RSA KNOWLEDGE

RSA SecurCare® Online

AM8.1-How to Troubleshoot ODA login failures

Article Content

Article Number

000029925

Product Details

RSA Product Set: SecurID
RSA Product/Service Type: Authentication Manager
RSA Version/Condition: 8.1.0, AM 8.1 SP1
Platform: VMware, hardware Appliance
Platform (Other): hardware Appliance Dell or Intel
O/S Version: ESXi 5.0, Suse Linux 11
Product Name: null
Product Description: null

Issue

Specified user getting authentication failure, however server not displaying denied attempt. Problem is intermittent or sporadic. Sometimes after entering the On Demand TokenCode, ODT, the user ends up back at the login or logon prompt instead of being allowed access, but no authentication failure appears in the AM logs or real time authentication monitor, real time monitor, RTM

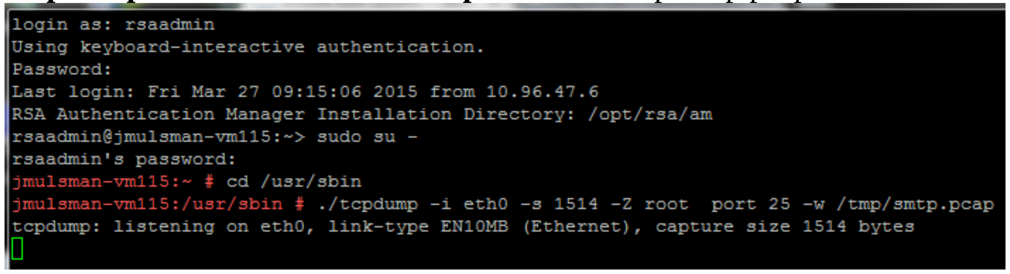
Tasks

To troubleshoot this or similar ODA authentication failures, you need two network packet captures running on both the Primary and any Replicas, filtered on UDP port 5500 for Authentication and TCP port 25 for SMTP mail

Resolution

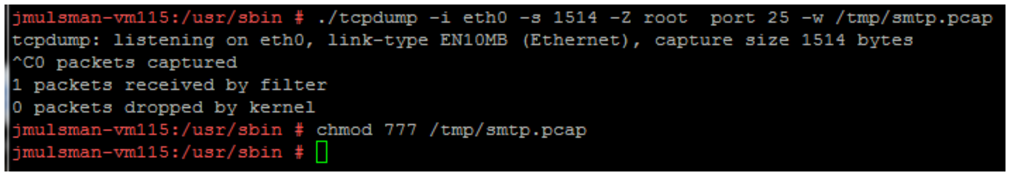
start the TCPDump on both the Primary and Replica in separate SSH sessions, to capture both smtp and Authentication traffic saved to a file. When the next ODA intermittent login failure happens, then stop the captures and send the network packet capture files to RSA. This way we can see if both the Primary and Replica are each sending an email, or if the replica is sending 2 emails, or neither is sending any emails, etc…

SSH to the Virtual Appliance with the operating system account rsaadmin.
sudo su -
<same password again>   This makes you root
#   cd /usr/sbin
./tcpdump -i eth0 -s 1514 -Z root port 25 -w /tmp/smtp.pcap



```
login as: rsaadmin
Using keyboard-interactive authentication.
Password:
Last login: Fri Mar 27 09:15:06 2015 from 10.96.47.6
RSA Authentication Manager Installation Directory: /opt/rsa/am
rsaadmin@jmulsman-vm115:~> sudo su -
rsaadmin's password:
jmulsman-vm115:~ # cd /usr/sbin
jmulsman-vm115:/usr/sbin # ./tcpdump -i eth0 -s 1514 -Z root  port 25 -w /tmp/smtp.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1514 bytes
```

[In a separate SSH window]
./tcpdump -i eth0 -s 1514 -Z root port 5500 -w /tmp/auth.pcap
[When the logon failure occurs, stop the TCPdump with a <ctrl> C   ^C, change permissions]
chmod 777 /tmp/smtp.pcap
chmod 777 /tmp/auth.pcap   This grants full permissions to everyone, makes it easy to copy file off with WinSCP



```
jmulsman-vm115:/usr/sbin # ./tcpdump -i eth0 -s 1514 -Z root  port 25 -w /tmp/smtp.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1514 bytes
^C0 packets captured
1 packets received by filter
0 packets dropped by kernel
jmulsman-vm115:/usr/sbin # chmod 777 /tmp/smtp.pcap
jmulsman-vm115:/usr/sbin # 
```

Use WinSCP or Filezilla to copy the pcap file off of the Appliance. You may also want to download and send the troubleshooting logs or an Authentication report

Notes

Big Picture of an On-Demand Authentication, ODA/ODT login success, User enters PIN first, PIN triggers email/SMS delivery of On-Demand TokenCode, then User Enters ODT to complete authentication. The second login screen often says to enter the Next TokenCode, even for an ODA.

Authentication Manager   Agent

1. Replica/Primary   <-------------------------------PIN for UserID
2.   ------------------------------->   email with On-Demand TokenCode
3. Replica/Primary   <-------------------------------UserID enters ODA code
4.   -------------------------------->   Successful Authentication

We have noticed that if the Step 3 authentication is more than 60 seconds after the Step 1 Enter PIN, some agents timeout and do not send the step 3 Authentication request, and nothing shows in the RSA AM logs because it never arrived, and the User has to enter their PIN again to trigger a second email/SMS ODT