Click Here

From time to time in the vSphere Client interface I come across the notification: Your password will expire in xx days. I decided to learn how to manage password policies in VMWare vSphere, how to change the time when a password expiry notification appears for local and domain vSphere users and set the password settings for some users to never expire. Here is what I have found.Password & Lockout Policy on VMWare Single Sign On (SSO)In my case, I decided to disable the password expiration for the local user (since nobody works under this local account permanently, and the vSphere administrators authenticate under their Active Directory domain accounts).By default, the SSO policy is applied for vSphere local users, which requires a user password to be changed every 90 days.You can find the SSO password policy settings in the following section of the vSphere Client: Administration -> Single Sign On -> Configuration.As you can see on the Password Policy tab, the following requirements are applied to the passwords of all local vCSA users:The minimum password length is 8 characters (maximum 20 characters);A password expires in 90 days (maximum lifetime);The last 5 passwords are not allowed to be reused;Some password complexity restrictions.Click Edit and change the policy settings. For example, you can change Maximum lifetime to 365 (it means that you have to change passwords once a year) or enter 0 here (meaning that the password is not expired).Change Password Expiration Settings to Never Expire for Local VMWare vCSA UsersIf you do not want to change your password policy for all vCenter users, you can change the password policy and the expiration settings for the specific user. For example, you want to set the password for the local backup_user to never expire. To do it, connect to your vCSA host using the SSH client.You will need the dir-cli tool, which is located in /usr/lib/vmware-vmafd/bin/.cd /usr/lib/vmware-vmafd/bin/Check that the local user exists:./dir-cli user find-by-name --account backup_userEnter password for :Account: backup_userUPN: /You can change the password for this user:./dir-cli password reset --account backup_user --password OldBackupP@$$ --new NewBackupP@$$Or you can set password to never expire:./dir-cli user modify --account backup_user --password-never-expiresEnter password for :Password set to never expire for [backup_user]Root Password Expiration on vCenter VCSAWhen you install the vCenter Server Appliance, the password lifetime for root user is set to 365 days (vCenter 6.5 or earlier) or 90 days (vSphere 6.7). So root is also subject to password expiration policy.You can view the password policy settings in the vCSA Appliance Management (. Go to the Administration section and check the values in the Password expiration settings section.Password expires: YesPassword validity (days): 90Password expires on: Jun 13, 2020, 2:00:00 AMYou can change the password expiration settings for root or set it to never expire (if its value is 0).Also you can check the root password expiration setting from your vCSA console:chage -l rootLast password change : Mar 15, 2019Password expires : Jun 20, 2019Password inactive : neverAccount expires : neverMinimum number of days between password change : 0Maximum number of days between password change : 90Number of days of warning before password expires : 7It is interesting that the vCSA Appliance Management interface does not prompt root to change the password or show any password expiring warning.However, if you try to upgrade the vCenter Server Appliance you may come across the following error message:Appliance (OS) root password is expired or is going to expire soon. Please change the root password before installing an update.Or when trying to change the expired root password in vCSA Appliance Management, a warning may appear:Permission Denied. Set the maximum number of days when the password will expire. Administrator configuration updated successfully.In this case, you have to change the root password in the vCSA console with this command:passwdChanging Password Expiration Notification Settings on VMWare vCenterBy default an expiring password notification in a vCenter Client starts to appear 30 days before it expires.If users authenticate in vCenter using their AD accounts, the domain password policy is applied for user passwords. A user will see a notification prompting them to change the password 30 days before it expires. So if your domain policy enforces password change once in 30 days, VMWare vCenter users constantly see an annoying warning Your password will expire.In vCSA you can configure how many days before the password expires a user will see this notification.If you are using vSphere HTML5 client, this setting is specified in the configuration file on the vCenter Server Appliance server: /etc/vmware/vsphere-ui/webclient.properties.Open the file and find the sso.pending.password.expiration.notification.days parameter.Change its value to 7. It means that the password expiry notification will appear 7 days before it happens. Then restart your vSphere client:service-control --stop vsphere-ui service-control --start vsphere-uiIf you are using the old Web Client (Flex), you will have to change the value of the sso.pending.password.expiration.notification.days parameter in the /etc/vmware/vsphere-client/webclient.properties file.After you have edited the setting, restart the Web Client service:service-control --stop vsphere-client service-control --start vsphere-client Has your vCenter root user password expired? Dont worrythis is a common issue, and its easy to fix. VMware enforces password expiration policies as a security measure, but being locked out unexpectedly can be frustrating. Fortunately, regaining access is straightforward. This guide will walk you through the step-by-step process to reset the expired root password and get back into your vCenter Server without hassle. VMware vCenter Server follows standard security practices, including enforced password expiration for the root user. This is intended to improve security by ensuring passwords are changed periodically. However, if youre caught off guard, it can temporarily lock you out. Lets walk through the recovery process. Open a browser and go to:https://:5480(Replace with your actual vCenter IP address.) Log in using the root user. If the password has expired, youll be prompted to change it immediately. Click the link to change the password. Enter the current (expired) password, then create and confirm a new password. Ensure the new password meets VMwares password policy. Click Save. If successful, youll see a confirmation message. Log out and log back in using the new root password to ensure everything is working properly. If VAMI is inaccessible due to network or system issues, you can change the root password using the vSphere Client. Log in with an admin-level account. Go to:Administration Single Sign-On Users and Groups Locate the root user, then select the option to reset the password. Log out and back in to confirm the new root password works. If youve forgotten the root password and cant log in via VAMI or vSphere, reset it in single-user mode. Reboot the vCenter Server Appliance. At the GRUB menu, press e to edit the boot parameters. Find the kernel line and append:rw init=/bin/bash Press Ctrl + X to boot. Once in the shell: passwd Enter the new password when prompted. Then reboot the appliance: reboot After reboot, log in to the VAMI using the new root password to ensure its been reset successfully. Enforce MFA and strong password policies. Monitor expiration dates using alerts or scheduled reviews. Use a password manager for secure tracking. Avoid using the root account for daily operationscreate and delegate roles with least privilege access. An expired vCenter root password can be a minor inconvenience, but its easily fixed. Whether you reset it via the web interface or the console, youre just a few steps away from regaining access. After 90 days, the password for the 5480 port expires and you need to change it.To do this, we will need console access to the VCSA.Authenticate using the expired root password at the VM prompt, and choose Troubleshooting Mode Options:Enable SSHUse a SSH session to authenticate with the vCenterOnce authenticated, do:shellIf running this commandchage -l rootGives you this output, a password change is needed Run passwd rootAnd change the password.Disable SSH again if needed. The root password is something that every server admin should keep in a well-secured vault or database, and believe me a text file is not a good place. It would also be a good idea to remember the root password, but sometimes thats not easy. Passwords are usually very complex, containing about 15 or more various characters. One day, there may be a situation where you forget the root password for your vCenter Server Appliance, or the password has just expired. Resetting the root password of the vCenter Server Appliance is a relatively easy task, however, it requires restarting the vCenter Server VM. Restarting vCenter does not affect VMs as they are running on ESXi hosts, however cluster features such as DRS, HA or vMotion will not work during reboot. In this article, I will show you how to reset vCenter Server root password step by step. This method works for vCenter Server Appliance version 6.5 / 6.7 / 7.x / 8.x. Resetting root password in vCenter Server Appliance Resetting the root password requires restarting the vCenter Server Appliance VM. This is needed because we need to access the GRUB bootloader menu, which is not available when the VM is running. Before restarting, take a snapshot of the vCenter Server Appliance VM in case there are any issues and you need to roll back. Follow the root password reset instructions: 1. Take a snapshot. Right-click on vCenter Appliance VM. From Snapshots menu choose Take Snapshot. 2. Now you need to access the ESXi that your vCenter Server VM is running on. This is to access the VCSA VM through the console. Log in to the ESXi web GUI, select VCSA VM and from the Console menu select Open browser console. A console window will pop-up. 3. Once you have console opened it is time to reboot the vCenter Server Appliance VM. Right-click on the VM and choose Guest OS, then Restart. 4. Now watch the console. When you see the Photon screen, press E. 5. You are now in the GRUB bootloader menu. Use the arrow keys to go to the end of the linux line and right after $systemd_cmdline make a space and add the following: rw init=/bin/bash Once added, press F10 to continue booting. 6. Type following command: mount -o remount,rw / Press Enter. 7. To change the password, type the following command: passwd And enter the new root password twice. Confirm by pressing Enter. 8. If the password has been updated successfully it is time to reboot the VCSA. Type the following command: umount / Press Enter. Then reboot the appliance by running the following command: reboot -f Press Enter. 9. Once vCenter is up, confirm that the new root password is working by logging into vCenter Server Appliance Management Interface (VAMI). If the new password is ok, vCenter is running fine, you can go ahead and delete the snapshot. Setting password to never expire If you have a strong root password, consider disabling root password expiration. This can be done in VAMI, under Administration, then Edit next to Password Expiration Settings. Just select Password expires No. Thank you for reading! Here are some links you may be interested in: Christian Wells February 15, 2024February 15, 2024 No Comment VMware ESXi stands as a cornerstone in the realm of server virtualization, providing a robust platform for managing virtual environments. As the backbone of many IT infrastructures, securing and maintaining access to your ESXi hosts is paramount. This includes the ability to reset the root password, a task that becomes crucial when the password is forgotten or when taking over an existing environment without proper documentation. This guide aims to demystify the process of resetting the root password on VMware ESXi hosts, ensuring administrators can regain control and maintain the security integrity of their virtual environments. The root account on an ESXi host is the gateway to full administrative capabilities, from creating and managing virtual machines (VMs) to configuring the network and storage resources. Losing access to this account can significantly impede your ability to manage your virtual environment, making password recovery an essential skill for any system administrator. Before proceeding with the root password reset, ensure you have physical or remote console access to the ESXi host. The process involves booting into a special troubleshooting mode, which requires direct interaction with the hosts console during the boot process. Restart the ESXi Host: Initiate a reboot of the ESXi host. This can be done directly from the server console or remotely via a management interface like the Integrated Dell Remote Access Controller (iDRAC) for Dell servers or the HP Integrated Lights-Out (iLO) for HP servers. Access the Boot Loader: As the host boots, youll be greeted with the VMware boot menu. Press Shift+R to access the boot options, where you can enter the troubleshooting mode. Enter Troubleshooting Mode: The system will prompt you to confirm entering troubleshooting mode. Confirm the prompt to proceed. Once in troubleshooting mode, the system will provide you with access to a limited shell where you can perform the password reset. Access the Shell: At the prompt, select the option to access the shell. Remount the Filesystem: To reset the password, youll need to remount the systems filesystem with write permissions: /sbin/mount -o remount,rw / Reset the Root Password: Use the passwd command to initiate the password reset for the root account: passwd root You will be prompted to enter a new password and confirm it. Choose a strong, memorable password to enhance the systems security. Restart the ESXi Host: After successfully changing the password, exit the shell and restart the ESXi host to apply the changes and return to normal operation: reboot After resetting the root password, take a moment to review your ESXi hosts security settings. Ensure that access to the host is properly secured, both physically and through the network. Consider implementing additional security measures, such as IP-based access controls and regular password changes, to maintain the integrity of your virtual environment. For those managing virtual environments, especially on platforms like VMware ESXi, the complexity of ensuring security and accessibility can be daunting. Shape.host offers Linux SSD VPS services, providing a secure, high-performance foundation for your virtualization needs. With Shape.host, users can enjoy the benefits of fast SSD storage and robust security features, backed by expert support. Whether hosting Linux distributions on VMs or managing a complex virtual environment, Shape.hosts Linux SSD VPS services ensure your infrastructure is reliable, secure, and optimized for performance, allowing you to focus on managing your virtual environments with confidence. Tags:Resetting the Root Password in VMware ESXi Host My root user password expired in vCenter Hello, I can no longer access a vCenter service appliance that I own. The password, I believe, expired in December. Since I'm new to vCenter, I thought that I would be asked to change my password and that I would still be able to use my old one. Is it possible for an expired password to fully lock you out? This vCenter root password expired issue may arise with the following symptoms: When you try to log on to the management website: 5480 with root, it says the password is expired. When you installed vCenter, password change for local users is defined by default policy. You left the default setting to expire the root password in your vCenter Appliance 6.5/6.7/7.0. Why does it occur? The main reason is the default password policy, which is defined to expire after 90 days. In order to avoid root password expired, you can change the root password using SSH client or disable root user password expired for vCenter over the GUI. I will introduce the detailed steps to solve the issue of vCenter root password expired in the following article. Solution: vCenter root user password expired [2 quick tips] By default, the SSO policy is applied for vSphere local users. It requires a user password to be changed every 90 days. You can reset the root password and change password expiration settings from the vCenter Server Management Interface. Reset vCenter root password in vCSA 7.0 If you cant log into the web console, you could still log into the appliance via SSH. Then invoke the shell command, and reset the root password with the passwd command. To do it, connect to your vCSA host using the SSH client. 1. Enable the SSH access to vCSA in the Access >> SSH login >> Enabled section of the Appliance Management (. 2. Open your Putty SSH session and log in as root. Type shell and run this passwd command to vCenter change the root password expired. vCenter change root password expired policy to avoid it expiring again If you can log into vCenter now, you can then disable root password expiration by editing password policy to make it never expire. To check your password policy in vCenter, you can go to the Administration section and see the values in the Password expiration settings section. As you can see on the Password Policy tab, the following requirements are applied to the passwords of all local vCSA users: A password expires in 90 days (maximum lifetime); The minimum password length is 8 characters (maximum 20 characters); The last 5 passwords are not allowed to be reused; Some password complexity restrictions. And by editing the policy, you can then disable root password expiration again. How to change the settings of password expiration policy: If you do not want the root user password to expire in vCenter, you can disable password expiration policy by following these steps. 1. Connect to the Port 5480 of your appliance and sign in as root. 2. Go to the menu Administrator of your appliance. 3. In the Password expiration settings section, click Edit and select the password expiration policy. 4. In the opened wizard, select No to disable vCenter root password expiration. 5. Click Save to apply the new password expiration settings. Now the password of the root user never expires. When installing patches or upgrades, do not forget to backup VCSA. Having a proper backup can save you especially if you're in a production environment. For better protection, virtual machine backup is also necessary to prevent your VMs from malware attack and data loss. Scalable VM protection for expanding vCenter environment 96% of businesses experienced at least one of the major causes of data loss: human errors, hard drive failures, outages, fire and natural disasters, so a professional VM backup tool is necessary that offers better data protection for organizations. If you are searching for the premier backup solution for your enterprise, you will not find a better option than AOMEI Cyber Backup paired with your organization. Here I want to introduce a professional VMware backup software AOMEI Cyber Backup which performs automated backups for virtual machines and supports various versions including ESXi 6.0-7.0. You are able to backup your multiple virtual machines with its flexible strategies. With AOMEI Cyber Backup, you can enjoy these features easily. Auto VM Backup: schedule VMware or Hyper-V virtual machine backups in batch without human errors and perform hot backup to keep business continuity. Flexible vSphere Backup: batch backup large numbers of VMs managed by vCenter Server, or multiple VMs on a standalone ESXi host. Multiple Storage Destinations: backup to a local drive, or network destinations like NAS. Cloud Storage: easily archive backup versions to Amazon S3 for a better data storage solution. Retention Policy: delete unwanted or expired backups automatically, saving storage costs. Hit the button below to download AOMEI Cyber Backup 30-day free trial. Best practice for vCenter virtual machine backup 1. Bind Devices: Access to AOMEI Cyber Backup web client, navigate to Source Device > VMware > + Add VMware Device to Add vCenter or Standalone ESXi host. And then click > Bind Device. 2. Create Backup Task: Navigate to Backup Task > + Create New Task, and select VMware ESXi Backup as the Backup Type. 3. Set Task Name, Device, Target, Schedule, and Cleanup as needed. Task Name: you can change the task name or use the default name with an ordinal. Device: batch select large numbers of VMs managed by vCenter Server for centralized backup. Target: selecting to back up to a local path, or to a network path. Used paths will be saved in Favorite Storage for handy selection. Archive: add Amazon S3 buckets. Then go to check Archiving backup versions to Amazon S3 and click Select to choose the added Amazon S3. Schedule (optional): perform full, differential, or incremental backup, and automate execution according to the frequency you specified. Cleanup (optional): configure a retention policy to auto delete old backup files and save storage space. 4. Run Backup: Click Start Backup and select Add the schedule and start backup now, or Add the schedule only. 5. Restore: Click Restore to restore virtual machine from backup, saving the trouble of re-configuring a new one. Select a VM backup and click Restore to original/new location. It allows you to restore the entire VMware virtual machine to the original or another host easily and quickly. Summary When you deploy vCenter Server, you set the initial password of the root user, which expires after 90 days by default. If you want to disable vCenter root password expiration, this feature can be deactivated by performing the steps in this article. You can change the root password and the password expiration settings from the vCenter Server Management Interface. September 14, 2024bytheDXT The root password for VMware vCenter expires every 90 days by default. Depending on your vCenter setup, you may want to disable the root password expiry. In this post, I will show you step-by-step how to disable the root password expiry for VMware vCenter using the GUI and the CLI. Log in to the vCenter Server Management interface as root (it used to be called the vCenter Server Appliance Management Interface (VAMI)). Click on Edit beside Password expiration settings.Select No and click Save. The password expiry for the root user is now disabled. SSH into vCenter. Run the command shell to start a BASH session. To turn off the password expiry for the root account, we will use the command chage which is the change user password expiry information command. Run the following command to see the currently configured expiry settings for the root user chage -l rootRun the following command to turn off the expiry for the root user chage -I -1 -m 0 -M -1 -E -1 rootRunning chage -l root again will confirm that the settings are now in place and the root account no longer has a password expiry. The parameters we used with chage are: -I is the number of days of inactivity before the account is locked after a password expires. If this was set to 5 days and the account was not used for 5 days after the password expires, then on the 6th day, the account would be locked. We use the -1 parameter to disable all of this. -m is the number of days before the password can be changed. We use 0 to allow immediate password changes. -M is the maximum number of days before a password is considered expired. We use -1 again to deactivate this. -E is the expiry date for the account. As this is the root account, we dont want it to expire. We use the parameter -1 again to turn this off. Thats all it takes to disable the root password expiry in VMware vCenter. If you want to read more, here is the VMware documentation. book Article ID: 321369 calendar_today Updated On: Products VMware vCenter Server Issue/Introduction This article provides steps to reset the root password if you have lost or forgotten the existing root password without reboot / 6.7u1 / 7.x / 8.x Symptoms:Logging in to the root account of vCenter Server Appliance (VCSA) fails.The root account of the vCenter Server Appliance6.7 U1 and later is locked or account is expired.Forgot the root password.The root account password has beenlost or forgottenYou are unable to login to vCenterNote: The above symptoms can also occur on an external Platform Services Controller (PSC) running on vSphere 6.5 and 6.7. Environment VMware vCenter Server 7.xVMware vCenter Server 8.xVMware vCenter Server Appliance 6.x Cause With the change within VCSA 6.7 U1, the SSO user who is part of SystemConfiguration.BashShellAdministrator group will be able to log in to Bash shell and can call any commands using sudo and without password. This aims at reducing the gap between the root and SSO administrator user. The user has to enable shell to log in to the bash shell. By default, the user will be logged into appliance shell.For passwords that have expired, the default vCenter Server Appliance password expires after 90 days. For more information, seeChange the Password and Password Expiration Settings of the Root User. Resolution The resolution has two sections for the problem that we usually encounter:Steps to reset the Root Password in VCSA.Steps to follow if you have forgotten the Root Password.Connect SSH to VCSA and login using where vsphere.local is your default SSO Domain. If first time logging in, enable shell then enter shell.shell.set --enable trueshellOnce in shell as sso-user, run the below command to change to root shell.sudo -iUnlock the 'root' account using below command if it is already locked due to multiple logins with incorrect password.pam_tally2 --user=root --resetFor 8.0 U2 onwards:/usr/sbin/faillock --user root --resetNote: pam_tally2 is deprecated in Photon 4, use faillock insteadThen once in root shell, run passwd to change the root password.passwdConfirm that you can access the vCenter Server Appliance using the new root password.Follow Steps 1 and 2 from Section a.Then continue by running the following steps:Run the following command to change the root password.sudo passwd rootConfirm that you can access the vCenter Server Appliance using the new root password. You could set the Root password to never expire in order to prevent this issue by running command:chage -I -1 -m 0 -M 99999 -E -1 root or at the VAMI (https://:5480)Note: If you continue to have issues, seeUnable to login to the vCenter Server Appliance shell using root account even after password reset Additional Information For 7.0U1 and 6.7U3j there are a few changes:The Root user will be prompted for resetting the password when they try to SSH to the machine if expired or expiring.You can also login to VAMI using the SSO administrator and reset the root password from there.Email notification is sent earlier to prevent from having the Root password expired.An alarm will be triggered in vsphere-ui to notify the user about the password expiry.Changes in 8.0 U2 and above versions:You will get below error while executing pam_tally2 in 8.0 U2 or above versions, as this utility was deprecated in Photon 4 and 8.0 U2 is using Photon 4 version. The alternate utility on Photon 4 is "/usr/sbin/faillock" to unlock the accounts."-bash: pam_tally2: command not found"Note : In 8.0 U2 and above while running the command : /usr/sbin/faillock we might see the error : /usr/sbin/faillock: Error opening the tally file for root: permission denied.Log into vCenter via SSH as user and run the following command to unlock the accounts : sudo faillock --reset --user rootFor more information, see: You can update the password of the root user in the vCenter Server via appliance shell if account is not lockedProcedure Access the appliance shell and log in as a user who has a super administrator role. The default user with a super administrator role is root.login using where vsphere.local is your default SSO Domain.Run the localaccounts.user.password.update --username user name --password command. localaccounts.user.password.update --username root --passwordEnter and confirm the new password when prompted. More information: Managing Local User Accounts in vCenter Server. thumb_up Yes thumb_down No Has your vCenter root user password expired? Dont worry. Well walk you through the steps to fix this issue. Lets get started. Before we dive into the solution, its important to understand why the vCenter root user password expires. VMware vCenter Server, like many other systems, enforces password policies to enhance security. By default, the root user password is set to expire after a certain period. This is a standard security measure to ensure that passwords are regularly updated. However, if youre not prepared for this, it can catch you off guard. So, what can you do when you encounter this issue? First, you need to access the vCenter Server Appliance Management Interface (VAMI). To do this, open a web browser and navigate to . Replace your-vcenter-ip with the IP address of your vCenter Server. Once youre on the login page, enter the username as root and the current password. If the password has expired, youll see a message prompting you to change it. Passwords On the login page, youll see an option to change the password. Click on this link. Youll be prompted to enter the old password and then provide a new password. Make sure the new password meets the password policy requirements. After entering the new password, click on the Save button. If everything is entered correctly, youll receive a confirmation that the password has been successfully changed. Now that youve changed the password, its crucial to verify that it works. Log out of the VAMI and then log back in using the new password. If you can log in successfully, youve successfully updated the root user password. Sometimes, you might not be able to access the VAMI due to network issues or other reasons. In such cases, you can use the vSphere Client to change the password. Open the vSphere Client and log in with an account that has administrative privileges. Navigate to the Administration section and then select Single Sign-On followed by Users and Groups. Find the root user in the list of users and select it. Youll see an option to reset the password. Click on this option and follow the prompts to enter a new password. After changing the password, log out of the vSphere Client and log back in using the new password for the root user. If you can log in successfully, the password change was successful. Managing passwords in a vCenter environment can be challenging, but here are some tips to help you: Regularly review and update passwords to comply with security policies. Use a password manager to keep track of your passwords securely. Set up notifications for password expirations to avoid being locked out unexpectedly. If you forget the root password, you can still recover it. Heres how: Reboot the vCenter Server Appliance and access the console. During the boot process, press the e key when you see the GRUB menu. Add rw init=/bin/bash to the end of the kernel line. Press Ctrl + X to boot into single-user mode. Once youre in the shell, you can reset the root password using the passwd command. In the shell, type passwd and follow the prompts to enter a new password. After setting the new password, type reboot to restart the appliance. Once the appliance has rebooted, log in to the VAMI using the new password to ensure it works. Dealing with an expired vCenter root user password can be frustrating, but its a manageable issue. By following the steps outlined above, you can quickly resolve the problem and get back to managing your vCenter environment. As well as official support, you can also reach out to the VMware Forums should you need any further assistance. Remember to keep your passwords secure and up-to-date to avoid similar issues in the future. If you have any other questions or need further assistance, feel free to reach out. If you enjoyed this article, please consider subscribing to my email list! If your VMware vCenter Server Root Password has expired and you cant log in, dont panic. Our latest step-by-step guide shows how to reset the password even if you dont know the old one and how to configure expiration settings to avoid it next time. So, youre running your VMware infrastructure within your organization and one day you come to the office and you cannot login. Your root password for VMware vCenter Server Appliance (VCSA) has expired. What do you do? Which steps you need to proceed to change this password and also, well explain how to do a reset of this password in case you dont know it, for example you managing a virtual environment where the password is unknown. Well also explain why its important to use complex passwords.Note that resetting the root password of the vCenter Server Appliance is a relatively easy task, however, it requires restarting the vCenter Server virtual machine (VM). Lets dive into it.By default, the root password of the VCSA expires 90 days after the default deployment and installation of VCSA. So, if you dont configure it right away when you do the deployment, 90 days later youll find that you have a problem. Usually when that happens, youll find an option to change the root password on the login page. Youll have to provide the old root password, and then create a new one.How to change password expiration settingsIn the vCenter Server Management Interface, click Administration.In the Password section, click Edit.Configure the password expiration settings for the root user.vCenter server root password expiration settingsYou have the possibility to enter a new value for the password validity days and email for expiration warning.Root password validity (days) The number of days after which the password expires. The maximum is 9999 days.Email for expiration warning The email address to whichvCenter Server sends a warning message before the expiration date.If you want to change the PasswordClick the Change and then enter the current password, then create a new password. Enter the current password and the new password, then click Save.And thats it. You dont have the possibility to change the complexity for password requirements. At least not from the UI.What if you cant access Virtual Machine Management Interface (VAMI)?If thats the case, and you cant login into the VAMI, then change the password, you can use vSphere client and use the Single Sign-ON administrator password.Go to the Administration section and then go to Single Sign-ON and then Users and Groups.Change the root password from within vSphere web clientWell, and thats it.How you should manage your vCenter passwords on regular basis?You should review and update passwords to comply with security policies.Good practice is to use password manager to keep track of your passwords in a secure environment (not in digital txt format stored somewhere in the admins desktop.You could set up an outlook reminder which will prompt you to go and update your password avoiding you to be locked out. Well, if that happens, you can reset the root password via single user mode. How do you do that?Youll need to reboot the vCenter Server Appliance and access the console. During the boot process, press the e key when you see the GRUB menu. Add rw init=/bin/bash to the end of the kernel line.Reset root password of your VCSAPress F10 to continue booting.Type this:mount -o remount,rw /Press Enter.In the Command prompt, enter the commandpasswdand provide a new root password (twice for confirmation):passwdUnmount the filesystem by running this command (yes, the unmount command isumount its not a spelling error):umount /Reboot the vCenter Server Appliance by running this command:reboot -fConfirm that you can access the vCenter Server Appliance using the new root password.Note that this procedure is applicable for vCenter server 8.0U2 and higher. For lower vCenter server versions, such as 7.x, please head to the VMware/Broadcom KB here.Why using complex passwords?Have you ever wondered why the complexity of passwords matter? Use of a complex password helps to increase the time and resources required to compromise the password.Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.You should at least set this:From the vSphere Client, go to Administration > Single Sign On > Configuration > Local Accounts > Password Policy.View the value of the Character requirements setting.Character requirements: At least 1 lowercase charactersIf the password policy is not configured with Character requirements policy requiring 1 or more lowercase characters you should activate it.While you are there: Administration > Single Sign On > Configuration > Local Accounts > Password Policy.Click Edit. Edit password policies for local accounts via vSphere Web ClientSet lowercase characters to at least 1 and click Save.Final WordsWhen it comes to managing several clients virtual infrastructures, youll have to be organized. Remember that you should keep your passwords secure and up-to-date to avoid issues like this in the future.By following the steps above, you can quickly get out of troubles and resolve your problems and get back to manage your vCenter environment.While you can set your vCenter server password to Never Expire, you might follow your company security policy. If that password is a really strong password, you might consider disabling password expiration altogether.

Vmware vcenter appliance root password expired. Vmware vcenter server management password expired. Vmware root password expired. Vmware appliance os root password expired. Vmware appliance management root password expired. Vmware shd password expired. Vmware 7 root password expired. Vmware appliance root password expired. Vmware esxi root password expired. Vmware horizon failed changing expired password. Vmware esxi password expired. Vmware appliance management password expired. Vmware vcsa root password expired. Failed changing expired password vmware. Vmware cloud gateway password expired.