Default Accounts in VMware vSphere

VMware Compliance

Table of contents

Default Accounts in VMware vSphere

Introduction

Efforts in security and regulatory compliance frequently aim to compare the default settings of VMware vSphere components with the active configurations in a given environment. This document outlines the standard accounts present in a fresh installation of VMware ESXi and VMware vCenter Server.

Isolating services on the same operating system using distinct user accounts is a longstanding security practice. VMware employs this approach for its appliance services where feasible.

Although we strive to update this document for major and update versions, other product updates might alter the findings. The product available from VMware Customer Connect is the definitive source. If discrepancies arise between this document and your environment, compare with the version from VMware Customer Connect. We also appreciate feedback on discrepancies via the feedback mechanism at the top of this page.

Engineered solutions, including but not limited to HPE GreenLake and Dell VxRail, might introduce or modify local accounts in supported and acceptable ways. Details about these solutions are beyond the scope of this document and should be sought directly from the respective partners.

This document focuses on local and default accounts. While it's possible to configure the products for external authentication, like Microsoft Active Directory, accounts accessed in this way are not covered here.

Disclaimer

This document is intended to provide general guidance for organizations that are considering VMware solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided “AS IS.” VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

Intended Audience

This document is based on hyperconverged on-premises deployments of VMware vSphere 7.0.3 and 8.0.2, commonly referred herein to as vSphere 7 and vSphere 8, respectively. We urge readers to consistently apply patches and updates, as they are integral to maintaining a robust security stance.

Numerous engineered data center and hybrid cloud infrastructure products incorporate VMware vSphere in their solutions. If you use vSphere in this manner, consult the product's support if discrepancies arise.

For the latest version of this document, visit: https://via.vmw.com/scg

Feedback

Noticed an error, ambiguity, or have a suggestion for enhancement? We value your feedback. Kindly use the feedback tool at the top of this page to share your insights, which will direct your comments to the authors and site administrators.

ESXi Shell Access

Beginning in ESXi 8.0.0, local accounts can have their shell access disabled. This has two primary effects:

- That account cannot log in via SSH or the ESXi console.
- That account, no matter what privilege level it has, cannot alter the shell access parameters of other local accounts.

While the broader VMware ecosystem is familiar with most security controls in vSphere, newer controls can have unintended consequences. For instance, one might inadvertently lock out all administrative shell access and find traditional recovery methods ineffective due to Configuration Encryption and other security measures introduced since ESXi 7.0.2. Exercise caution when using these controls.

For more information consult the vSphere 8 Security Configuration & Hardening Guide before enabling.

ESXi Default Local Accounts

The VMware Hypervisor (VMware ESXi) ships with two built-in accounts, root and dcui, and when managed with VMware vCenter Server is commonly enabled with a third account, vpxuser.

root

The root account is created at installation. It is required for administration and is not removable.

The password can be changed both manually and programmatically through product UIs and APIs, as well as using the 'passwd' command at an ESXi shell. There is not a provision to automatically change or rotate the password.

The password is not a "default" as it is specified by the administrator at installation.

The password is subject to the ESXi password complexity and history parameters, such as Security.PasswordQualityControl. More information can be found in the vSphere Security Configuration & Hardening Guides.

The password is stored as a salted SHA512 hash, consistent with UNIX and UNIX-like operating systems.

Equivalent administrative access can be granted to alternate accounts added post-install for day-to-day use by vSphere administrators, so that log monitoring alerts (Log Insight et al) can be created for direct use of this account. It is not recommended to disable shell access for this account on ESXi 8.0.0 or newer.

dcui

The dcui account is created at installation. It is required for direct console service isolation and is not removable.

The password can be changed both manually and programmatically through product UIs and APIs, as well as using the 'passwd' command at an ESXi shell, though it is recommended to leave it locked. There is not a provision to automatically change or rotate the password.

There is no default password. The account is locked through the UNIX standard method of replacing the password in /etc/shadow with a value incompatible with a SHA512 hash (such as 'x' or '!' or '*').

The account should not have a password configured, but if one was, it would be subject to the ESXi password complexity and history parameters, such as Security.PasswordQualityControl. More information can be found in the vSphere Security Configuration & Hardening Guides.

The password, if set, would be stored as a salted SHA512 hash, consistent with UNIX and UNIX-like operating systems.

There are no reasons for vSphere administrators to log into ESXi in this manner. As such, this account may have its shell access removed in ESXi 8.0.0 and newer. More information can be found in the vSphere Security Configuration & Hardening Guides. Additionally, log monitoring alerts (Log Insight et al) can be set to alarm if this account is accessed.

vpxuser

The vpxuser account is created when ESXi is first attached to vCenter Server. It is required for administration by vCenter Server. To attach ESXi to vCenter Server the vSphere Administrator provides root or equivalent credentials. vCenter Server uses those credentials to create and secure the 'vpxuser' account. All subsequent access by vCenter Server is through vpxuser.

The password can, but should not, be changed manually via API, CLI, or UI, as vCenter Server will then need to be reconnected. vCenter Server will automatically rotate the password on an interval governed by the VirtualCenter.VimPasswordExpirationInDays advanced vCenter Server parameter, measured in days, with a minimum of 1 and default of 30 days.

The randomly generated password is 32 characters using four character classes (numbers, special characters, upper, and lower case). This password is randomly generated for each ESXi host.

The password is subject to the ESXi password complexity and history parameters, such as Security.PasswordQualityControl. More information can be found in the vSphere Security Configuration & Hardening Guides.

The password is stored as a salted SHA512 hash on ESXi, consistent with UNIX and UNIX-like operating systems. To enable management, vCenter Server stores the vpxuser password in an encrypted format inside the vCenter Server database on the vCenter Server Appliance.

This account is not removable and an alternate cannot be substituted. Shell access may be removed on ESXi 8.0.0 and newer but will impact management capabilities from vCenter Server. More discussion of this can be found above and in the vSphere Security Configuration & Hardening Guides. There are no reasons for vSphere administrators to log into ESXi with this account, so log monitoring alerts (Log Insight et al) can be set to alarm if this account is accessed from anywhere but vCenter Server.

vCenter Server Appliance Default Local Accounts

The VMware vCenter Server Appliance (VCSA) has numerous service accounts in order to isolate services. These accounts are required by the product and not removable.

Of these accounts, only root has a password set. The password is not a “default” as it is specified by the administrator at installation.

Local account passwords can be changed both manually and programmatically through product UIs and APIs, though it is recommended to leave the accounts locked. There are no provisions to automatically change or rotate passwords. It is possible to manage these passwords using standard Linux commands outside of the product UIs and APIs.

Accounts that are locked are locked through the UNIX standard method of replacing the password in /etc/shadow with a value incompatible with a SHA512 hash (such as ‘x’ or ‘!’ or ‘*’).

The passwords set on accounts are subject to the VCSA password quality settings which are visible in the VCSA Virtual Appliance Management Interface (VAMI). They are stored as salted SHA512 hashes, consistent with UNIX and UNIX-like operating systems.

vCenter Server 7

Accounts present on a “stock” installation of VMware vCenter Server 7 are as follows. Descriptions of the accounts and their purposes can be found in the GECOS field (field 5) in /etc/passwd.

analytics
apache
bin
certauth
certmgr
cis-license
content-library
daemon
deploy
dnsmasq
eam
envoy
imagebuilder
infraprofile
lookupsvc
messagebus
named
netdumper
nobody
ntp
observability
perfcharts
pod
pschealth
root
rpc
smmsp
sps
sshd
sso-user
systemd-bus-proxy
systemd-journal-gateway
systemd-journal-remote
systemd-journal-upload
systemd-network
systemd-resolve
systemd-timesync
tftp
topologysvc

trustmanagement
updatemgr
vapiEndpoint
vdtc
vlcm
vmafdd-user
vmcad-user
vmcam
vmdird
vmonapi
vpgmonusr
vpostgres
vpxd
vpxd-svcs
vsan-health
vsm
vsphere-ui
vstatsuser
vtsdbmonusr
vtsdbuser
wcp

vCenter Server 8

Accounts present on a “stock” installation of VMware vCenter Server 7 are as follows. Descriptions of the accounts and their purposes can be found in the GECOS field (field 5) in /etc/passwd.

analytics
apache
bin
certauth
certmgr
cis-license
content-library
daemon
deploy
dnsmasq
eam
envoy
envoy-hgw
envoy-sidecar
hvc
idmservice
imagebuilder
infraprofile
lighttpd
lookupsvc
messagebus
named
netdumper
nobody
ntp
observability
perfcharts
pod
postgres
pschealth
rhttpproxy
root
rpc

sca
smmsp
sps
sshd
sso-user
sts
systemd-bus-proxy
systemd-journal-gateway
systemd-journal-remote
systemd-journal-upload
systemd-network
systemd-resolve
systemd-timesync
tftp
topologysvc
trustmanagement
updatemgr
vapiEndpoint
vdtc
vlcm
vmafdd-user
vmcad-user
vmcam
vmdird
vmonapi
vpgmonusr
vpostgres
vpxd
vpxd-svcs
vsan-health
vsm
vsphere-ui
vstatsuser
vtsdbmonusr
vtsdbuser
wcp

vSphere Single Sign-On Default Accounts

VMware vSphere Single Sign-On components have four accounts present in a “stock” implementation: administrator, waiter-<UUID>, krbtgt, and K/M.

administrator

The administrator account is created at installation. It is required for administration and not removable.

The password can be changed both manually and programmatically through product UIs and APIs. There is not a provision to automatically change or rotate the password, nor manage it outside of the product UIs and APIs.

The password is not a “default” as it is specified by the administrator at installation.

The password is subject to the vSphere SSO password complexity and history settings, except for lockout, as the administrator account cannot be locked out. More information can be found in the vSphere Security Configuration & Hardening Guides.

The password is stored as a SHA512 hash in the SSO LDAP subsystem.

waiter-

The waiter account is created at installation. It is required for administration and not removable. Its name contains a UUID which, by definition, varies between installations.

The password can be changed both manually and programmatically through product UIs and APIs, though it is not recommended. In lieu of changing the password, the account can be disabled if the environment does not use the vSphere Auto Deploy feature.

The password is not a “default” but is a randomly generated 20 character password set at installation.

The password, when changed, is subject to the vSphere SSO password complexity and history settings. More information can be found in the vSphere Security Configuration & Hardening Guides.

The password is stored as a SHA512 hash in the SSO LDAP subsystem.

krbtgt

The krbtgt/VSPHERE.LOCAL (or your chosen SSO domain) account is created at installation. It is required for administration and not removable.

The password can be changed both manually and programmatically through product UIs and APIs, though it is not recommended. In lieu of changing the password, the account can be disabled if the environment does not use SASL/Kerberos authentication such as through Integrated Windows Authentication.

The password is not a “default” but is a randomly generated 20 character password set at installation.

The password, when changed, is subject to the vSphere SSO password complexity and history settings. More information can be found in the vSphere Security Configuration & Hardening Guides.

The password is stored as a SHA512 hash in the SSO LDAP subsystem.

K/M

The K/M account is created at installation. It is required for administration and not removable.

The password can be changed both manually and programmatically through product UIs and APIs, though it is not recommended. In lieu of changing the password, the account can be disabled if the environment does not use SASL/Kerberos authentication such as through Integrated Windows Authentication.

The password is not a “default” but is a randomly generated 20 character password set at installation.

The password, when changed, is subject to the vSphere SSO password complexity and history settings. More information can be found in the vSphere Security Configuration & Hardening Guides.

The password is stored as a SHA512 hash in the SSO LDAP subsystem.