# CASE 1 User Crontab Password Expired

|  |
| --- |
| **Noti**:  crond[1801]: (root) FAILED to authorize user with PAM (Authentication token is no longer valid; new one required) |

## Scenarios

|  |
| --- |
| - **Prepare the case**:  **1. Add: /etc/crontab**:  \* \* \* \* \* root rsync -av --delete /home/dath/test/ /home/root/test/  **2. Tail to check the log**:  tail -10f /var/log/cron  Jan 8 22:58:01 nobody CROND[1718]: (root) CMD (rsync -rav --delete /home/dath/test/ /home/root/test/)  Jan 8 22:59:01 nobody CROND[1726]: (root) CMD (rsync -rav --delete /home/dath/test/ /home/root/test/)  Jan 8 23:00:01 nobody CROND[1746]: (root) CMD (rsync -rav --delete /home/dath/test/ /home/root/test/) |

|  |
| --- |
| - **Fail case**:  **1. Set the root account to be “Password Expired”:**  # chage -W 0 root  # chage -M 69 root  [root@nobody test]# chage -l root  Last password change : Oct 30, 2017  Password expires : Jan 07, 2018 (Current date: Jan 08, 2018)  Password inactive : never  Account expires : never  Minimum number of days between password change : 0  Maximum number of days between password change : 70  Number of days of warning before password expires : 0  **2. Login root to check**:  bash-4.1$ su root  Password:  You are required to change your password immediately (password aged)  Changing password for root.  **3. Tail the Log to check the CASE1-ERROR**:  tail -10f /var/log/cron  Jan 8 23:17:01 nobody CROND[1789]: (root) CMD (rsync -rav --delete /home/dath/test/ /home/root/test/)  Jan 8 23:18:01 nobody crond[1801]: (root) FAILED to authorize user with PAM (Authentication token is no longer valid; new one required)  Jan 8 23:19:01 nobody crond[1804]: (root) FAILED to authorize user with PAM (Authentication token is no longer valid; new one required)  Jan 8 23:20:01 nobody crond[1805]: (root) FAILED to authorize user with PAM (Authentication token is no longer valid; new one required) |

# CASE 2 User Crontab Account Expired

|  |
| --- |
| **Noti**:  (root) FAILED to authorize user with PAM (User account has expired) |

## Scenarios

|  |
| --- |
| - **Prepare the case**:  **1. Add: /etc/crontab**:  \* \* \* \* \* root rsync -av --delete /home/dath/test/ /home/root/test/  **2. Tail to check the log**:  tail -10f /var/log/cron  Jan 8 22:58:01 nobody CROND[1718]: (root) CMD (rsync -rav --delete /home/dath/test/ /home/root/test/)  Jan 8 22:59:01 nobody CROND[1726]: (root) CMD (rsync -rav --delete /home/dath/test/ /home/root/test/)  Jan 8 23:00:01 nobody CROND[1746]: (root) CMD (rsync -rav --delete /home/dath/test/ /home/root/test/) |

|  |
| --- |
| - **Fail case**:  **1. Set the root account to be “Account Expired”:**  # chage -W 0 root  # chage -M 69 root  [root@nobody test]# chage -l root  Last password change : Oct 30, 2017  Password expires : never  Password inactive : never  Account expires : Jan 08, 2017 (Current: Jan 08, 2018)  Minimum number of days between password change : 0  Maximum number of days between password change : 70  Number of days of warning before password expires : 0  **2. Login root to check**:  bash-4.1$ su root  Password:  Your account has expired; please contact your system administrator  su: incorrect password  **3. Tail the Log to check the CASE1-ERROR**:  tail -10f /var/log/cron  Jan 8 23:00:01 nobody CROND[1746]: (root) CMD (rsync -rav --delete /home/dath/test/ /home/root/test/)  Jan 8 23:01:01 nobody crond[1762]: (root) FAILED to authorize user with PAM (User account has expired)  Jan 8 22:56:01 nobody crond[1698]: (root) FAILED to authorize user with PAM (User account has expired) |