Service Category: EC2 or VMs

Issue Description&Cause of the Issue:

EC2 instance failed to start when changing the instance state Server.

InternalError: Internal error on launch during starting an instance.

Resolution proposed/employed:

Step 1: Detach the attached EBS volumes (excluding the Root volume) and then try starting the instance.

Step 2: If it fails to start, take AMI of that instance and launch it again.

Step 3: Take snapshots of the detached EBS volumes and create the volume again.

Step 4: Attach the re-created EBS volumes to the re-launched instance and then start the instance.

Service/resource category : Storage : EBS, S3 & EFS

Issue Description&Cause of the Issue: EBS storage full- partition increase required

EBS storage full

Resolution proposed/employed:

step 1: cmd: df -h ,

step 2: cmd: lsblk -o +SERIAL (you will get voiume ids),

step 3: increase those EBS Ids - volume,

step 4: sudo xfs_growfs -d /path/ (*for ext 4 partitions)

Service/resource category :EC2 or VMs

Issue Description&Cause of the Issue: Instances failed to auto-start as scheduled

One or more instances failed to start due to 'Insufficient Capacity' error, due to unavailability of specific instance type on demand by AWS.

Resolution proposed/employed:

Step 1: Change the instance type of unavailable instance/s to the respective higher or equivalent type while it is in stopped state. (Note: This is a temporary solution. Moving the instance into a

different AZ could also be considered.)

Step 2: Start the instances manually.

Step 3: Change the instance type back to the initial one when all the servers have been stopped and monitor the auto start closely before the scheduled start time. (Steps 1-3 may need to be

repeated.)

Service/resource category : Storage : SAP Router

Issue Description&Cause of the Issue: SAP disconnects within 5 mins of activity.

SAPRouter Idle session timeout value issue. ClientAliveInterval set to default of 3 mins in Linux Instance.

Resolution proposed/employed:

Step 1: sudo vi /etc/ssh/sshd_config.

Step 2: Timeout value = ClientAliveInterval * ClientAliveCountMax. Increase the ClientAliveInterval time to the required time.

Step 3: sudo systemctl reload sshd

Service/resource category: EC2 or VMs

Issue Description&Cause of the Issue: EC2 instance failed to start/reboot and unable to connect to the server. Error or missed entry in /etc/fstab file.

Resolution proposed/employed:

Step 1: Stop the faulty instance A.

Step 2: Detach the root volume of instance A.

Step 3: Launch a new instance B in the same region & same AZ.

Step 4: Attach the root volume of A as an additional volume to instance B.

Step 5: Login to instance B and mount the root volume of A and edit the /etc/fstab file: cmd:

```
mkdir /repair

      mount  /dev/xvdf1  /repair  OR mount -o nouuid /dev/xvdf1  /repair        cd /repair
vi /etc/fstab        cd
```

Step 6: Unmount the root volume of A and detach it from instance B.

Step 7: Re-attach the volume back to instance A.

Service/resource category:EC2 or VMs

Issue Description&Cause of the Issue: Data not getting collected in CloudWatch metrics. 0/2 server Status checks for the instance.

Resolution proposed/employed:

Step 1: Ask client approval for server reboot.

Step 2: Reboot the server during the mentioned time by the client.

Step 3: If reboot doesn't help, stop and then start the server.

User login & Permissions

User login issue User login issue

1) Open Server Manager

2) Open Computer Management from Tools

3) Local users and groups

4) Select the user and open properties

5) Select Member of and add Remote Desktop Users and click ok

Service/resource category: Patching

Issue Description&Cause of the Issue: SLES 15 patching issue with Docker, mozilla version, License agreement issue

SLES 15 patching issue with Docker, mozilla vsersion, License agrrement issue

Resolution proposed/employed:

1) Select the ec2 instance and click on connect

2) In the CLI console type sudo su

3) execute this command "zypper update docker-libnetwork" to update docker lib

4) execute this command "zypper update mozilla-nss" to update mozilla

5) Open the file cat /etc/zypp/zypper.conf file and set autoAgreementWithLicense=yes

Service/resource category: Patching

Issue Description&Cause of the Issue:

SLES 12 patching issue with Python version

SLES 12 patching issue with Python version

Resolution proposed/employed:

1) check python version : rpm -qa python-PyYAML
2) If the verson is 3.12 then update the version using : zypper update python-PyYAML

Service/resource category: User login & Permissions

Issue Description&Cause of the Issue:

Informatica server user login issue

Informatica server user login issue

Resolution proposed/employed:

1) Open Server Manager
2) Open Computer Management from Tools
3) Local users and groups
4) Add new user
5) Select Member of and add the necessary permission

Service/resource category: Patching

Issue Description&Cause of the Issue:

TOSCA server patching issue due to low storage TOSCA server patching issue due to low storage

Resolution proposed/employed:

1) Open AWS Management Console
2) Click on EC2 services
3) Click on EBS Volumes
4) Select the EBS Volume and extend the size

Service/resource category: User login & Permissions

Issue Description&Cause of the Issue:

Enable MFA for Open VPN - Jira Enable MFA for Open VPN - Jira

Resolution proposed/employed:

Step 1: Login to open vpn server

Step 2: Add enforce MFA policies with user group policy

Step 3: Add user to the group.

Service/resource category: User login & Permissions

Issue Description&Cause of the Issue:

AWS Instance Scheduler Configuration   To start and stop instances on a particular time window

Resolution proposed/employed:

Step 1: Login to the server

Step 2: Go to Lambda function with boto3 script

Step 3: Add cronjob expression to schedule it in a particular time frame and add the lamda function

Service/resource category:

User login & Permissions

Issue Description&Cause of the Issue:

Not authorized to see Amazon support portal.Not authorized to see Amazon support portal

Resolution proposed/employed:

Step 1: Login to the server

Step 2: Go to IAM role

Step 3: add the user to user group and enable MFA

Step 4: Configure MFA on personal devices

Step 5: Login with MFA

Service/resource category: RDP

Issue Description&Cause of the Issue:

RDP connection Remote Access (RDP) for the 5 TOSCA Agents on AWS

Remote Access (RDP) for the 5 TOSCA Agents on AWS

Resolution proposed/employed:

1) Open Server Manager

2) Open Computer Management from Tools

3) Local users and groups

4) Select the user and open properties

5) Select Member of and add Remote Desktop Users and click ok

Service/resource category: User login & Permissions

Issue Description&Cause of the Issue:

Install components for SDI (User Creation) Install components for SDI (User Creation)

Resolution proposed/employed:

Step 1: Login to the linux server

step 2: Login as root

step 3: create a new user

step 4: set the password

Step 5: cat etc/passwd --> add group id

Service/resource category: Backups - AMI &S3

Issue Description&Cause of the Issue:

AMI Backup of Development systems.AMI Backup of all mentioned Development systems

Resolution proposed/employed:

Step 1: Login to the linux server

Step 2: go to aws backup

Step 3: go for protected resources

Step 4: give the instance id

Step 5: choose instance and create ondemand backup

Step 6: click on create backup now

Step 7: choose retention period

Service/resource category: RDP

Issue Description&Cause of the Issue:

RDP connection Remote Desktops password expired for user account

Remote Desktops password has expired for my user account

Resolution proposed/employed:

Step 1: login to remote desktop as an admin user

Step 2: open server manager

Step 3: open computer management from tools

Step 4: select local user and group

Step 5: select the specific user

Step 6: reset password

Service/resource category: INTERNET

Issue Description&Cause of the Issue:

Public/Internet access

Check the Public Internet Access of the servers   Check the Public Internet Access of the servers

Resolution proposed/employed:

Step 1: ping 8.8.8.8

Step 2: use wget/curl with url

Service/resource category: Ports/connectivity

Issue Description&Cause of the Issue:

Enable port range 6400-6499 for France network for accessing BI Launchpad   Enable port range 6400-6499 for France network for accessing BI Launchpad

Resolution proposed/employed:

Step 1: go to security group

Step 2: Add port range in inbound rule

Step 3: save the security group

Step 4: Attach it to the server

Service/resource category: RDP connection

Issue Description&Cause of the Issue:

Removing RDP Internet access from jmpDEV02 and jmpDEV03.Removing RDP Internet access from jmpDEV02 and jmpDEV03

Resolution proposed/employed:

Step 1: go to security group

Step 2: remove the RDp port(3389)

Step 3: save the security group

Step 4: Attach it to the server

Service/resource category: Scheduling & Automation

Issue Description&Cause of the Issue:

To Stop automatic stop/start for Solman servers in Prod account To Stop automatic stop/start for Solman servers in Prod account

Resolution proposed/employed:

Step 1: go to cloudwatch event and disable cronjob expressions

Step 2: remove lambda association

Service/resource category: INSTALLATION

Issue Description&Cause of the Issue:

Installation/Upgradation

Install WinScp on 10.128.17.16 Install WinScp on 10.128.17.16

Resolution proposed/employed:

Step 1: Need to enable NAT gateway for internet access

Step 2: RDP to the the server

Step 3: Download winScp and install

Service/resource category: Load Balancer

Issue Description&Cause of the Issue:

Application Not working with WebDispatcher Load Balancer URL WAF behind the Load Balancer blocked the SQL query traffic from internet

Resolution proposed/employed:

Step 1: Go to WAF dashboard.

Step 2: Open the rule set and search for CrossSiteScripting_BODY rule Step 3: Update the rule action to "count"

Service/resource category: Patching

Issue Description&Cause of the Issue:

SLES Patching issue: zypper command failed to execute   Python package broken

Resolution proposed/employed:

Step 1: Connect to the server

Step 2: Uninstall lxml and re-install with altest version

Step 3: Execute /

Service/resource category: SECURITY

Issue Description&Cause of the Issue:

SecurityDeep security Agent status showing offline in Trend Micro Dashboard for GSMAPPDBPRD1 10.128.17.4   Deep security Agent status showing offline in Trend Micro Dashboard

Resolution proposed/employed:

Step 1: Connect to the server

Step 2: Deactivate the DS Agent using /opt/ds_agent/dsa_control -r

Step 3: Activate the agent using /opt/ds_agent/dsa_control -a

dsm://agents.deepsecurity.trendmicro.com:443/ "tenantID:536B0713-0803-AF90-B5A51281B076B61A" "token:38C371F0-D1AE-D7D7-76BA-4F3F1B648637"

Service/resource category: Load Balancer

Issue Description&Cause of the Issue:

Load Balancer Target Health check failed.The URL used by ALB for health test of Web dispatcher has been disabled due to security considerations

Resolution proposed/employed:

Step 1: Go to Health Check tab of Target Group section in EC2 Dashboard

Step 2: Click on Edit Button and update Healthcheck path as provided. Save the changes

Step 3: Health check path will be updated now and Target will be healthy

Service/resource category: User login & Permissions

Issue Description&Cause of the Issue:

Some users getting Google Authenticator code error even after using correct passcode   Some time Google Authenticator fails to sync. It has to be reset.

Resolution proposed/employed:

Step 1: Connect to Open VPN server.

Step 2: Run below commands cd /usr/local/openvpn_as/scrip

Service/resource category: Ports/connectivity

Issue Description&Cause of the Issue:

HFM Connectivity issue between GBQ and HFM Non-Prod Application   Traffic was getting blocked for the HFM NonProd application after the access was blocked over the open internet and restricted to the different stakeholders' offices. This happened due route table entry missed for HFM server

Resolution proposed/employed:

Step 1: Go to route table

Step 2: Edit the route

Step 3: Entry new route for HFM server target as VPC peering ID

Service/resource category:OS Hardening

Issue Description&Cause of the Issue:

HANA Dev, QA and Sandbox is not configured to use tsc Update clock source of SAP Hana to Time Stamp Counter (TSC)

Resolution proposed/employed:

Step 1: Conect to the server

Step 2: Find the current clock setting using cat

/sys/devices/system/clocksource/clocksource0/current_clocksource

Step 3: Find available clocks using cat

/sys/devices/system/clocksource/clocksource0/available_clocksource xen tsc hpet acpi_pm

Step 4: Override current clock source using bash -c 'echo tsc >

/sys/devices/system/clocksource/clocksource0/current_clocksource'

Service/resource category:EC2 or VMs

Issue Description&Cause of the Issue:

Some configuration files are not getting copied from DEV server to PROD server DEV drive was not mapped in prod server

Resolution proposed/employed:

Step 1: Connect to the source server from where file will be shared.

Step 2: Right click on the folder or drive and go to properties. Select sharing tab.

Step 3: Go to Advance sharing and set the permission as per the requirement. Click on OK and Apply.

Step 4: Now Connect to Target server and go to map network drive option

Step 5: Add the Source server Ip like \\10.128.9.12 and browse. It will ask for Admin credential

(provide admin credential of current server from where access set up is getting done)

Step 6: Select on the required drive to be mapped and click ok. That drive will be mapped to this server and file can be copied.

Service/resource category:SAP Router

Issue Description&Cause of the Issue:

SAP cloud connector not accessible from the internet.

Resolution proposed/employed:

1. Private IP was used in the link instead of the public IP of the Jump server.
2. Port 8443 was not opened on the Jump server.

Step 1: Use the Public IP in the link instead of the private IP of the Jump server.

Step 2: Allow inbound traffic from internet to Port 8443 in the Security Group of the instance.

Step 3: Connect to the Jump server and add a new inbound rule to open Port 8443 to the Jump

server. Follow the below path:

Windows -> Firewall and network protection -> Advanced settings -> Inbound Rules -> New Rules

-> Mention the Port and finish it

Service/resource category: Connectivity - VPN, DirectConnect & OpenVPN

Issue Description&Cause of the Issue:

AWS VPN tunnel down Customer side firewall tunnel down- software bug.

Resolution proposed/employed:

Step 1. Check aws side tunnel setup.

Step 2. call the customer to share screen

Step 3. open sophos firewall GUI.

Step 4. stop their failover for the tunnel

Step 5. Start the tunnel manually from firewall see once that connection comes green then turn on fail over . (customer will perform the same action from their end, we can guide them)

Service/resource category

RDP connection Windows activation issue

Issue Description & Cause of the Issue

Unknown

Resolution proposed/employed

Step 1. RDP into the server & open powershell

Step 2. For Windows Server 2012 R2 and earlier: Update EC2Config, and then restart the instance.

For Windows Server 2016 and later: Run the following command to set the correct route to the Microsoft KMS server:

```
PS C:>Import-Module "C:\ProgramData\Amazon\EC2Windows\Launch\Module\Ec2Launch.psd1"

PS C:>Add-Routes

PS C:>Set-ActivationSettings

PS C:>slmgr /ato
```

Service/resource category

SSH

Issue Description & Cause of the Issue

Not able to connect to DB server through Session Manager or Putty. Outbound Rule was not present (access to internet) in the server's Security Group.

Resolution proposed/employed

Step 1. First, try connecting (SSH) to the private server through NAT instance (or any such

instance in Public subnet of the VPC).

Step 2. Check the status of ssm-agent by this command ---> systemctl status amazon-ssm-agent

Step 3. Enable the ssm-agent if disabled ---> sudo systemctl enable amazon-ssm-agent

Step 4. If this still does't work, then try to ping google.com or 8.8.8.8 and check if packages are recieved or not. If not, then it means that the server doesn't have access to the internet to install the systemctl packages.

Step 5: Check the Outbound rules of the respective Secuirty Group. Add the rule if there's none or have any discrepency in it. Also check whether NAT instance allows traffic from that private server or not.

Step 6: Now restart the ssm-agent in the private server through the NAT instance ----> systemctl

restart amazon-ssm-agent

Service/resource category

Ports/Connectivity

Issue Description & Cause of the Issue

Not able to send emails from Cloud SAP server through Office 365. Login attempt failed found in trace output.

Resolution proposed/employed

Step 1: Submit a request to AWS for removing the email sending/receiving limitations from the EC2 instances on the account.

Step 2: Get the Public IP of NAT instance whitelisted on the SMTP server.

Step 3: Done by the SAP Application team - After maintaining the Microsoft mail server (MS Office 365) userid/password in SCOT configuration of the cloud SAP application server, it started working.

Service/resource category

Storage - EBS, S3 & EFS

Issue Description & Cause of the Issue

Backup copy to s3 not getting completed on time and uploaded partially from the BW Prod system.With increased backup size and the number of parallel read write to the local HDD increased because of which the burst balance decreased and backup generation started with baseline throughput of ~25mbps. Also, as data copy to S3 started at 11:30 PM, the throughput of 20MBPS got divided between read and write operation and hence the backup time increased significantly (~20 hrs).

Resolution proposed/employed

Step 1: The delete script to remove the older backups was disabled from the crontab to complete the backup copy upload to s3.

Step 2: A temporary SSD disk was mounted as /backup1 and the next backup taken was redirected towards this temp mount. Also, backup copy was moved from this temp mount to s3 fof few days.

Step 3: With SSD volume, since there is no burst balance concept within 3000 iops, the backup generation and copy to S3 was getting completed within 1 hour each.

Step 4: After few days of observation and RCA, the HDD disk was permanently replaced with the

SSD disk of the same size.

Service/resource category

SAP Router

Issue Description & Cause of the Issue

Not able to connect to the Cloud servers (Dev, QA and Prod) through SAP Router string via VPN.VPC CIDR block or servers IPs not allowed on the VPN firewall at the customers end.

Resolution proposed/employed

VPC CIDR block or servers IPs were whitelisted on the VPN firewall at the customers end.

Service/resource category

DNS

Issue Description & Cause of the Issue

DNS Rsolution isssue for private domain (for server) maintained in AWS end.Record Entry is not there in private hosted zone

Resolution proposed/employed

Step 1: Go to private hosted zone

Step 2: Edit the record set

Step 3: Enter a new record (A type) with DNS and target as server IP

Step 4: Test DNS resolution

Service/resource category

DNS

Issue Description & Cause of the Issue

DNS Resolution not working for Internet facing

Load Balancer Record Entry is not there in public Hosted zone

Resolution proposed/employed

Step 1: Go to pubic hosted zone

Step 2: Edit the record set

Step 3: Enter a new record (Alias type) with DNS and target as Load balancer default DNS

Step 4: Test DNS resolution

Service/resource category

DNS

Issue Description & Cause of the Issue

DNS Resolution not working for private domain (DNS maintained in on prem)DNS outbound resolver not configured properly

Resolution proposed/employed

Step 2: Create outbound resolver rule with the necessary configuration of DNS server

Step 3: Share the outbound resolver across all the required AWS Account using RAM

Step 3: Accept the shared rules from other Accounts Step: Test DNS resolution

Service/resource category

Patching

Issue Description & Cause of the Issue

Server is showing Patching Non compliant New patches released and that has to be deployed in the server

Resolution proposed/employed

Step 1: Ensure the server is manged by SSM

Step 2: Set Patch Baseline

Step 3: Apply patches using

Service/resource category

Application & service/system

Issue Description & Cause of the Issue

User not able launch Redshift query Editor. Though user has Redshift access but to access Query Editor new permission has to be added

Resolution proposed/employed

Step 1: Go to IAM and search for the user

Step 2: Edit existing customer managed policy

Step 4: Ad

Service/resource category

Ports/Connectivity

Issue Description & Cause of the Issue

Windows server is not reachable in custom HTTPS port is opened in Security group but still application is not reachable. Windows Defender firewall blocks the inbound traffic

Resolution proposed/employed

Step 1: Login to Windows Server

Step 2: Go to windows Defender Advanced setting

Step 3: Create

Service/resource category

Ports/Connectivity

Issue Description & Cause of the Issue

Server connectivity not working for custom ports in Oracle Linux Server Port is opened in Security group but still application is not reachable. Iptables blocks connectivity on custom ports

Resolution proposed/employed

Step 1: Check iptables service is running (service iptables status)

Step 2: Stop iptables service (service iptables stop)

Step 3: Application should be reachable

Service/resource category

Connectivity - VPN, DirectConnect & OpenVPN

Issue Description & Cause of the Issue

Data Transfer speed is very slow over site to Site VPN.Normal SCp or SFTp speed from on-prem to AWS server is very slow. Try data Transfer to S3 over S3 private Link

Resolution proposed/employed

Step 1: Provision S3 interface endpoint allow on-prem CIDR in endpoint security group

Step 2: Install AWS CLI in on-prem server

Step 3: AWS configure wth proper keys with S3 permission

Step 4: Use AWS S3 CP or sync command with --endpoint-url of S3 private Link.

Service/resource category

Storage - EBS, S3 & EFS Not able to mount EFS in Oracle Linux

Issue Description & Cause of the Issue

This happenes if nfs utils is not present in server or 2049 port is not allowed in EFS security Group

Resolution proposed/employed

Step 1: Check internet connectivity on the server

Step 2: run yum update -y

Step 3: yum install nfs-utils

Step 4: mount the EFS volume using EFS mount command

Service/resource category

Application & service/system

Issue Description & Cause of the Issue

The sapstartsrv process failed to start in the Sandbox App server.The sapstartsrv process failed to start in the Sandbox App (backup server similar to Prod App) server due to missing files in the /sapmnt

directory. The /sapmnt folder was mounted on an EFS with no stored/shared data required to initiate the service.

Resolution proposed/employed

Step 1: Since the Sandbox App server was a replica of the Production App server, the existing mount point configurations of the Prod App server was investigated against the Sandbox App server's configuration. It was found that, the /sapmnt mount of the Sandbox DB server was needed to be shared and mounted on the Sandbox App server (similar to the Production systems).

Step 2: The unused EFS was unmounted and its entry from /etc/fstab was removed as well.

Step 3: The /sapmnt directory of the Sandbox DB server was shared and mounted onto the Sandbox App server with the same name via NFS ('yast' was used for sharing and mounting the directory between the NFS server and the client).

Step 4: Entry for this shared folder was added to the /etc/fstab file as well.

Service/resource category

User login & Permissions

Issue Description & Cause of the Issue

Unable to write to a nfs shared file and getting

'Access denied' or 'read-only access' message. In the NFS permissions settings, root_squash was enabled by default. 'root_squash' will allow the root user on the client to both access and create files on the NFS server as root, since the user (sap admin) accessing the file was not 'root' thus access to write was getting denied.

Resolution proposed/employed

Step 1: In nfs server, check the /etc/exports file, change the 'root_squash' to 'no_root_squash' if the user accessing the shared folder is other than 'root'.

Step 2: Then restart the nfs server service: cmd: systemctl restart nfsserver

Step 3: In the nfs client, delete the previously mounted folder and mount it again using 'yast' (for SUSE Linux only).

Step 4: If getting error like 'server busy' or 'unmounting ... ', click on 'CONTINUE' anyway.

Step 5: Check the entries in the /etc/fstab file and add entry for the shared folder again, if needed.

Service/resource category

EC2 or VMs

Issue Description & Cause of the Issue

IRN not getting generated. CPU utilization of PROD server reaching 100% at particular time. NAT instance was scheduled in start/stop with non-prod server due to which prod server was not getting internet connectivity.

Resolution proposed/employed

Step 1: Initially rebooted server at 9 am IST for couple of days. After that CPU utilization was below threshold.

Step 2: Checked in TOP command nothing found in that and also no job was running at that particular time when CPU was hitting 100%.

Step 3: Figured out it must be due to start/stop of NAT instance. Kept NAT running for couple of days

Step 4: No issue reported again as Prod server was getting internet connectivity. Reserved the NAT instance.

Service/resource category

Connectivity - VPN, DirectConnect & OpenVPN

Issue Description & Cause of the Issue

SAP Dev team not able to connect to the AWS servers through the Client VPN.The static route configuration on the client's network firewall and the router settings was conflicting. Also, the client was trying to connect to an unavailable IP address of the AWS network

(2nd IP address is reserved by the AWS)

Resolution proposed/employed

Step 1: The 'tracert' output for an on-prem network's host was evaluated from our AWS server and was seen that the packages were getting dropped after leaving the VPN tunnel gateway.

Step 2: Client and their Microtik team made chnages in the configuration of their Router Firewall after the cause was found out.

Step 4: Users were created on the on-prem network to allow the Dev team of PwC to enter the client network. From there, they were able to connect to the AWS servers via the IPSec tunnel (VPN tunnel)

Service/resource category

CloudWatch

Issue Description & Cause of the Issue

Not getting SNS notification when CloudWatch metric goes into alarm state.CloudWatch Alarms does not have authorization to access the SNS topic encryption key

Resolution proposed/employed

Step 1: Check the 'History' tab of the alarm (which is In Alarm state)

Step 2: Check the error message received when action was triggered

Step 3: If the error message says 'CloudWatch Alarms does not have authorization to access the SNS topic encryption key', then go to the SNS topic configured to send the notifications.

Step 4: Select the SNS topic, select Edit and then 'Disable' the encryption.

Service/resource category

Storage - EBS, S3 & EFS

Issue Description & Cause of the Issue

Mount point gets unmounted automatically when another volume is detached.   While replacing a disk, when the old volume is detached, the newly attached volume under the same mount point/name gets automatically unmounted:

Had an /etc/fstab entry for the same mountpoint but a different device. Due to a badly implemented feature in the systemd manager, it automatically removes mounts whenever the device doesn't exist.

Resolution proposed/employed

Step 1: Check to see if this is the problem: >> journalctl -n 100

Step 2: Remove the entry from /etc/fstab, then run the below before mounting the device again.

```
>> systemctl daemon-reload
```

Step 3: Try to mount the device at a different location

Service/resource category

SSH

Issue Description & Cause of the Issue

Not able to connect to server through PuTTY. Jump server (Bastion Host) and DB server not hosted in the same VPC and not connected via any resource.

Resolution proposed/employed

Step 1. Open Reachability Analyzer in the VPC dashboard under the Network Analysis tab.

Step 2. Open the Create and Analyze path.

Step 3. Select the source type & destination type as instance and then the provide the corresponding details.

Step 4. Provide the port number (22) along with the protocol type (TCP).

Step 5. Click the "Create and Analyze path" and then the explanation wil be shown stating " The VPCs are not connected by a supported resource" and correspondingly take the AMI of the DB server and then launch it through the same VPC as of Jump server.

Service/resource category

Storage - EBS, S3 & EFS

Issue Description & Cause of the Issue

Expected D-drive space not visible after delettion of some files   Compress files' to save disk space enabled in drive settings. This hampers the drive to show the correct space immediately after file deletion.

Resolution proposed/employed

Step 1: Open Drive properties

Step 2: Uncheck Compress files to save disk space

Step 3: Apply

Service/resource category

EC2 or VMs

Issue Description & Cause of the Issue

Instance failed 2/2 status check A system status check failure indicates a problem with the AWS systems that your instance runs on.

Resolution proposed/employed

When a problem with an underlying host impacts production, we can stop and start the instance to migrate from the current underlying host.

Service/resource category

Patching

Issue Description & Cause of the Issue

Patching issue - python installation failure.Python package unable to update through Patch manager

Resolution proposed/employed

Step-1 Open Terminal window

Step-2 Run zypper update python-PyYAML

Service/resource category

Patching

Issue Description & Cause of the Issue

Installation of patches failed docker, container and mozilla patches when getting

Resolution proposed/employed

1) Open the Compliance reporting tab after failed installation appears.

2) The patches that are causing

Service/resource category

Scheduling & Automation

Issue Description & Cause of the Issue

Multiple Email alerts for one backup transfer to S3 bucket.Two Cron daemons running on the system

Checks done for identifying the issue:

Resolution proposed/employed

Check 1: Multiple entries in crontabs for triggering the same script

```
>> crontab -l
```

Check 2: If check 1 shows one entry for the backup cronjob, check for same crontab installed for multiple users

```
>> cd /var/spool/cron/tabs

>> ls -ltr
```

Check 3: If check 3 shows tab for only 1 user, check for ultiple cron daemons running on the system

```
>> ps -aux | grep "cron"          >> pidof cron
```

Resolution: If 2 cron daemons are found, manually kill the zombie or duplicate cron daemon.

```
>> kill -9 <pid of duplicate cron daemon>
```

Service/resource category

Ports/Connectivity

Issue Description & Cause of the Issue

Lambda and Glue - Amazon Redshift Integration

Lambda function and Glue was unable to connect to the Redshift cluster (Redshift in private subnet), resulting in a timeout error

Resolution proposed/employed

1. Lambda function was not in the same VPC and subnet as the Redshift cluster.

2. Glue Connectors were not created/enabled, so glue wasn't able to access redshift.

1. Lambda function was moved inside the same VPC and subnet as the Redshift cluster.

2. Redshift security group rules were reviewed and adjusted to ensure appropriate inbound connections.

3. Glue Connectors were created in Glue Console, making the connection between the Redshift

(Private) and Glue Jobs