CLUSTER OPERATION MANUAL

FIP

(ASCS & ERS)

Version 1.0

Contents

[1 PURPOSE 2](#_Toc92310135)

[2 SCOPE 2](#_Toc92310136)

[3 Prerequisites 2](#_Toc92310137)

[3.1.1 Create Azure Fence agent STONITH device 2](#_Toc92310138)

[4 INSTANCE CALCULATION 4](#_Toc92310139)

[5 HA details 5](#_Toc92310140)

[6 HA Overview 6](#_Toc92310141)

[7 Load Balancer setup 7](#_Toc92310142)

[7.1 Load Balancer Configuration 7](#_Toc92310143)

[7.2 REFERENCE DOCUMENTS / LINKS 13](#_Toc92310144)

[8 Install & Configure SuSE Pacemaker cluster 14](#_Toc92310145)

[8.1 CRM Configuration 22](#_Toc92310146)

[8.2 REFERENCE DOCUMENTS / LINKS 25](#_Toc92310147)

[9 Cluster patching process 26](#_Toc92310148)

[10 HA TEsting 27](#_Toc92310149)

[11 DOCUMENT REVISION HISTORY 27](#_Toc92310150)

# PURPOSE

The purpose of this document is to configure High Availability on servers using Azure NetApp Files 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.
* SAP NetWeaver requires shared storage for the transport and profile directory. In our case, we will deploy Azure Net app Files resources.
* 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.

### Create Azure Fence agent STONITH device

The STONITH device uses a Service Principal to authorize against Microsoft Azure. Follow these steps to create a Service Principal.

1. Go to [https://portal.azure.com](https://portal.azure.com/)
2. Open the Azure Active Directory blade  
   Go to Properties and write down the Directory ID. This is the **tenant ID**.
3. Click App registrations
4. Click New Registration
5. Enter a Name, select "Accounts in this organization directory only"
6. Select Application Type "Web", enter a sign-on URL (for example [http://localhost](http://localhost/)) and click Add.  
   The sign-on URL is not used and can be any valid URL
7. Select Certificates and Secrets, then click New client secret
8. Enter a description for a new key, select "Never expires" and click Add
9. Write down the Value. It is used as the **password** for the Service Principal
10. Select Overview. Write down the Application ID. It is used as the username of the Service Principal.

#### Create a custom role for the fence agent

The Service Principal doesn't have permissions to access your Azure resources by default. You need to give the Service Principal permissions to start and stop (deallocate) all virtual machines of the cluster. If you did not already create the custom role, you can create it using [PowerShell](https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-powershell#create-a-custom-role) or [Azure CLI](https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-cli)

Use the following content for the input file. You need to adapt the content to your subscriptions that is, replace c276fc76-9cd4-44c9-99a7-4fd71546436e and e91d47c4-76f3-4271-a796-21b4ecfe3624 with the Ids of your subscription. If you only have one subscription, remove the second entry in AssignableScopes.

JSON

{

"Name": "Linux Fence Agent Role",

"description": "Allows to power-off and start virtual machines",

"assignableScopes": [

"/subscriptions/e663cc2d-722b-4be1-b636-bbd9e4c60fd9",

"/subscriptions/e91d47c4-76f3-4271-a796-21b4ecfe3624"

],

"actions": [

"Microsoft.Compute/\*/read",

"Microsoft.Compute/virtualMachines/powerOff/action",

"Microsoft.Compute/virtualMachines/start/action"

],

"notActions": [],

"dataActions": [],

"notDataActions": []

}

#### Assign the custom role to the Service Principal

Assign the custom role "Linux Fence Agent Role" that was created in the last chapter to the Service Principal. Do not use the Owner role anymore! For detailed steps, see [Assign Azure roles using the Azure portal](https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal).

Make sure to assign the role for both cluster nodes.

#### Client Specific details

subscriptionId=94d6ed7c-2ce4-4292-b7a1-aa60e5aab40a

resourceGroup=Resource group name

tenantId=2658e698-ac38-4347-a56f-3f96a6bfa8ff

login=570ed24c-105d-400b-a83e-6fd8043b19ea

passwd="Ko.7Q~ZAylTj8Fgo4LbpIR85zqyRJcImGsiLF"

# INSTANCE CALCULATION

|  |  |
| --- | --- |
| NN | ASCS Instance Number |
| EE | ERS Instance Number |

* If using Standard Load Balancer, select **HA ports**
* If using Basic Load Balancer, create Load balancing rules for the following ports

For ASCS (NN-01) and ERS (EE-10):

|  |  |
| --- | --- |
| **Instance** | System |
| 32NN | 3201 |
| 36NN | 3601 |
| 39NN | 3901 |
| 81NN | 8101 |
| 5NN13 | 50113 |
| 5NN14 | 50114 |
| 5NN16 | 50116 |
| 32EE | 3210 |
| 33EE | 3310 |
| 5EE13 | 51013 |
| 5EE14 | 51014 |
| 5EE16 | 51016 |
| 620NN, 621EE (Probe) | 62001, 62110 |

# HA details

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Component** | | | | | | | | | | | **Hostname Name** | | | | | **IP Address** | | | | **SID** | **Comments** | | | | | | | |
| Fiori for S/4HANA On-Premise Edition (ASCS ) | | | | | | | | | | | fipcs01use2pr | | | | | 10.213.34.31 | | | | FIP | VM - Physical IP | | | | | | | |
| Fiori for S/4HANA On-Premise Edition (ERS ) | | | | | | | | | | | fipcs02use2pr | | | | | 10.213.34.33 | | | | FIP | VM - Physical IP | | | | | | | |
| Fiori for S/4HANA ASCS VIP 1 - ASCS | | | | | | | | | | | sapfipcs01pr | | | | | 10.213.34.32 | | | | FIP | Load Balancer Front End IP | | | | | | | |
| Fiori for S/4HANA ASCS VIP 2 - ERS | | | | | | | | | | | sapfipcs02pr | | | | | 10.213.34.34 | | | | FIP | Load Balancer Front End IP | | | | | | | |
| Fiori for S/4HANA APP VIP 3 - PAS | | | | | | | | | | | sapfipap01pr | | | | | 10.213.34.90 | | | | FIP | Virtual IP 1 | | | | | | | |
| Fiori for S/4HANA APP VIP 4 - AAS | | | | | | | | | | | sapfipap02pr | | | | | 10.213.34.91 | | | | FIP | Virtual IP 2 | | | | | | | |
| **Load balancer** | | |  | | | | |  | | | | | |  | | | | |  | | | |  | |  |
| **Name** | | | **SKU** | | | | | **Frontend IP** | | | | | | **Backend pool** | | | | | **Health probe** | | | | **Load balancing rule** | | **NAT rule** |
| sap-ilb-fipapp-use2-pr-01 | | | Standard | | | | | FIPP\_ASCS\_FrontendIP01 | | | | | | FIP-BKP-Pool01 | | | | | FIP-HEALTH01 | | | | FIP-LB01 | | - |
| FIP\_ERS\_FronendIP01 | | | | | | FIP-HEALTH02 | | | | FIP-LB02 | | - |
| **Backend pool** | |  | | | |  | | |  | | | | | |  | | |
| **Name** | | **IP version** | | | | **VM** | | | **NIC** | | | | | | **IP address** | | |
| FIP-BKP-Pool01 | | IPv4 | | | | fipcs01use2pr | | | fipcs01use2pr\_nic01 | | | | | | 10.213.34.31 | | |
| fipcs02use2pr | | | fipcs02use2pr\_nic01 | | | | | | 10.213.34.33 | | |
| **Health probe** |  | | | |  | |  | | |  | | | | | | |
| **Name** | **Protocol** | | | | **Port** | | **Interval** | | | **Unhealthy threshold** | | | | | | |
| FIP-HEALTH01 | TCP | | | | 62001 | | 5 | | | 2 | | | | | | |
| FIP-HEALTH02 | TCP | | | | 62110 | | 5 | | | 2 | | | | | | |
| **Loadbalancingrule** |  | | |  | | | | | | | |  |  | | | | |  | | | |  | |  | |  |  |  | |
| **Name** | **IP version** | | | **Frontend IP** | | | | | | | | **Protocol** | **HA Port** | | | | | **Backend Port** | | | | **Backend pool** | | **Health probe** | | **Session persistence** | **Idle timeout** | **Floating IP** | |
| FIP-LB01 | IPv4 | | | FIPP\_ASCS\_FrontendIP01 | | | | | | | | TCP | Selected | | | | | 62001 | | | | FIP-BKP-Pool01 | | FIP-HEALTH01 | | Client IP and Protocol | 30 | Enable | |
| FIP-LB02 | IPv4 | | | FIP\_ERS\_FronendIP01 | | | | | | | | TCP | Selected | | | | | 62110 | | | | FIP-BKP-Pool01 | | FIP-HEALTH02 | | 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 FIP.

| # | 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 addresses for ASCS      1. Create the frontend IP addresses for ERS |
| 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 62001 for ASCS       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 62001, keep Interval 5 and Unhealthy threshold 2       4. Click OK      * 1. Port 62110 for ERS |
| 5 | Load-balancing rules | 1. Load-balancing rules    1. Create a rule for the ASCS       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 for ASCS, backend pool, and health probe you created earlier       4. Select HA ports       5. Make sure to enable Floating IP       6. Click OK      * Repeat the steps above to create load balancing rules for ERS |

## 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: fipcs01use2pr \  attributes azName=fipcs01use2pr standby=off  node 2: fipcs02use2pr \  attributes standby=off azName=fipcs02use2pr  primitive fs\_FIP\_ASCS01 Filesystem \  params device="10.213.32.103:/ascsers-use2-pr/FIP/ASCS" directory="/usr/sap/FIP/ASCS01" fstype=nfs options="sec=sys,vers=4.1" \  op start timeout=60s interval=0 \  op stop timeout=60s interval=0 \  op monitor interval=20s timeout=40s  primitive fs\_FIP\_ERS10 Filesystem \  params device="10.213.32.103:/ascsers-use2-pr/FIP/ERS" directory="/usr/sap/FIP/ERS10" fstype=nfs options="sec=sys,vers=4.1" \  op start timeout=60s interval=0 \  op stop timeout=60s interval=0 \  op monitor interval=20s timeout=40s  primitive nc\_FIP\_ASCS01 azure-lb \  params port=62001  primitive nc\_FIP\_ERS10 azure-lb \  params port=62110  primitive rsc\_azure-events azure-events \  op monitor interval=10s  primitive rsc\_sap\_FIP\_ASCS01 SAPInstance \  operations $id=rsc\_sap\_FIP\_ASCS01-operations \  op monitor interval=11 timeout=60 on-fail=restart \  params InstanceName=FIP\_ASCS01\_sapfipcs01pr START\_PROFILE="/sapmnt/FIP/profile/FIP\_ASCS01\_sapfipcs01pr" AUTOMATIC\_RECOVER=false \  meta resource-stickiness=5000 failure-timeout=60 migration-threshold=1 priority=10 target-role=Started  primitive rsc\_sap\_FIP\_ERS10 SAPInstance \  operations $id=rsc\_sap\_FIP\_ERS10-operations \  op monitor interval=11 timeout=60 on-fail=restart \  params InstanceName=FIP\_ERS10\_sapfipcs02pr START\_PROFILE="/sapmnt/FIP/profile/FIP\_ERS10\_sapfipcs02pr" AUTOMATIC\_RECOVER=false IS\_ERS=true \  meta priority=1000 target-role=Started  primitive rsc\_st\_azure stonith:fence\_azure\_arm \  params subscriptionId=94d6ed7c-2ce4-4292-b7a1-aa60e5aab40a resourceGroup=sap-rg-fip-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  primitive vip\_FIP\_ASCS01 IPaddr2 \  params ip=10.213.34.32 cidr\_netmask=24 nic=eth0 \  op monitor interval=10 timeout=20  primitive vip\_FIP\_ERS10 IPaddr2 \  params ip=10.213.34.34 cidr\_netmask=24 nic=eth0 \  op monitor interval=10 timeout=20  group SAP-FIP\_ASCS01 fs\_FIP\_ASCS01 nc\_FIP\_ASCS01 vip\_FIP\_ASCS01 rsc\_sap\_FIP\_ASCS01 \  meta resource-stickiness=3000  group SAP-FIP\_ERS10 fs\_FIP\_ERS10 nc\_FIP\_ERS10 vip\_FIP\_ERS10 rsc\_sap\_FIP\_ERS10  clone cln\_azure-events rsc\_azure-events  colocation col\_sap\_FIP\_no\_both -5000: SAP-FIP\_ERS10 SAP-FIP\_ASCS01  order ord\_sap\_FIP\_first\_start\_ascs Optional: rsc\_sap\_FIP\_ASCS01:start rsc\_sap\_FIP\_ERS10:stop symmetrical=false  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 \  no-quorum-policy=ignore \  stonith-timeout=150s \  startup-fencing=true \  hostName\_fipcs01use2pr=fipcs01use2pr \  hostName\_fipcs02use2pr=fipcs02use2pr \  azure-events\_globalPullState=IDLE \  last-lrm-refresh=1634208646  rsc\_defaults rsc-options: \  resource-stickiness=1 \  migration-threshold=3  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

Please follow the below steps to patch the server

Lock the python-azure-mgmt-compute package as there is a dependency for cluster (python-azure-mgmt-compute-4.6.2-2.6.3.noarch is required)

# rpm -qa | grep compute\*

# zypper addlock python-azure-mgmt-compute

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)

**If it’s a cluster server follow the below steps (before rebooting) for OS(Linux) patch installation**

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

# HA TEsting

# DOCUMENT REVISION HISTORY

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