CLUSTER OPERATION MANUAL

BDP

(HANA DB)

Version 1.0

Contents

[1 PURPOSE 2](#_Toc92712111)

[2 SCOPE 2](#_Toc92712112)

[3 Prerequisites 2](#_Toc92712113)

[4 INSTANCE CALCULATION 3](#_Toc92712114)

[5 Details 4](#_Toc92712115)

[6 HA Overview 5](#_Toc92712116)

[7 Load Balancer setup 6](#_Toc92712117)

[7.1 Load Balancer Configuration 6](#_Toc92712118)

[7.2 REFERENCE DOCUMENTS / LINKS 14](#_Toc92712119)

[8 Install & Configure SuSE Pacemaker cluster 14](#_Toc92712120)

[8.1 CRM Configuration 22](#_Toc92712121)

[8.2 REFERENCE DOCUMENTS / LINKS 25](#_Toc92712122)

[9 Cluster patching process 26](#_Toc92712123)

[10 HA TEsting 27](#_Toc92712124)

[11 DOCUMENT REVISION HISTORY 27](#_Toc92712125)

# PURPOSE

The purpose of this document is to configure High Availability for HANA DB servers with client technical solution arena for the BHF Project.

# SCOPE

This section brings the scope to configure HA on SUSE Linux servers.

# Prerequisites

Below are the prerequisites for SUSE high availability configuration:

* Make Sure Full server back up in place for both the nodes.
* The cluster must include a valid STONITH method. In our case STONITH device using Azure fence agent, we need to have the detail of the fencing agent configuration.
* Name resolution of the cluster nodes and the virtual IP address must resolve on all cluster nodes.

# INSTANCE CALCULATION

|  |  |
| --- | --- |
| HN | Instance Number |

  For HANA DB (HN-02)

SAP HANA 2.0 - system database

|  |  |
| --- | --- |
| **Instance** | S/4HANA  BDP |
| 3HN13 | 30213 |
| 3HN14 | 30214 |
| 625HN (Probe) | 62502 |

SAP HANA 2.0 -tenant database (02)

|  |  |
| --- | --- |
| **Instance** | S/4HANA BDP |
| 3HN40 | 30240 |
| 3HN41 | 30241 |
| 3HN42 | 30242 |
| 625HN (Probe) | 62502 |

# Details

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Component** | | | | | | **Hostname Name** | | | | | **IP Address** | | | | | | **SID** | | | | | **Comments** | | | | | |
| SAP BusinessObjects Data Services on HANA (HANA DB ) | | | | | | bdpdb01use2pr | | | | | 10.213.32.135 | | | | | | BDP | | | | | VM - Physical IP | | | | | |
| SAP BusinessObjects Data Services on HANA (HANA DB ) | | | | | | bdpdb02use2pr | | | | | 10.213.32.137 | | | | | | BDP | | | | | VM - Physical IP | | | | | |
| SAP BusinessObjects Data Services on HANA (HANA DB ) - VIP 1 | | | | | | sapbdpdb01pr | | | | | 10.213.32.136 | | | | | | BDP | | | | | Virtual IP 1 | | | | | |
| SAP BusinessObjects Data Services on HANA (HANA DB ) - VIP 2 | | | | | | sapbdpdb02pr | | | | | 10.213.32.138 | | | | | | BDP | | | | | Virtual IP 2 | | | | | |
| SAP BusinessObjects Data Services on HANA (HANA DB ) - VIP 3 | | | | | | sapbdpdb03pr | | | | | 10.213.32.183 | | | | | | BDP | | | | | Load Balancer Front End IP | | | | | |
| **Load balancer** | | | | |  | | | | |  | | | | |  | | | | | |  | | | | |  | |
| Name | | | | | SKU | | | | | Frontend IP | | | | | Backend pool | | | | | | Health probe | | | | | Load balancing rule | |
| sap-ilb-bdpdb-use2-pr-01 | | | | | Standard | | | | | BDP\_FRONTEND | | | | | BDP-BKP-Pool01 | | | | | | BDP-HEALTH01 | | | | | BDP-LB01 | |
|  | | | | |  | | | | |
| **Backend pool** | | | | | | |  | | | | |  | | | | | |  | | | | |  | | | | |
| Name | | | | | | | IP version | | | | | VM | | | | | | NIC | | | | | IP address | | | | |
| BDP-BKP-Pool01 | | | | | | | IPv4 | | | | | bdpdb01use2pr | | | | | | bdpdb01use2pr\_nic01 | | | | | 10.213.32.136 | | | | |
| bdpdb02use2pr | | | | | | bdpdb02use2pr\_nic01 | | | | | 10.213.32.138 | | | | |
| **Health probe** | | | | | | | |  | | | | |  | | | | | |  | | | | |  | | | |
| Name | | | | | | | | Protocol | | | | | Port | | | | | | Interval | | | | | Unhealthy threshold | | | |
| BDP-HEALTH01 | | | | | | | | TCP | | | | | 62502 | | | | | | 5 | | | | | 2 | | | |
| **Load balancing rule** | |  |  |  | | | | |  | | | | |  | |  | | | |  | | | | |  | |  |
| Name | IP version | Frontend IP | Protocol | Port | | | | | Backend Port | | | | | Backend pool | | Health probe | | | | Session persistence | | | | | Idle timeout | | Floating IP |
| BDP-LB01 | IPv4 | BDP\_FRONTEND | TCP | 62502 | | | | | - | | | | | BDP-BKP-Pool01 | | BDP-HEALTH01 | | | | Client IP and Protocol | | | | | 30 | | Enable |

# HA Overview



# Load Balancer setup

## Load Balancer Configuration

The below tasks will be followed to configure Load Balancer for BDP.

| # | Step | Notes |
| --- | --- | --- |
| 1 | Ensure Contributor Privileges | Contributor Privileges on Azure subscription is required to execute tasks. |
| 2 | Load Balancer Configuration | 1.Create load balancer (internal, standard) |
|  |  | 1. Create the frontend IP address |
| 3 | Create the backend pool | 1. Create the backend pool 2. Open the load balancer, select backend pools, and click Add 3. Enter the name of the new backend pool      1. Click Add |
| 4 | Create the health probes | 1. Create the health probes    1. Port 62502       1. Open the load balancer, select health probes, and click Add       2. Enter the name of the new health probe       3. Select TCP as protocol, port 62502, keep Interval 5 and Unhealthy threshold 2       4. Click OK |
| 5 | Load-balancing rules | 1. Load-balancing rules    1. Create a rule       1. Open the load balancer, select Load-balancing rules and click Add       2. Enter the name of the new load balancer rule       3. Select the frontend IP address, backend pool, and health probe you created earlier       4. Select HA ports       5. Make sure to enable Floating IP       6. Click OK |

## REFERENCE DOCUMENTS / LINKS

Below are the links for documents mentioned in this document

|  |  |
| --- | --- |
| **Document Name** | **Microsoft Azure Documentation Link** |
| Deploy Azure Load Balancer manually via Azure portal | <https://docs.microsoft.com/en-us/azure/virtual-machines/workloads/sap/high-availability-guide-suse-netapp-files#deploy-azure-load-balancer-manually-via-azure-portal> |

# Install & Configure SuSE Pacemaker cluster

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

| # | Step | Notes |
| --- | --- | --- |
| 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. |

## CRM Configuration

|  |  |
| --- | --- |
| **Step** | **Notes** |
| # crm config show | node 1: bdpdb01use2pr \  attributes azName=bdpdb01use2pr hana\_bhp\_srmode=sync hana\_bhp\_site=SITE1 hana\_bhp\_op\_mode=logreplay lpa\_bhp\_lpt=1640330012 hana\_bhp\_vhost=sapbdpdb01pr hana\_bhp\_remoteHost=sapbdpdb02pr standby=off  node 2: bdpdb02use2pr \  attributes azName=bdpdb02use2pr lpa\_bhp\_lpt=30 hana\_bhp\_site=SITE2 hana\_bhp\_srmode=sync hana\_bhp\_op\_mode=logreplay hana\_bhp\_remoteHost=sapbdpdb01pr hana\_bhp\_vhost=sapbdpdb02pr standby=off  primitive nc\_BHP\_HDB02 azure-lb \  params port=62502 \  meta resource-stickiness=0  primitive rsc\_SAPHanaTopology\_BHP\_HDB02 ocf:suse:SAPHanaTopology \  operations $id=rsc\_sap2\_BHP\_HDB02-operations \  op monitor interval=10 timeout=600 \  op start interval=0 timeout=600 \  op stop interval=0 timeout=300 \  params SID=BHP InstanceNumber=02  primitive rsc\_SAPHana\_BHP\_HDB02 ocf:suse:SAPHana \  operations $id=rsc\_sap\_BHP\_HDB02-operations \  op start interval=0 timeout=3600 \  op stop interval=0 timeout=3600 \  op promote interval=0 timeout=3600 \  op monitor interval=60 role=Master timeout=700 \  op monitor interval=61 role=Slave timeout=700 \  params SID=BHP InstanceNumber=02 PREFER\_SITE\_TAKEOVER=true DUPLICATE\_PRIMARY\_TIMEOUT=7200 AUTOMATED\_REGISTER=True  primitive rsc\_azure-events azure-events \  op monitor interval=10s  primitive rsc\_ip\_BHP\_HDB02 IPaddr2 \  meta target-role=Started \  operations $id=rsc\_ip\_BHP\_HDB02-operations \  op monitor interval=10s timeout=20s \  params ip=10.213.32.183  primitive rsc\_st\_azure stonith:fence\_azure\_arm \  params subscriptionId=94d6ed7c-2ce4-4292-b7a1-aa60e5aab40a resourceGroup=sap-rg-bdp-use2-pr tenantId=2658e698-ac38-4347-a56f-3f96a6bfa8ff login=570ed24c-105d-400b-a83e-6fd8043b19ea passwd="\*\*\*\*\*\*" pcmk\_monitor\_retries=4 pcmk\_action\_limit=3 power\_timeout=240 pcmk\_reboot\_timeout=900 \  op monitor interval=3600 timeout=120 \  meta target-role=Started  group g-primary rsc\_ip\_BHP\_HDB02 nc\_BHP\_HDB02  ms msl\_SAPHana\_BHP\_HDB02 rsc\_SAPHana\_BHP\_HDB02 \  meta notify=true clone-max=2 clone-node-max=1 targetrole=Started interleave=true target-role=Started  clone cln\_SAPHanaTopology\_BHP\_HDB02 rsc\_SAPHanaTopology\_BHP\_HDB02 \  meta clone-node-max=1 target-role=Started interleave=true  clone cln\_azure-events rsc\_azure-events  colocation col\_saphana\_ip\_BHP\_HDB02 4000: g-primary:Started msl\_SAPHana\_BHP\_HDB02:Master  order ord\_SAPHana\_BHP\_HDB02 Optional: cln\_SAPHanaTopology\_BHP\_HDB02 msl\_SAPHana\_BHP\_HDB02  property SAPHanaSR: \  hana\_bhp\_site\_srHook\_SITE2=SOK \  hana\_bhp\_site\_srHook\_sapbdpdb01dr=SFAIL \  hana\_bhp\_site\_srHook\_SITE3=SFAIL \  hana\_bhp\_site\_srHook\_SITE1=PRIM  property cib-bootstrap-options: \  have-watchdog=false \  dc-version="1.1.19+20181105.ccd6b5b10-3.28.1-1.1.19+20181105.ccd6b5b10" \  cluster-infrastructure=corosync \  cluster-name=hacluster \  stonith-enabled=true \  maintenance-mode=false \  placement-strategy=default \  no-quorum-policy=stop \  stonith-timeout=300s \  last-lrm-refresh=1640243969 \  startup-fencing=true \  concurrent-fencing=true \  hostName\_bdpdb01use2pr=bdpdb01use2pr \  azure-events\_globalPullState=IDLE \  hostName\_bdpdb02use2pr=bdpdb02use2pr  rsc\_defaults rsc-options: \  resource-stickiness=1000 \  migration-threshold=5000  op\_defaults op-options: \  timeout=600 \  record-pending=true |
| # crm stat  On node 1 |  |
| # crm stat  On node 2 |  |

## 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> |

# Cluster patching process

**If it’s a cluster server follow the below steps (before rebooting) for OS(Linux) patch installation**   
Additional application server was stopped. Basis has performed application checks after stopping additional app server which was working fine.

1. IO team will place the Cluster in maintenance mode
2. Login to Secondary Node and validate the cluster roles are running on the primary node.
3. Install OS patches on the Secondary Node and reboot the Secondary Node.
4. Once the Secondary Node is up and running fine, perform server sanity health checks.
5. Login to primary Node and switch the cluster role to secondary node.
6. Install OS patches on the primary Node and reboot the primary Node.
7. Once the primary Node is up and running fine, perform server sanity health checks.
8. Login to Secondary Node and switch the cluster role to primary node. Login to primary and validate cluster roles are running file.
9. Inform Application team and Database Team to perform application availability\functionality test.
10. IO team will remove the cluster from maintenance mode post application team confirmation

To perform any changes to the CRM config or maintenance work, Run the following commands on one of the Pacemaker cluster nodes

crm configure property maintenance-mode = "true"

Execute the below command to disable Maintenance mode.

crm configure property maintenance-mode = "false"

Please follow the below steps to patch the server

zypper update -y (To install the update)

Once patches installed please Reboot the server, you can do it on terminal by using init 6/reboot commands or in Azure portal by using restart option

#reboot

Once patching has been completed successfully and servers is Up. Please take post checks

#zypper lu

#zypper pchk

#rpm -qa --last | more (Please take 1st page screenshot)

# HA TEsting

# DOCUMENT REVISION HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Date** | **Author** | **Reason / Change Description** |
| 1.0 |  |  | Initial Document |
|  |  |  |  |