SVC cluster and add the second node. The first step is to determine what additional nodes are available to add by using the command: **svcinfo lsnodecandidate**.

63. Type 'admin' and press the Enter key.
64. At the prompt, type 'svcinfo lsnodecandidate'
65. Press Enter.

You can see that there is one node available to add. Follow the instructions to add the second node.

66. At the prompt, type 'svctask addnode -panelname 000359 -iogrp 0 - name node2'.
67. Press Enter.

You can see that node 2 was added successfully. To list the nodes in the cluster, use the command: **svcinfo lsnode**

68. At the Prompt, type 'svcinfo lsnode'.
69. Press Enter.

The PuTTY screen now displays the two nodes in the cluster.

70. Click the browser window to bring it back into focus.

From the Action pane of the IBM TotalStorage SAN Volume Controller – Web Interface browser screen, you can view information about the cluster or nodes, modify the IP addresses and set the time and date stamp for the cluster.

71. Click 'Display VPD' from the Action menu on the left of the window.
72. Click the 'Display Cluster VPD' button.

The vital product data for the cluster is now displayed.

73. Click the 'Modify IP Addresses' link.

You will not be changing any of the IP addresses in this lab. However, this is the screen you would use to modify the IP addresses of the cluster, if necessary.

74. Click 'Set Cluster Time' from the Action menu on the left of the window.

This screen allows you to confirm and adjust the time and date settings.

75. Close the browser by clicking the X in the upper right corner of the browser window.
76. Close the PuTTY window by clicking the X in the upper right corner of the window.
77. Click the 'OK' button.

Congratulations! You have completed this lab.