# SuSE pacemaker CLuster setup

## Instructions for Engineer

This activity should take 180 minutes to complete.

## How to install & Configure SuSE Pacemaker cluster

The below tasks will be followed to install & configure SuSE Pacemaker cluster.

| # | Step | Notes | Elapsed Time checkpoint |
| --- | --- | --- | --- |
| 1 | Ensure Admin Privileges | Admin Privileges are required to execute tasks. |  |
| 2 | Cluster Installation | 1. Update SLES on node1, node2   sudo zypper update     1. Install component, needed for cluster resources on node1, node2   sudo zypper in socat     1. Install azure-lb component, needed for cluster resources on node1, node2    sudo zypper in resource-agents    Note Check the version of package resource-agents and make sure the minimum version requirements are met:   * For SLES 12 SP4/SP5, the version must be at least resource-agents-4.3.018.a7fb5035-3.30.1. * For SLES 15/15 SP1, the version must be at least resource-agents-4.3.0184.6ee15eb2-4.13.1.      1. Configure the operating system on node1, node2   In some cases, Pacemaker creates many processes and thereby exhausts the allowed number of processes. In such a case, a heartbeat between the cluster nodes might fail and lead to failover of your resources. We recommend increasing the maximum allowed processes by setting the following parameter.    # Edit the configuration file  sudo vi /etc/systemd/system.conf    # Change the DefaultTasksMax  #DefaultTasksMax=512  DefaultTasksMax=4096    #and to activate this setting  sudo systemctl daemon-reload    # test if the change was successful  sudo systemctl --no-pager show | grep DefaultTasksMax    Reduce the size of the dirty cache. For more information, see [Low write performance on SLES 11/12 servers with large RAM](https://www.suse.com/support/kb/doc/?id=7010287).    sudo vi /etc/sysctl.conf    # Change/set the following settings  vm.dirty\_bytes = 629145600  vm.dirty\_background\_bytes = 314572800     1. Configure cloud-netconfig-azure for HA Cluster on node1, node2     Note Check the installed version of package **cloud-netconfig-azure** by running **zypper info cloud-netconfig-azure**. If the version in your environment is 1.3 or higher, it is no longer necessary to suppress the management of network interfaces by the cloud network plugin. If the version is lower than 1.3, we suggest to update package **cloud-netconfig-azure** to the latest available version.    Change the configuration file for the network interface as shown below to prevent the cloud network plugin from removing the virtual IP address (Pacemaker must control the VIP assignment). For more information, see [SUSE KB 7023633](https://www.suse.com/support/kb/doc/?id=7023633).    # Edit the configuration file  sudo vi /etc/sysconfig/network/ifcfg-eth0    # Change CLOUD\_NETCONFIG\_MANAGE  # CLOUD\_NETCONFIG\_MANAGE="yes"  CLOUD\_NETCONFIG\_MANAGE="no"     1. Enable ssh access on node1     sudo ssh-keygen    # Enter file in which to save the key (/root/.ssh/id\_rsa): -> Press ENTER  # Enter passphrase (empty for no passphrase): -> Press ENTER  # Enter same passphrase again: -> Press ENTER    # insert the public key you copied in the last step into the authorized keys file on the second server  sudo vi /root/.ssh/authorized\_keys    # copy the public key  sudo cat /root/.ssh/id\_rsa.pub     1. Enable ssh access on node2     sudo ssh-keygen    # Enter file in which to save the key (/root/.ssh/id\_rsa): -> Press ENTER  # Enter passphrase (empty for no passphrase): -> Press ENTER  # Enter same passphrase again: -> Press ENTER    # insert the public key you copied in the last step into the authorized keys file on the second server  sudo vi /root/.ssh/authorized\_keys    # copy the public key  sudo cat /root/.ssh/id\_rsa.pub     1. Enable ssh access on node1   # insert the public key you copied in the last step into the authorized keys file on the first server  sudo vi /root/.ssh/authorized\_keys     1. Install Fence agents on node1, node2   sudo zypper install fence-agents    Important If using Suse Linux Enterprise Server for SAP 15, be aware that you need to activate additional module and install additional component, that is prerequisite for using Azure Fence Agent. To learn more about SUSE modules and extensions see [Modules and Extensions explained](https://www.suse.com/documentation/sles-15/singlehtml/art_modules/art_modules.html). Follow the instructions bellow to install Azure Python SDK.    The following instructions on how to install Azure Python SDK are only applicable for Suse Enterprise Server for SAP **15**.   * If you are using Bring-Your-Own-Subscription, follow these instructions     #Activate module PackageHub/15/x86\_64  sudo SUSEConnect -p PackageHub/15/x86\_64  #Install Azure Python SDK  sudo zypper in python3-azure-sdk     * If you are using Pay-As-You-Go subscription, follow these instructions     #Activate module PackageHub/15/x86\_64  zypper ar <https://download.opensuse.org/repositories/openSUSE:/Backports:/SLE-15/standard/> SLE15-PackageHub  #Install Azure Python SDK  sudo zypper in python3-azure-sdk     1. Setup host name resolution on node1, node2   You can either use a DNS server or modify the /etc/hosts on all nodes. This example shows how to use the /etc/hosts file. Replace the IP address and the hostname in the following commands. The benefit of using /etc/hosts is that your cluster becomes independent of DNS, which could be a single point of failures too.    sudo vi /etc/hosts  Insert the following lines to /etc/hosts. Change the IP address and hostname to match your environment    # IP address of the first cluster node  Ip\_node1 node1  # IP address of the second cluster node  Ip\_node2 node2     1. Install Cluster on node1     sudo ha-cluster-init -u    # ! NTP is not configured to start at system boot.  # Do you want to continue anyway (y/n)? y  # /root/.ssh/id\_rsa already exists - overwrite (y/n)? n  # Address for ring0 [10.0.0.6] Press ENTER  # Port for ring0 [5405] Press ENTER  # SBD is already configured to use /dev/disk/by-id/scsi-36001405639245768818458b930abdf69;/dev/disk/by-id/scsi-36001405afb0ba8d3a3c413b8cc2cca03;/dev/disk/by-id/scsi-36001405f88f30e7c9684678bc87fe7bf - overwrite (y/n)? n  # Do you wish to configure an administration IP (y/n)? n     1. **A**dd node2 to cluster     sudo ha-cluster-join    # ! NTP is not configured to start at system boot.  # Do you want to continue anyway (y/n)? y  # IP address or hostname of existing node (e.g.: 192.168.1.1) [] ip\_node1  # /root/.ssh/id\_rsa already exists - overwrite (y/n)? n     1. Change hacluster password to the same password on node1, node2   sudo passwd hacluster     1. Adjust corosync settings on node1, node2     Add the following bold content to the file if the values are not there or different. Make sure to change the token to 30000 to allow Memory preserving maintenance. For more information, see [this article for Linux](https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-and-updates#maintenance-that-doesnt-require-a-reboot) or [Windows](https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-and-updates#maintenance-that-doesnt-require-a-reboot).    **[...]**  **token: 30000**  **token\_retransmits\_before\_loss\_const: 10**  **join: 60**  **consensus: 36000**  **max\_messages: 20**    interface {  [...]  }  transport: udpu  }  nodelist {  node {  ring0\_addr:10.0.0.6  }  node {  ring0\_addr:10.0.0.7  }  }  logging {  [...]  }  quorum {  # Enable and configure quorum subsystem (default: off)  # see also corosync.conf.5 and votequorum.5  provider: corosync\_votequorum  expected\_votes: 2  two\_node: 1  }    Then restart the corosync service    sudo service corosync restart |  |
|  | Default Pacemaker configuration for Azure fence agent | * 1. Enable the use of a STONITH device and set the fence delay on node1   sudo crm configure property stonith-timeout=144  sudo crm configure property stonith-enabled=true     1. # List the resources to find the name of the SBD device   sudo crm resource list  sudo crm resource stop stonith-sbd  sudo crm configure delete stonith-sbd  sudo crm configure primitive stonith-sbd stonith:external/sbd \  params pcmk\_delay\_max="15" \  op monitor interval="15" timeout="15"   1. Execute following commands, if you are using Azure fence agent as STONITH. After assigning roles to both cluster nodes, you can configure the STONITH devices in the cluster.   sudo crm configure property stonith-enabled=true  crm configure property concurrent-fencing=true  # replace the bold string with your subscription ID, resource group of the VM, tenant ID, service principal application ID and password  sudo crm configure primitive rsc\_st\_azure stonith:fence\_azure\_arm \  params subscriptionId="subscription ID" resourceGroup="resource group" tenantId="tenant ID" login="application ID" passwd="password" \  pcmk\_monitor\_retries=4 pcmk\_action\_limit=3 power\_timeout=240 pcmk\_reboot\_timeout=900 pcmk\_host\_map="prod-cl1-0:prod-cl1-0-vm-name;prod-cl1-1:prod-cl1-1-vm-name" \  op monitor interval=3600 timeout=120  sudo crm configure property stonith-timeout=900 |  |
|  | Pacemaker configuration for Azure scheduled events | Azure offers [scheduled events](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/scheduled-events). Scheduled events are provided via meta-data service and allow time for the application to prepare for events like VM shutdown, VM redeployment, etc. Resource agent [**azure-events**](https://github.com/ClusterLabs/resource-agents/pull/1161) monitors for scheduled Azure events. If events are detected, the agent will attempt to stop all resources on the impacted VM and move them to another node in the cluster. To achieve that additional Pacemaker resources must be configured.     1. Make sure the package for the **azure-events** agent is already installed on node1, node2 and up to date     sudo zypper info resource-agents    **2.** Configure the resources in Pacemaker on node1    #Place the cluster in maintenance mode  sudo crm configure property maintenance-mode=true    #Create Pacemaker resources for the Azure agent  sudo crm configure primitive rsc\_azure-events ocf:heartbeat:azure-events op monitor interval=10s  sudo crm configure clone cln\_azure-events rsc\_azure-events    #Take the cluster out of maintenance mode  sudo crm configure property maintenance-mode=false    Note  After you configure the Pacemaker resources for azure-events agent, when you place the cluster in or out of maintenance mode, you may get warning messages like:  WARNING: cib-bootstrap-options: unknown attribute 'hostName\_ **hostname**'  WARNING: cib-bootstrap-options: unknown attribute 'azure-events\_globalPullState'  WARNING: cib-bootstrap-options: unknown attribute 'hostName\_ **hostname**'  These warning messages can be ignored. |  |

# References and information

## REFERENCE DOCUMENTS / LINKS

Below are the links for documents mentioned in this document

|  |  |
| --- | --- |
| **Document Name** | **Microsoft Azure Documentation Link** |
| Setting up Pacemaker on SUSE Linux Enterprise Server in Azure | <https://docs.microsoft.com/en-us/azure/virtual-machines/workloads/sap/high-availability-guide-suse-pacemaker#cluster-installation> |

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Created / Reviewed by | Remarks |
| 1.0 | 10/12/2020 | Sunil.Ramachandra | Initial version created |