XenServer

XenCenter®

cloud SOFTWARE GROUP

XenServer Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

About XenCenter® 45
Getting started 45
What's new in XenCenter® 46
What's new in 2026.4.1 46
Fixed Issues 46
Known issues in 2026.4.1 46
Earlier releases 47
What's new in 2026.4.0 47
Fixed Issues 47
What's new in 2026.3.0 47
Fixed Issues 48
What's new in 2026.2.1 48
Fixed Issues 48
What's new in 2026.2.0 48
Fixed Issues 49
What's new in 2026.1.0 49
Fixed Issues 49
What's new in 2025.5.0 50
Fixed Issues 50
What's new in 2025.4.0 51
What's New 51
Fixed Issues 52
What's new in 2025.3.0 52
What's New 52
Fixed issues 53
2025.2.1 54

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues 54
2025.2.0 54
What's New 54
Fixed issues 55
2025.1.0 56
What's New 56
Fixed issues 57
XenCenter 2024.4.0 57
What's New 57
Fixed issues 58
XenCenter 2024.3.1 58
What's new 58
Fixed issues 59
XenCenter 2024.3.0 59
What's new 59
Fixed issues 60
XenCenter 2024.2.1 60
What's new 61
Fixed issues 61
XenCenter 2024.2.0 61
What's new 61
Fixed issues 63
XenCenter 2024.1.0 63
What's new 63
Fixed issues 64
XenCenter 2023.4.0 65
What's new 65
Fixed issues 66

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenCenter 2023.3.2 66

What's new 66

Fixed issues 66

XenCenter 2023.3.1 66

What's new 66

Fixed issues 67

XenCenter 8.2.7 67

Installing XenCenter® 68

System requirements 68

Install XenCenter 68

Connect XenCenter to the XenServer host 69

Configure XenCenter to use an external SSH console 70

Uninstall XenCenter 70

Starting or Exiting XenCenter® 71

Starting XenCenter 71

Exiting XenCenter 71

Uninstalling XenCenter® 71

Uninstalling by using `msiexec` 72

Exploring the XenCenter® workspace 73

The Toolbar 74

Using the **Back** and **Forward** buttons on the **Toolbar** 74

Showing and hiding the **Toolbar** 75

The **Resources** Pane 75

The **Navigation** Pane 76

Infrastructure 77

Objects 77

Organization views 77

Objects by folder 78

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Objects by Tag 78

Objects by Custom Field 78

vApps 79

VM groups 79

Saved searches 79

Notifications 79

Alerts 80

Updates 80

Events 80

The Tabs 80

Citrix® 80

Console 81

Switch to Remote Desktop or **Switch to Default Desktop** 81

Switch to Graphical Console or **Switch to Text Console** 81

Open SSH Console 81

Send Ctrl+Alt+Del 81

Undock (Alt+Shift+U) 81

Find Console 82

Redock (Alt+Shift+U) or **Reattach Console** 82

Scale 82

Fullscreen (Ctrl+Enter) 82

General 83

GPU 83

High availability 83

Home 84

Memory 84

Networking 84

NICs 85

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Performance 85
Search 85
Snapshots 86
Storage 86
USB 87
Users 88
WLB 88
Resource Status Icons 88
Pools 88
Servers 89
Virtual machines, VM templates, and vApps 90
VM snapshots 91
Storage 91
Keyboard Shortcuts 92
Navigating XenCenter 92
Shortcut keys 92
Changing XenCenter® Options 93
Save and restore settings 93
Security settings 95
XenCenter Updates settings 96
Confirmations settings 96
Display settings 97
Console settings 97
Connection settings 100
Proxy server 100
Connection timeout 101
Active Directory 101
External Tools settings 101

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hidden Objects 101
Organizing Resources 102
Using Folders 102
To create a folder 102
To move resources into and out of folders 103
To rename a folder 103
To delete a folder 103
Using Tags 104
To create a tag 104
To delete a tag 104
To tag a resource 105
To untag a resource 105
Using Custom Fields 105
To create a custom field 106
To assign a value to a custom field on a resource 106
To delete a custom field 106
Searching Resources 107
Create a Search Query 107
To create a search query 107
Filter and Group Search Results 108
To filter your search results 108
To group search results 109
Saved Searches 109
To apply a saved search 109
To delete a saved search 110
Export and Import Searches 110
To export the current search 110
To import a search 110

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To save the imported search as a new custom search 110
About XenServer® Licensing 111
Related documentation 111
XenServer Current Release 111
Licensing Overview 111
Citrix® Licensing 112
Licensing XenServer servers 113
License expiry 113
License grace period 113
Related documentation 114
XenServer Current Release 114
Managing XenServer® Licenses 114
Available licenses 114
To discover the license status of servers and pools 115
Check licensing details 115
To assign a XenServer license 116
To release a XenServer license 117
Related documentation 117
XenServer Current Release 117
Citrix® integration 118
Feedback 118
Compatibility 118
Limitations 119
Citrix Virtual Apps and Desktops permissions 119
Connect to Citrix 119
Remove a Citrix connection 120
Pools and Citrix® 120
Citrix tab 120

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Overview 120

General 121

Sessions 121

Machine Catalogs 121

Delivery Groups 122

Machines 122

Hosts and Citrix® 122

Citrix tab 122

Overview 123

General 123

Sessions 123

Machine Catalogs 124

Delivery Groups 124

Machines 124

Warnings 125

VMs and Citrix® 125

Citrix tab 125

Overview 125

General 125

Machine Catalog 126

Delivery Group 126

Sessions 126

Warnings 127

Managing Servers 128

Connecting and disconnecting 128

Configuring networking 128

More information 128

Connecting and Disconnecting Servers 129

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add a server 129
To add a server to XenCenter 129
Security Certificates 130
Disconnect a Server 130
Reconnect a Server 131
To reconnect to a connected server using different login credentials 131
Reboot a Server 131
To reboot a server 132
Shut Down a Server 132
To shut down a server 132
Restart Toolstack 132
To restart the toolstack 133
Configuring Host Power On 134
Prerequisites for Host Power On 134
To enable or disable Host Power On 135
Related documentation 136
Power on a server remotely 136
Related documentation 136
Run in maintenance mode 136
To place a server in maintenance mode 137
To take a server out of maintenance mode 137
Related documentation 137
Install a TLS certificate on your server 137
Requirements 138
Install a certificate 138
View certificate information 139
Enabling certificate verification for your pool 139
Reset server identity certificates 140

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Certificate alerts 140
Related documentation 140
Store Your Server Connection State 141
To turn automatic reconnection on or off 141
Using a main password 141
Back up and Restore a Server 142
To back up your server configuration and software 143
To restore server software and configuration from backup 143
Related documentation 143
Remove a Server From XenCenter® 143
Configuring Networking 144
Network types 144
Single-Server private network 144
External network 144
Bonded network 145
Notes 145
Related documentation 146
XenServer Current Release 146
Add a network 146
To add an external network 146
To add a single-server private network 147
To add a new bonded network 147
To add an SR-IOV Network 149
Related documentation 149
Remove a Network 149
Related documentation 149
View and Change Network Properties 150
To view a server's current networking configuration 150

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To change a server's networking configuration 150
Related documentation 152
Configuring NICs 152
Viewing available NICs 153
To create a NIC bond 153
Deleting a NIC bond 155
Dedicating a NIC to a specific function 155
Related documentation 155
Configuring IP Addresses 155
To assign an IP address to a NIC 156
To remove a secondary interface 157
To change the management interface 157
Related documentation 158
Managing SSH and Console Sessions 158
Overview 158
Benefits 159
Enabling SSH Access 159
Disabling SSH Access 159
Bulk Operations 160
View Server Properties 160
General 160
Certificates 160
License Details 161
Version Details 161
Updates 161
Management Interfaces 161
Memory 162
CPUs 162

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GFS2 Clustering Status 162
SSH Access 162
Changing Server Properties 162

General properties - Name, Description, Folder, and Tags 162

iSCSI IQN (General tab) 163
To change the iSCSI IQN value for a managed server 163

Custom Fields 163

Alerts 164

Email Notifications (standalone servers) 164

Multipathing 164

Power on (standalone servers) 164

Drivers 164

Log Destination 165
To specify a remote XenServer log destination 165

GPU 165
Placement Policy 165
Integrated GPU pass-through 166

NRPE 166

SNMP 167
Console 167
Servers in pools 167

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Standalone servers 168
Changing the Control Domain Memory 169
To update the dom0 memory 169
Related documentation 170
XenServer Current Release 170
Exporting and Importing a List of Managed Servers 170
To export your list of managed servers 170
To import a list of servers 170
Managing Pools 171
Related documentation 171
XenServer Current Release 171
Pool Requirements 171
Hardware requirements 171
Other requirements 172
Homogeneous pool 172
Heterogeneous pool 173
Shared pool storage 174
Related documentation 174
XenServer Current Release 174
Create a New Pool 174
To create a pool 174
More pool configuration steps 176
Related documentation 176
XenServer Current Release 176
Add a Server to a Pool 176
To add a server to an existing pool 176
To place a server in a new pool 178
Related documentation 178

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenServer Current Release 178
Remove a Server From a Pool 178
Related documentation 178
XenServer Current Release 178
Destroy a server from a pool 179
Export Resource Data 179
Resource Data 180
Server 180
Networks 180
VDI 180
Storage 181
VMs 181
GPU 182
View Pool Properties 182
General 182
Certificates 183
Updates 183
Management Interfaces 183
GFS2 Clustering Status 183
SSH Access 184
Change Pool Properties 184

General properties - name, description, folder, tags 184

Custom fields 184

Email options 185

Power on 185


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Drivers 185


GPU 186


Security 186


Live patching 186


Network 187


GFS2 Clustering 187


Global VM Options 188

Performance enhancements 188

Automatic Secure Boot certificate updates 188


NRPE 188


SNMP 189

Console 190

Pool security 190

Change the root password 190

Rotate the pool secret 191

Related documentation 191

XenServer Current Release 191

Delete a Pool 191

Managing Storage 192

Related documentation 193

XenServer Current Release 193

Creating a New SR 193

SR creation steps 193

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation 195
XenServer Current Release 195
NFS Storage 195
To configure an NFS SR 195
Related documentation 196
Software iSCSI Storage 196
To create a software iSCSI SR 196
Related documentation 198
Hardware HBA Storage 198
To create a hardware HBA SR 198
Related documentation 199
SMB Storage 199
To configure an SMB SR 200
Related documentation 200
Software FCoE Storage (deprecated) 201
To create a Software FCoE SR 201
Related documentation 202
ISO Storage 202
To configure a new ISO SR on NFS storage 202
To configure a new ISO SR on CIFS/SMB storage 203
Related documentation 203
Thin-provisioned shared GFS2 block storage 204
1. Plan your GFS2 environment 204
2. Configure redundant networking infrastructure 205
3. Create a dedicated bonded network 205
4. Set up a GFS2 clustered pool 208
5. Increase your control domain memory 209
6. Configure storage multipathing 209

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Create a GFS2 SR 210
Constraints 213
Related documentation 214
Storage properties 214
Viewing storage properties 214
General 214
Storage 215
Search 215
Changing SR properties 215
General 215
Custom fields 216
Alerts 216
Read Caching 216
Related documentation 217
XenServer Current Release 217
Removing an SR 217
To detach a storage repository 217
To forget a storage repository 218
Related documentation 218
XenServer Current Release 218
Reattaching an SR 219
To reattach a detached SR 219
Related documentation 219
XenServer Current Release 219
Storage Multipathing 219
To enable multipathing 220
Related documentation 220
XenServer Current Release 220

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Storage Read Caching 221
To disable read caching 221
To enable read caching 222
Related documentation 222
XenServer Current Release 222
PVS-Accelerator 222
Enable PVS-Accelerator 222
Configure PVS-Accelerator in XenServer 223
Complete the cache configuration in PVS 224
Cache operation 224
Related documentation 225
XenServer Current Release 225
Reclaiming Freed Space 225
Related documentation 226
XenServer Current Release 226
Live LUN Expansion 226
Related documentation 227
XenServer Current Release 227
Corosync Upgrade Wizard 227
Overview 227
Before you Start 227
Pre-Checks 227
Upgrade process 227
XenCenter RPU behavior during upgrade 228
Creating VMs 229
XenServer® VM Tools 229
Using templates 230
Related documentation 230

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenServer Current Release 230
Creating a New VM 231
Overview of VM creation steps 231
Related documentation 234
XenServer Current Release 234
VM Template and BIOS Options 234
Select a BIOS option 234
Related documentation 235
VM Name and Description 235
Related documentation 236
OS Installation Media 236
OS installation media options 236
Boot mode 236
vTPM 237
Related documentation 237
Home Server 237
Workload Balancing (WLB) and Virtual GPU considerations 238
Related documentation 238
VM Group 238
Related documentation 240
VM CPU and Memory Allocation 240
Options 240
VM power state scenarios 242
Related documentation 242
GPU 242
Enabling Intel GPU pass-through 244
Related documentation 245
Virtual Storage Configuration 245

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Options 245
Related documentation 246
Virtual Networking Configuration 246
Related documentation 247
Complete New VM Creation 247
Related documentation 247
Express (unattended) VM Creation 247
Related documentation 248
XenServer Current Release 248
Creating New Templates 248
To convert an existing VM into a template 248
To save a copy of a snapshot as a new template 248
To import a template from an XVA file 249
Export a Template to a File 249
To export a template to a file 249
Related documentation 250
XenServer Current Release 250
Copying VMs and Templates 250
Copying a VM 250
To copy a VM within the pool 250
To copy a VM to a different pool 251
Copying a template 252
To copy a template within the pool 252
To copy a template to a different pool 252
Related documentation 253
XenServer Current Release 253
Configuring VMs 254
Installing XenServer® VM Tools 254

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenServer VM Tools for Windows 254
XenServer VM Tools for Linux 255
Finding out the virtualization state of a VM 256
Updating XenServer VM Tools 257
Updating the I/O drivers 257
Updating the Management Agent 258
Related documentation 258
XenServer Current Release 258
Configuring Virtual Storage 258
Related documentation 259
XenServer Current Release 259
Add Virtual Disks 259
Related documentation 260
Attach Virtual Disks 260
Related documentation 260
Detach Virtual Disks 261
Related documentation 261
Move Virtual Disks 261
About storage live migration 262
To move a virtual disk 262
Related documentation 262
Delete Virtual Disks 263
Related documentation 263
Change Virtual Disk Properties 263
General properties - name, description, folder, tags 263
Custom fields 264
Disk size and location 264
Device options 264

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation 265
Configuring VM Networking 265
Add a Virtual Network Interface 266
Related documentation 266
Activate/deactivate a Virtual Network Interface 266
Related documentation 267
Remove a Virtual Network Interface 267
Related documentation 267
Change Virtual Network Interface Properties 267
Related documentation 268
Configuring Virtual GPU 268
Related documentation 269
XenServer Current Release 269
Configuring VM Memory 269
Dynamic Memory Control (DMC) 269
Dynamic and static memory range 270
DMC memory constraints 271
To enable DMC 271
To disable DMC 271
Related documentation 272
XenServer Current Release 272
View VM Properties 272
General 272
Boot Options 273
CPUs 273
Read Caching 273
Device Security 273
Updates 273

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Change VM Properties 274
General 274
Custom fields 274
CPU and memory 274
Number of vCPUs (for Windows VMs) 274
Maximum number of vCPUs (for Linux VMs) 275
Topology 275
Current number of vCPUs (for Linux VMs) 275
vCPU priority for this virtual machine 275
Boot options 275
Start options 276
Start order 276
Attempt to start next VM after 276
HA restart priority 276
Alerts 277
Home server 277
GPU 277
USB 278
Related documentation 278
XenServer Current Release 278
Managing VMs 279
Start a VM 279
To start a VM on a specific server 279
To start the VM on the optimal or home server 280
Related documentation 280
XenServer Current Release 280
Suspend and Resume a VM 280
To suspend a VM 280

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To resume a suspended VM 281
To resume a suspended VM on a specific server 281
To resume the VM automatically on the optimal or home server 281
Related documentation 282
XenServer Current Release 282
Shut Down a VM 282
To perform a soft shutdown 282
To perform a forced shutdown 283
Related documentation 283
XenServer Current Release 283
Reboot a VM 283
To reboot a VM cleanly 284
To do a forced reboot 284
Related documentation 284
XenServer Current Release 284
Restart the VM device model 285
To restart the device model 285
Run a Remote Console Session 285
Linux VMs 285
SSH console 286
Windows VMs 286
Manage VM groups 287
Manage VM groups dialog 288
Create a VM group 289
Delete a VM group 289
Update the properties of a VM group 290
Related documentation 290
XenServer Current Release 290

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migrate Virtual Machines 290
Live migration 290
Storage live migration 291
Compatibility requirements 292
Live migration and storage live migration limitations 293
Move VMs 293
To migrate or move a VM 294
Related documentation 295
XenServer Current Release 295
Delete a VM 295
Related documentation 296
XenServer Current Release 296
Changed Block Tracking 296
Disabling changed block tracking on a VM 296
Viewing the changed block tracking status for a VDI 297
Secure Boot Certificates 297
Review certificate state in XenCenter 297
Flag or unflag VMs for certificate update 298
Importing and Exporting VMs 299
Supported import and export formats 299
Which format to Use? 300
(Windows VMs only) Installing XenServer VM Tools for Windows 300
(Linux VMs only) Operating System Fixup 300
Operating System Fixup requirements 301
Open Virtualization Format (OVF and OVA) 301
What's in an OVF package? 302
Which format do I use? 303
(Windows VMs only) Installing XenServer® VM Tools for Windows 303

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(Linux VMs only) Using Operating System Fixup 303
More information about OVF 303
Related documentation 303
XenServer Current Release 303
Disk Image Formats (VHD, VHDX, AVHDX, and VMDK) 304
Supported disk image formats 304
(Windows VMs only) Installing XenServer® VM Tools for Windows 305
(Linux VMs only) Using Operating System Fixup 305
Related documentation 305
XenServer Current Release 305
Import VMs From OVF/OVA 306
Prerequisites 306
Import an OVF package 306
Errors when trying to start an imported VM 309
Related documentation 309
XenServer Current Release 309
Import VMs From Disk Images 309
Prerequisites 309
Import a disk image 310
Next steps 313
Related documentation 313
XenServer Current Release 313
Import VMs From XVA 313
Prerequisites 314
Import an XVA package 314
Related documentation 315
XenServer Current Release 315
Export VMs as OVF/OVA 315

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites 315
Export an OVF/OVA package 316
Export VMs as XVA 317
Prerequisites 317
Export an XVA package 317
About Snapshots 319
Types of snapshots 319
Disk-only snapshots 319
Disk and memory snapshots 319
Accessing orphaned snapshots 320
Related documentation 320
XenServer Current Release 320
Take a VM Snapshot 320
Related documentation 321
XenServer Current Release 321
Revert to a Snapshot 321
Related documentation 321
XenServer Current Release 321
Create a New VM From a Snapshot 321
To create a VM from a snapshot 322
To create a VM from an orphan snapshot 322
Related documentation 322
XenServer Current Release 322
Create a New Template From a Snapshot 322
To save a snapshot as a new template 322
To save an orphan snapshot as a new template 323
Related documentation 323
XenServer Current Release 323

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Export a Snapshot to a File 323
To export a snapshot to a file 323
To export an orphan snapshot 323
Related documentation 324
XenServer Current Release 324
Delete a Snapshot 324
To delete a snapshot 324
To delete an orphan snapshot 324
Related documentation 324
XenServer Current Release 324
Scheduled Snapshots 324
Related documentation 325
XenServer Current Release 325
Create Scheduled Snapshots 325
Related documentation 326
Manage scheduled snapshots 326
Enabling a snapshot schedule 326
Disabling a snapshot schedule 327
Editing a snapshot schedule 327
Deleting a snapshot schedule 328
Related documentation 328
Revert VMs to Snapshots 328
Related documentation 328
XenServer® vApps 329
Using the **Manage vApps** dialog box 329
Related documentation 330
XenServer Current Release 330
Create a vApp 330

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation 331
XenServer Current Release 331
Modify vApps 331
Using the **Manage vApps** dialog 331
Related documentation 332
XenServer Current Release 332
Delete a vApp 332
Related documentation 333
XenServer Current Release 333
Start and Shut Down vApps 333
To start a vApp 333
To shut down a vApp 333
Related documentation 334
XenServer Current Release 334
Export and Import vApps 334
To export a vApp 334
To import a vApp 334
Related documentation 335
XenServer Current Release 335
Protecting VMs and vApps 336
High Availability 336
Disaster recovery 336
Related documentation 337
XenServer Current Release 337
High availability 338
Heartbeats for availability 338
Server fencing 339
Capacity planning for failure 340

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Overcommit protection 341
Working with an HA-enabled pool 341
High availability and role-based access control (RBAC) 342
Related documentation 342
XenServer Current Release 342
High availability Requirements 342
Related documentation 343
XenServer Current Release 343
VM Restart Settings 343
High availability restart priority 343
Start order 344
Delay interval (Attempt to start next VM after) 344
Related documentation 344
XenServer Current Release 344
Configure high availability 344
Related documentation 346
XenServer Current Release 346
Disable high availability 346
Related documentation 346
XenServer Current Release 346
Enable high availability 346
Related documentation 347
XenServer Current Release 347
Change High Availability settings 347
To change high availability restart priority and VM startup sequence settings 347
To change the server failure limit for a pool 348
To increase the maximum failure capacity for a pool 348
Related documentation 349

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenServer Current Release 349
Disaster Recovery (DR) 350
Understanding DR 350
Disaster recovery terminology 351
Disaster recovery infrastructure 351
Failover, failback, and test failover with the **Disaster Recovery** wizard 352
Failover 352
Failback 353
Related documentation 354
XenServer Current Release 354
Configuring disaster recovery 354
Related documentation 355
XenServer Current Release 355
Failover 355
Related documentation 357
XenServer Current Release 357
Failback 357
Related documentation 358
XenServer Current Release 358
Test Failover 358
Related documentation 360
XenServer Current Release 360
Access Control (AD and RBAC) 361
Related documentation 361
XenServer Current Release 361
Managing Users 361
AD authentication in XenServer environment 362
Related documentation 363

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenServer Current Release 363
Role Based Access Control overview 363
Using Active Directory accounts for XenServer user accounts 363
RBAC process 364
Local super user 364
RBAC roles 365
Related documentation 366
XenServer Current Release 366
Definitions of RBAC roles and permissions 366
Join a domain and add users 366
Secure LDAP (LDAPS) 367
To join the XenServer or pool to a domain 367
To add an Active Directory user or group to a pool 368
To leave the domain 368
Related documentation 369
XenServer Current Release 369
Assign roles to users and groups 369
To change or assign a role to a user or group 369
Related documentation 370
XenServer Current Release 370
Calculating RBAC roles 370
When I log in, how does XenServer® compute the roles for the session? 370
Related documentation 371
XenServer Current Release 371
Audit changes 372
Related documentation 372
XenServer Current Release 372
Workload Balancing Overview 373

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation 374
XenServer Current Release 374
Getting Started with Workload Balancing 374
Related documentation 374
XenServer Current Release 374
Workload Balancing Basic Concepts 375
Related documentation 375
Connecting to Workload Balancing 375
Prerequisites 376
To connect to the Workload Balancing virtual appliance 376
Related documentation 378
Introduction to basic tasks 378
Determining the best host on which to start a VM 378
Accepting Workload Balancing recommendations 379
Related documentation 379
XenServer Current Release 379
Choosing an optimal server for VM initial placement, migrate, and resume 379
How do placements work? 380
What does optimal mean? 380
To start a virtual machine on the optimal server 381
To resume a virtual machine on the optimal server 381
Related documentation 382
Accepting Optimization Recommendations 382
Basis for optimization recommendations 382
To accept an optimization recommendation 383
Understanding WLB recommendations under High Availability 383
Related documentation 384
Working with Workload Balancing Reports 384

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Types of reports 384
Generating reports 384
Related documentation 384
XenServer Current Release 384
Using Workload Balancing Reports for Tasks 384
Evaluating the effectiveness of your performance thresholds 385
Troubleshooting administrative changes 385
Related documentation 385
Generating and Managing Workload Balancing Reports 385
To generate a Workload Balancing report 385
To navigate in a Workload Balancing report 386
To print a Workload Balancing report 386
To export a Workload Balancing report 387
Related documentation 387
Workload Balancing Report Glossary 387
Chargeback utilization analysis 387
Host health history 391
Pool optimization performance history 392
Pool audit trail 392
Pool Health 394
Pool health history 395
Pool optimization history 395
Virtual machine motion history 396
Virtual Machine Performance history 396
Related documentation 397
Audit Log Events 397
Related documentation 399
Editing Workload Balancing Settings 399

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How Workload Balancing settings apply 400
To display the Workload Balancing settings dialog box 400
Related documentation 401
XenServer Current Release 401
Adjusting the Optimization Mode 401
To set an optimization mode for all time periods 402
To specify times when the optimization mode changes automatically 402
To delete or pause a scheduled optimization mode task 402
To edit a scheduled optimization mode task 403
Related documentation 403
Optimizing and Managing Power Automatically 403
Accepting optimization recommendations automatically 403
Enabling Power Management 404
Understanding Power Management behavior 404
Designing environments for Power Management and VM consolidation 406
To apply optimization recommendations automatically 406
To select servers for power management 407
Related documentation 408
Changing the Critical Thresholds 408
Overview 408
Default settings for thresholds 409
How other thresholds trigger recommendations 410
To change the critical thresholds 411
Related documentation 411
Tuning Metric Weightings 411
How metric weightings apply in Maximum Performance mode 412
How metric weightings apply in Maximum Density mode 412
To edit metric weighting factors 413

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation 413
Excluding Hosts from Recommendations 413
When to exclude hosts 413
To exclude hosts from placement and optimization recommendations 414
Related documentation 414
Excluding VMs from Recommendations 414
When to exclude VMs 414
To exclude VMs from placement and optimization recommendations 415
Related documentation 415
Advanced Settings 415
VM migration interval 416
Recommendation count 416
Recommendation severity 418
Optimization aggressiveness 418
To configure virtual machine recommendation intervals 419
Pool audit trail granularity 420
Related documentation 420
Administering Workload Balancing 420
Related documentation 421
XenServer Current Release 421
Disconnecting from Workload Balancing 421
To disconnect from Workload Balancing 421
Related documentation 422
Reconfiguring a Pool to Use Another WLB Appliance 422
To use a different Workload Balancing appliance 422
Related documentation 423
Updating Workload Balancing credentials 423
To disconnect from Workload Balancing 423

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To reenable Workload Balancing and specify the new credentials 423
Related documentation 424
Entering maintenance mode with Workload Balancing Enabled 424
To enter maintenance mode with Workload Balancing enabled 425
To take the server out of maintenance mode 425
Related documentation 425
Troubleshooting Workload Balancing 426
General troubleshooting tips 426
Error messages 426
Related documentation 426
XenServer Current Release 426
Issues Entering Workload Balancing Credentials 426
Related documentation 427
Issues Starting Workload Balancing 427
Related documentation 427
Issues with Workload Balancing certificates 427
Related documentation 428
Workload Balancing Connection Errors 428
Related documentation 428
Issues changing Workload Balancing servers 429
Related documentation 429
Conversion Manager 430
Supported guest operating systems 431
Understand XenServer 431
Compare VMware and XenServer terminology 431
Conversion overview 432
Summary of how to convert VMs 434
Related documentation 434

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenServer 9 434
What's new in Conversion Manager 434
What's new in 2026.1.0 435
Earlier releases 435
Conversion Manager 8.5.0 435
Conversion Manager 8.4.0 436
Conversion Manager 8.3.1 437
Get started with Conversion Manager 437
Prepare your environment 437
Install XenServer and create a pool 438
XenServer environment considerations 438
Import and configure the virtual appliance 443
Download the virtual appliance 443
Import the virtual appliance into XenServer 444
Configure the Conversion Manager virtual appliance 445
Convert VMware ESXi/vCenter VMs 446
Post-conversion tasks 450
Reactivate the Windows License on Windows VMs 450
Reboot your Windows VMs 450
Other conversion tasks 450
Troubleshoot Conversion Manager 451
Problems starting a converted VM 452
Blue screen with Windows STOP code 0x0000007B 452
Windows product activation 452
Lost network settings in a Windows VM 452
Unable to start VMware SCSI disk 452
Problems during conversion 453
Monitoring System Performance 454

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitor system performance with XenCenter® 454
Monitor system performance with NRPE 455
Monitor system performance with SNMP 455
Related documentation 455
XenServer Current Release 455
Viewing Performance Data 456
To view data from a longer or shorter time period 456
To view data from a different time period 457
To view VM lifecycle event data on a server 457
Configuring Performance Graphs 458
To add a graph 458
To edit a graph 458
To delete a graph 458
To reorder a graph 458
To change datasource color in graphs 458
To Change the graph type 459
NUMA optimization in XenCenter 459
Overview 459
Where to view NUMA status 459
Indicators 460
Enable metrics 460
Guidance and considerations 460
Monitoring host and dom0 resources with NRPE 460
Prerequisites 465
Constraints 465
Configure NRPE by using XenCenter 466
Related documentation 467
XenServer Current Release 467

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitoring host and dom0 resources with SNMP 468
Metric objects 468
Traps 470
Prerequisites 471
Constraints 472
Configure SNMP by using XenCenter 472
Related documentation 473
XenServer Current Release 473
Configuring Performance Alerts 474
Updates and Upgrades 477
Update your version of XenCenter® 477
Upgrade your hosts 477
Update XenServer® hosts 477
Related documentation 478
XenServer Current Release 478
Upgrade your hosts 478
Important: Before you upgrade 479
To upgrade XenServer using the **Rolling Pool Upgrade** wizard 480
Related documentation 482
XenServer Current Release 482
Update your XenServer® hosts 482
Configure updates for your pool 483
Updates from the CDN 483
Offline Updates 486
Update from a remote pool 487
Configure a remote pool as an update channel 487
View available updates for your pool 489
By server 490

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By update 492
Understand the guidance categories and update tasks 493
Guidance categories 493
Update tasks 495
Apply updates to your pool 496
Before you start 497
Install updates 497
Updates from the CDN 497
Offline Updates 498
Complete any pending update tasks 500
Related documentation 502
XenServer Current Release 502
Live patches 502
Live patching scenarios 503
Update XenCenter® 503
Update Notifications 504
Enable XenCenter® notifications 504
Prerequisites 504
Enable update notifications for your hosts 505
Install supplemental packs 506
To install a supplemental pack using XenCenter® 506
Related documentation 507
XenServer Current Release 507
Install driver disks 507
Install a driver disk by using XenCenter 508
Related documentation 508
XenServer 8.4 508
XenCenter® Alerts 509

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Working with alerts 510
Filter by Severity 510
Filter by Location 510
Filter by Date 510
Refresh 510
Export All 510
Dismiss All 511
Actions 511
Receiving alert notifications by email 511
To turn on email notifications 512
Receiving alert notifications with SNMP 512
Troubleshooting 513
Related documentation 513
XenServer Current Release 513
Using the XenCenter® Event Log 513
Viewing events in the current session 513
Viewing the XenCenter event log file 513
Working with events in the current session 514
Filter by status 514
Filter by server 514
Filter by Date 514
Dismiss All 514
Actions 514
Creating a Server Status Report 515
To generate a server status report 515
Related documentation 516
XenServer Current Release 516
Resolving SR Connectivity Problems 516

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation 517

XenServer Current Release 517

Getting Help 518

XenCenter® Document History 519

fix 523

© 1997–2026 Citrix Systems, Inc. All rights reserved.

About XenCenter®

XenCenter provides a rich user experience to manage multiple XenServer® hosts, resource pools, and the entire virtual infrastructure associated with them.

With XenCenter, you can manage your XenServer environment and deploy, manage, and monitor virtual machines from your Windows desktop machine.



This article assumes you've already installed XenServer on your server hardware.

Getting started

Let's get started with the XenCenter management console:

1. You can install XenCenter on most Windows systems, as long as your system has .NET 4.8 or later installed. For more information, see System requirements.
2. To install XenCenter, run the installer file you downloaded from our website. The installer guides you through the installation process. For more information, see Install XenCenter.
3. Now that you have XenCenter installed on your Windows system, take a moment to get familiar with the layout of the UI and its capabilities. For more information, see Exploring the XenCenter workspace.
4. Connect XenCenter to your XenServer hosts and start to manage them. For more information, see Add New Server.
5. Create XenServer storage repositories (SR) and attach them to your hosts with the **New SR** wizard. SRs provide storage that can be shared between managed servers. For more information, see Add New Storage.
6. Group managed servers together into a resource pool with shared storage using the **New Pool** dialog. For more information, see Create a New Pool.
7. Create VMs in your pools with the **New VM** wizard. For more information, see Create a New VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new in XenCenter®

XenCenter is updated independently of the version of XenServer. To remain supported, ensure that you are using the latest XenCenter version.

NOTE:

Unless otherwise specified, the XenCenter articles apply to XenServer® 8.4 or greater releases, even if only XenServer 8.4 is explicitly mentioned.

You can download XenCenter YYYY.x.x from the XenServer downloads page.

After installing a version of XenCenter YYYY.x.x, you can receive further updates to XenCenter automatically. For more information, see Updating XenCenter.

What's new in 2026.4.1

This update contains the following enhancement:

- XenCenter now offers the option to automatically flag newly created VMs for Secure Boot certificate update.

Fixed Issues

- If there are pending post-update tasks on a VM that has disk and memory snapshots, XenCenter erroneously shows the same post-update tasks for the snapshots. (CA-425866)

Known issues in 2026.4.1

- After a standalone host is rebooted, including when it's rebooted after applying updates, the host's **General** tab does not display the status of the system correctly. We recommend that you refresh the host's **General** tab by clicking a different object and back on the host, or by disconnecting and reconnecting.
- Changing the font size or dpi on the computer on which XenCenter is running can result in the user interface appearing incorrectly. The default font size is 96 dpi. Windows 10 refers to this font size as 100%. (CA-45514)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **VM Export** wizard preserves the original MAC address of the exported VM. In addition, the **VM Import** wizard allows import of a VM with a duplicate MAC address. This combination of behaviors can cause IP address conflicts if the original and imported VMs are served by the same DHCP server. To work around this issue, select "Auto-generate a MAC address" after import. (CP-53982)
- In XenCenter, when you attempt to import an OVF package or a disk image from a folder containing a hash character (#) in its name, the import fails with a null reference exception. (CA-368918)
- When attempting to run XenCenter from the command line while XenCenter is already running, any arguments with whitespace characters must be wrapped in both double and single quotes: '"example"'. (CA-389317)
- XenCenter can't verify the certificate when importing an OVF file. It fails with the error message "Signature verification failed." (CA-413933)
- If you attempt to cancel the import of an XVA file from the **Import Wizard**, XenCenter can crash. (CA-415171)

Earlier releases

This section lists features in previous releases along with their fixed issues. These earlier releases are superseded by the latest version of XenCenter. Update to the latest version of XenCenter when it is available.

What's new in 2026.4.0

Fixed Issues

- This update includes security fixes. For more information, see the Security Bulletin.

What's new in 2026.3.0

This update contains the following improvements:

- XenCenter now allows administrators to identify and schedule remediation for virtual machines (VMs) whose UEFI NVRAM only contains the legacy Microsoft 2011 UEFI Secure Boot certificate chain. See Secure Boot Certificates for more information.
- If SSH access is enabled on a system running XenServer 9, XenCenter now shows a warning on the pool's and the hosts' **General** tab.
- Functionality enhancements in the **New Conversion** wizard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed Issues

- XenCenter fails to import an OVF/OVA package containing VMs with more than 10 virtual disks. (XSI-2253)
- Sometimes XenCenter fails to connect to a Windows VM using Remote Desktop and shows a blank screen. (CA-418659)
- On occasion, the user is unable to type in XenCenter's search boxes. (XSI-2107)
- Miscellaneous user experience and context help improvements. (CP-310388, CA-425526)

What's new in 2026.2.1

This update contains the following improvements:

- XenCenter now allows enabling jumbo frames on the management network.
- XenCenter now displays the vCPU:CPU ratio on the server's **General** tab.
- In addition to a NIC's index, XenCenter now shows the NIC's name on the server's **NICs** tab.

Fixed Issues

- Sometimes XenCenter can crash after adding a server to a pool. (CA-426861)
- Adding an unlicensed server to a licensed pool fails due to failure to automatically apply the license to the joining server. (CA-428040)
- When the connection to a server is lost due to a server reboot, XenCenter can give up reconnecting too quickly. (CA-422352)
- Miscellaneous user experience issues. (CP-311878, CP-312720)

What's new in 2026.2.0

This update contains the following new features:

- XenCenter now offers certificate validation for the License Server.
- When upgrading to a new version, XenCenter includes enhanced pre-checks that issue a warning if the post-upgrade memory footprint of a XenServer host increases.

This update includes the following changes of behavior:

- XenCenter no longer provides the ability to install hotfixes from local media to Citrix Hypervisor 8.2 Cumulative Update 1. This does not affect the ability to upgrade to XenServer 8.4.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed Issues

- XenCenter displays the wrong license type for supporter hosts. (CA-425178)
- When importing disk images in air-gapped environments, XenCenter prevents uploading XenServer VM Tools files to the Conversion Manager virtual appliance. (CA-424791)
- Connection to a server can time out when XenCenter displays a warning whenever a new or modified certificate is found on the server. (CA-382627)
- Miscellaneous user experience issues. (CA-425615, CA-423745, CA-389397, CA-425534)

What's new in 2026.1.0

This update contains the following new features:

- XenCenter introduces support for Driver multi-versioning (DMV) on XenServer 9 hosts. You can use XenCenter to discover, select, install, and switch between approved driver versions and variants delivered through the streamed host updates. DMV removes the need for most third-party "driver disks", simplifies lifecycle operations when the kernel ABI (kABI) changes, and enforces signatures to block unapproved third-party binaries.
- XenCenter now shows NUMA optimization status for virtual machines (VMs) on XenServer 9 hosts. Use XenCenter to verify placement and to visualize NUMA-related metrics after you enable them.
- You can now use XenCenter to limit and manage VNC console sessions for virtual machines (VMs) and the control domain (Dom0) in XenServer.
- XenCenter now offers improved management of XenServer licenses.
- When installing updates on your servers, XenCenter now includes new pre-checks that issue a warning if the post-update tasks include VM reboots.
- If High Availability has been configured for a pool and then disabled, it can now be re-enabled, retaining the restart priorities previously specified for the VMs.

Fixed Issues

- If XenCenter manages many pools that use the same AD account, when the AD account password changes, XenCenter attempts to log in to all pools with the old password and can, as a result, lock out the AD account. (CP-54814)
- Changes to network settings using the **Properties** window are not persisted. (XSI-2089)
- When exporting a snapshot or a custom template as XVA file, XenCenter can crash if the name of the snapshot or template contains invalid Windows path characters. (XSI-2055)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **New Conversion** wizard blocks conversion of VMware ESXi/vCenter VMs when their total disk size is larger than 2TiB. (CA-424048)
- XenCenter cannot create a new bonded network on systems running XenServer 9 when one of the member NICs is a management interface. (CA-421968)
- When using the **Back** and **Forward** buttons on the toolbar to quickly move between resource views, some views are excluded. (CA-397590)
- Enhanced compatibility with the Conversion Manager virtual appliance.
- Improved GFS2 clustering management when removing thinly provisioned storage repositories. (CP-311077)
- Performance improvements by reducing unnecessary requests to the server. (CA-412104, CA-422495)
- Miscellaneous user experience issues (CA-421989, CP-311733, CA-423906, XSI-2113)

What's new in 2025.5.0

Released Dec 08, 2025

This update contains the following new features:

- XenCenter now displays the version of the XenServer VM Tools installed on a VM. This includes the version of the Management Agent and PV drivers for Windows guests and the agent version for Linux guests. Users can also search for and group VMs with specific versions of XenServer VM Tools.
- XenCenter now displays whether the server has booted in secure boot mode.
- XenCenter introduces support for new network operational metrics.

Fixed Issues

- Sometimes the server **Properties** window can crash when a user with insufficient RBAC permissions attempts to save changes. (CA-420006)
- Sometimes the server **Properties** window does not show all the drivers installed on the server. (CA-419461)
- When selecting bond members for a new bonded network, the list of NICs can contain duplicate entries. (CA-420665)
- XenCenter launches multiple instances of the **Repair Storage Repository** dialog box when the user attempts to repair additional storage repositories while the dialog box is open. (CA-415190)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When creating a new external network, XenCenter can erroneously show an informational message for VLAN 0 even if the selected VLAN number is not 0. (CA-389419)
- Incorrect help link on the **Corosync Upgrade** wizard. (CA-421480)
- Miscellaneous user experience issues (CA-410114, CA-419886, CP-310601, CP-310652, CA-417876, CP-309339).

What's new in 2025.4.0

Released Oct 23, 2025

What's New

This update contains the following new features:

- **Configure High Availability (HA) behavior on clean shutdown**

  You can now control how High Availability (HA) responds to internal VM shutdowns. Previously, HA treated all VM shutdowns including those initiated from within the VM as failures and automatically restarted the VM, which often caused confusion. With this update, you can specify whether HA should restart VMs after an internal shutdown.

  This setting was initially available via the API and CLI. It is now also exposed in the UI for easier access and configuration.

- **SSH Access Management**

  Administrators can now enable or disable SSH access to dom0 programmatically through the XenAPI and xe CLI.

  This enhancement allows centralized SSH control across multiple hosts and supports automation frameworks such as Ansible or Salt.

  It improves security compliance by reducing manual intervention and limiting SSH exposure when remote shell access is not required.

- **Corosync 3 Cluster Stack Upgrade**

  XenServer 8.4 introduces support for the Corosync 3 clustering stack, replacing Corosync 2.

  The new stack improves cluster stability, scalability, and communication reliability for GFS2-based storage pools.

  A dedicated upgrade process has been added to transition existing GFS2 clusters from Corosync 2 to Corosync 3.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This upgrade is a prerequisite for moving on from XenServer 8.4.

- New pre-checks have been added when performing a Rolling Pool Upgrade that leverage the updated upgrade plugin.
- The Citrix Integration feature is now GA and supported in production.

Fixed Issues

- When connecting to a pool and checking the license in use is not deprecated, XenCenter can crash. (CA-415868)
- When access to the pool has been granted to a user through group membership and not directly, the user is unable to connect to servers and VMs via the OpenSSH console (CA-414429).
- The link to the license server on the License Manager points to the wrong address. (CA-416292)
- Sometimes XenCenter can re-connect to a pool after the user has disconnected intentionally. (CA-399647)
- The **Start Upgrade** button on the Pre-checks panel of the **Rolling Pool UPgrade** wizard can become enabled while pre-checks are performed. (CA-417146)
- When renaming a folder through the Properties dialog of an object, the object is moved to a folder with the old name (CA-393524).
- Miscellaneous user experience issues and improvements to error handling. (CA-399641, CA-416280, CA-417646, CP-309841).

What's new in 2025.3.0

Released Aug 11, 2025

What's New

This update contains the following new features:

- **Easier pool join with update from a remote pool**: You can now configure your servers and pools to synchronize with and update from another pool. This feature enables you to more easily create a pool of servers that are all at the same update level. In addition to being able to manually configure a pool as an update channel, the **New Pool** and **Add to Pool** tasks perform this process automatically to make joining servers compatible with the pool.

  For more information, see Update your XenServer hosts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This update includes the following improvements:

- Improvements to the VM import mechanism. You are now prompted to select a template when importing VMs from OVA/OVF files, which provides greater consistency between imported VMs. The import mechanism also enables you to automatically install the Windows VM Tools on VMs in a pool that contains Conversion Manager 8.5.0 or later.
- Improvements to the **Import** wizard:
  - Disable the **Start the new VM(s) automatically as soon as the import is complete** option when the host has insufficient resources.
  - Remove duplicate information.
- Remove duplicated **Permissions Checks** tab in the **Server Status Report** wizard.
- If a host fails the certificate length pre-check when upgrading, progress is prevented until this failure is resolved. For more information, see Can I upgrade?.
- In Workload Balancing, increase the allowed maximum value for the critical threshold of Free Memory to 100 GB.
- In the **Add New Server** dialog box, improve the behavior when manipulating text with keyboard shortcuts.
- Improvements to behavior when using XenCenter to change the management network.

This update includes the following changes of behavior:

- XenCenter no longer provides the ability to automatically download and apply hotfixes to Citrix Hypervisor 8.2 Cumulative Update 1. This does not affect the ability to upgrade to XenServer 8.4.

Fixed issues

- When exporting one or more VMs as an OVF or OVA file from XenCenter and then importing them back, XenCenter raises an error after the import process ends. Attempting to start any of the imported VMs produces a second error. (CA-411119)
- Asynchronous host operations, such as creating a pool, can throw a NullPointerException if the connection to the XenServer host is lost. (CA-409158)
- The **Disaster Recovery - Failback** wizard prevents progress when a pre-check shows a warning. (CA-411227)
- XenCenter can crash if you try to update it when the update or install process is already running. (CA-407747)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sometimes XenCenter incorrectly shows that a storage repair operation has failed. (CA-403820)
- An error during VM import can cause XenCenter to become unresponsive. (CA-413300)
- When changing the network management after removing an IP address, the management network configuration does not persist. (CA-415174)

2025.2.1

Released Jun 18, 2025

Fixed issues

- When taking a host out of maintenance mode, if you select **Restore VMs**, only the first of the evacuated VMs is migrated back onto the host. The automatic migration of the subsequent VMs fails. You can manually migrate these VMs back to their original host. (XSI-1924)

2025.2.0

Released May 07, 2025

What's New

This update contains the following improvements:

- Improved live patching advice. XenCenter displays extra guidance when partial live patches are available for a set of updates. Use this information to avoid unnecessary host reboots.
- Improvements to the VM import mechanism. You are now prompted to select a template when importing VMs from disk images, which provides greater consistency between imported VMs.
- Ensure compatibility between XenCenter and the latest XenServer updates. If you attempt to apply a set of updates to your pool that are not compatible with your current version of XenCenter, XenCenter blocks the update and prompts you to update your XenCenter to the latest version. This check ensures that your XenCenter does not lose connection with your pool during the update process.
- Improvements to the root password change options. The option to change the pool root password is now shown only on the **Pool** menu. It was previously also shown on the **Server** menu.
- When you select multiple pools or standalone hosts to apply licenses to at the same time, XenCenter now handles these pools in parallel, rather than sequentially. This change speeds the licensing process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When a host exits maintenance mode, the previously evacuated VMs are now returned to it in parallel instead of one at a time. This speeds up the process of moving VMs back to their original host.

This update contains the following change in behavior:

- XenCenter no longer associates the following file types with itself: OVF, OVA, VHD, and VMDK.

Fixed issues

- For XenServer 8.4 pools, the performance graphs in XenCenter are blank. (XSI-1824)
- In **Networking > Properties**, changes to the **Automatically add network to new VMs** setting are not saved. (CA-407424)
- When XenCenter connects to a large pool with high availability enabled, if a host in that pool fences, XenCenter can crash and report an unexpected error. (CA-404129)
- The **Install Update** dialog can show an error when restarting the toolstack. (CA-399639)
- An uncaught exception when attempting to view the details of the update while installing the update. (CA-407544)
- In the host **Properties** dialog, on the **Log Destination** panel, XenCenter doesn't allow you to include a port in the field. (CA-404628)
- Incorrect help link on the **New Security Certificate** dialog. (CA-404836)
- Sometimes, when an import operation is interrupted, the partially imported VM cannot be deleted and the import cannot continue. (CA-380982)
- In the **Copy VM** dialog, if there is no storage network available to choose, the dialog allows you to proceed to the next step. This behavior causes an error. (CA-408106)
- After shutting down and reopening XenCenter, it sometimes fails to display saved hosts and pools. (CA-401317)
- The XenCenter logs can include an excessive amount of Citrix Virtual Apps and Desktops™ connection manager messages. (CA-408197)
- When using the **Install Update** wizard to update more than one standalone host, the wizard does not exit gracefully. (CA-407549)
- The data source 'runstate_blocked' is incorrectly shown as 'runstate_idle'. (CA-409548)
- When you open the **Conversion Manager** window, the **New Security Certificate** dialog repeatedly opens after it is canceled. It continues to open even if the **Conversion Manager** window is closed. (CA-409460)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When connecting to a pool that is part of an AD domain as a user within that domain that has not been explicitly added to the pool, the operation hangs. (CA-406952)
- An error can occur when a host exits maintenance mode during an emergency transition of the pool coordinator. (CA-404662)

2025.1.0

Released Mar 03, 2025

What's New

This update contains the following new features:

- **Show GFS2 cluster health information and alerts in XenCenter.** If GFS2 clustering is enabled in the pool, XenCenter shows a **GFS2 Cluster** section in the **General** tab for the pool and for the hosts in the pool. For more information, see View pool properties and View host properties. When the number of live hosts in a GFS2 clustered pool changes or the pool is close to losing quorum, XenCenter displays an alert. For more information, see Alerts.
- (XenServer 8.4 and Workload Balancing 8.4.0) **Automatic import of the Workload Balancing certificate**. When connecting XenServer to the Workload Balancing virtual appliance, XenCenter automatically imports the Workload Balancing certificate into the XenServer pool. This feature simplifies management of the trust relationship between XenServer and the Workload Balancing virtual appliance. For more information, see Connecting to Workload Balancing.

This update includes the following improvements:

- Update the displayed product version to XenServer 8.4
- Advise users about Citrix Hypervisor 8.2 Cumulative Update 1 upcoming end of life.
- Improved colors in the performance graphs for better visibility.
- Improvements to icon display in partially updated pools.
- Improvements to hotkey behavior.
- Improvements to the wording in the **New VM > GPU** panel.
- Improvements to the wording around XenCenter proxy settings.
- Improvements to message display around Conversion Manager connections.
- Improvements to behavior when evacuating a host.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- If you are managing a large number of hosts and pools with XenCenter 2024.3.0 or later, you might see high CPU usage and experience lag in the XenCenter UI. (CA-391284)
- XenCenter incorrectly adds automatically all networks when creating a VM unless those networks are explicitly marked to not add automatically. The correct behavior is to automatically include only those networks that are explicitly marked to be added automatically. (CA-403749)
- If you migrate a VM while viewing the **Citrix®** tab > **Machines** section, the view does not refresh and the VM still shows in its source location. (CA-402543)
- XenCenter shows a maximum of four networks on the **Configure Networking** page of the **New VM** creation wizard when creating a VM from a default template. (CA-400335)
- When importing a VM, if you use the **Previous** button to navigate back to the **Location** tab, the selected host values might have changed. (CA-380739)
- PVS Accelerator can't be enabled for a VM if its VIF with the lowest device number is not at device 0. (CA-402911)
- If the server has only a local XFS SR, you cannot create a new VM on it through XenCenter.
- When attempting to apply a supplemental pack to a XenServer 8.4 server, XenCenter incorrectly treats the pack as an offline updates bundle. (CA-406387)

XenCenter 2024.4.0

Released Dec 05, 2024

What's New

This update contains the following new features:

- (Preview) Citrix Integration. Connect XenCenter to the Citrix Virtual Apps and Desktops environment to see information about Citrix Virtual Apps and Desktops machines and sessions hosted in your XenServer pool. For more information, see Citrix Integration.
- (XenServer 8.4) Offline Updates for XenServer. Use this feature to update air-gapped servers, join a host to an existing pool that's at a higher level of updates, or better manage your update testing before production rollout. For more information, see Manual updates.
- Improved VM conversion. Together, XenCenter 2024.4.0 and Conversion Manager virtual appliance 8.4.0 enable you to automatically uninstall VMware Tools and install the XenServer VM Tools in the converted VM. For XenServer 8.4 only, this release also adds support for Windows 11 VMs for conversion. For more information, see Conversion Manager - What's New.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This update contains the following improvements:

- Quick Create VMs from snapshots. The Quick Create option is now also available for snapshots.

Fixed issues

- When using XenCenter to change the DNS settings, the IP config on the pool can change without warning. (CA-389459)
- The Active Directory domain check when adding a host to a pool can incorrectly fail. This failure is caused by the check being case-sensitive. (CA-399256)
- When creating VMs or importing XVAs, XenCenter allows selection of host or pool with unavailable SRs. (CA-359985)
- The **Exit Maintenance Mode** dialog offers to restore VMs it did not shut down, suspend or evacuate. (CA-311142)
- After resizing the main panel in XenCenter, long pool or server names can obscure the licensing or log-in information. (CA-399240)
- While applying hotfixes to a Citrix Hypervisor 8.2 Cumulative Update 1 pool or server, if you select to shut down VMs from the pre-checks panel, the shutdown operation can report an error even though it succeeds. (CA-389409)
- Not all VMs are restored when XenCenter brings a host out of maintenance mode. (CA-400059, CA-400930)
- Miscellaneous user experience issues. (CA-400057, CA-401369, CA-375830, CA-393494)

XenCenter 2024.3.1

Released Oct 10, 2024

What's new

This update contains the following new feature:

- For Windows VMs, custom templates, or snapshots, you can now manage I/O driver updates for XenServer VM Tools through Windows Update in the **New VM** wizard in XenCenter. For details on enabling I/O driver updates through Windows Update, see Overview of VM creation steps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- If a VM's `has-vendor-device` field is set to true and you then convert the VM into a template or a snapshot, XenCenter fails to retain this value, causing new VMs created from the template or snapshot to have an incorrect `has-vendor-device` value. (CA-391310)
- During a silent installation of XenCenter, the installer fails to remove the previous version because the sequence that detects existing installations only runs during standard UI installations. (CA-399231)
- When managing large numbers of Citrix Hypervisor 8.2 CU1 hosts in XenCenter, you might encounter GUI performance issues, including high CPU usage and occasional UI freezes. (CA-397980)
- Using XenCenter 2024.1.0 or later to set or edit a custom field with a value for an object causes any values in the object's `other_config` to be deleted. This issue can cause unexpected behavior depending on the object and your environment. We strongly recommend that you do not add or edit custom field values. (CA-397587)
- For XenServer 8.4 pools, when the VM Groups feature is disabled or unlicensed, some elements and menu options are incorrectly shown in XenCenter. (CA-396046)
- In the **Pre-checks** panel of the **Install Update** wizard, an info pop-up states that there are pending tasks to complete for snapshots, although this guidance is only ever applicable to VMs. (CA-395739)
- When performing a Rolling Pool Upgrade in XenCenter, the **Rolling Pool Upgrade** wizard's final page incorrectly displays 24-hour log timestamps as 12-hour time. (CA-393819)
- When viewing your pool or host, the licensing information does not display correctly if your license has expired. (CA-392951)
- In XenCenter 2024.1.0, the **Properties** pane of your pool or VM occasionally stops rendering correctly. (CA-389831)
- When a host is offline, the shared storage is reported as broken even though all the active hosts are correctly connected to the shared storage. (CA-353531)

XenCenter 2024.3.0

Released Aug 22, 2024

What's new

This update contains the following new feature:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- (XenServer 8.4) You can now assign your VMs to anti-affinity placement groups that are started on hosts in your pool according to the following anti-affinity placement rules:

  a. No single host is the only place all VMs in a particular group are running.

  b. The count of VMs within the group for each host is as even as possible.

  When a VM in one of these groups is started or evacuated from a host, XenServer chooses to place the VM on a host that enables the VM group to follow these rules as closely as possible.

  For more information, see Manage VM groups.

This update contains the following improvements:

- (XenServer 8.4) XenCenter now supports using IPMI for host power-on. For more information, see Configuring Host Power On.
- XenCenter shows a warning if you attempt to create a GFS2 SR on a thin-provisioned LUN. This configuration is not recommended and can cause you to run out of space. For more information, see Thin-provisioned shared GFS2 block storage.

Fixed issues

- If you connect to the same XenServer pool with multiple instances of XenCenter, neither XenCenter shows available updates. To attempt to work around this issue, you can disconnect and reconnect XenCenter from the pool. (CA-389319)
- If you select multiple VMs in the **Resources** pane, the actions available from the **VM** menu and the actions available on the context menu are inconsistent. (CA-61207)
- Some shortcut keys in the context menu are not unique. (CA-395822)
- Inaccurate information can sometimes be displayed in the **Boot Options** panel for a VM. (CA-396230)
- When you select multiple items in the **Organization** or **Infrastructure** views and then switch between these views, your selections are lost. (CA-391372)
- After Aug 17, 2024, automated updates to XenCenter 2024.2.1 stopped working. This failure is caused by an expired certificate. Automated updates have now resumed with the XenCenter 2024.3.0 release.

XenCenter 2024.2.1

Released Jul 09, 2024

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

This update includes the following improvements:

- Added information to the XenCenter installation wizard stating that the current installation removes all previous versions of the XenCenter application from your device.
- Improved the **Conversion Manager** window to display a warning before starting the conversion process if your VMware ESXi/vCenter VMs are running guest operating systems that are not supported for conversion.
- Removed the VM Recovery Mode feature.

Fixed issues

- On Citrix Hypervisor 8.2 Cumulative Update 1 hosts, when attempting to apply a hotfix through automated updates, XenCenter incorrectly shows the warning "The license is deprecated and may revert to Trial Edition if updates are applied". (XSI-1676)
- When performing actions related to Workload Balancing (such as connecting, pausing, or resuming), XenCenter might fail to show the correct state of the Workload Balancing appliance. (XSI-1674)
- You are unable to migrate a VM to another host using XenCenter 2024.2.0 if the Workload Balancing virtual appliance is offline.

XenCenter 2024.2.0

Released Jun 06, 2024

What's new

NOTE:

- XenCenter 2024.2.0 is required to receive production support with Citrix Hypervisor 8.2 Cumulative Update 1 and XenServer 8.4.

Upgrade notes:

- XenCenter 2024.2.0 supersedes earlier versions of XenCenter, including XenCenter 8.2.x. When you install XenCenter 2024.2.0, it removes other versions of XenCenter on your system.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If XenCenter 2024.2.0 is the first version of XenCenter with a version format YYYY.x.x that you have installed on your system, it imports your server list from any instance of XenCenter 8.2.x on the system. Passwords are not imported.
- If you already have a version of XenCenter YYYY.x.x installed in parallel with XenCenter 8.2.x, this version does not import your server list from XenCenter 8.2.x. To migrate your server list from XenCenter 8.2.x, complete the following steps in order:

  a. Export your data from XenCenter 8.2.x. Go to **File > Export Server List**.

  b. Install XenCenter 2024.2.0.

  c. Import your data into XenCenter 2024.2.0. Go to **File > Import Server List**.

  For more information, see Exporting and Importing a List of Managed Servers.

This update contains the following new features:

- (XenServer 8.4) **Import a VHDX or AVHDX disk image as a VM:** You can now import a VHDX/AVHDX file into a pool or specific host as a VM. VHDX is an improved version of the VHD format that provides better performance, fault tolerance, and data protection features in addition to a larger capacity. For information on how to use the XenCenter **Import** wizard to import a VHDX/AVHDX file, see Import Disk Images.

  If you are a Citrix customer, you can also use this feature to migrate your VMs from VMware to XenServer. As part of its software streaming technology, Citrix Provisioning stores a shared disk image (vDisk) as a VHDX/AVHDX file. By using the XenCenter **Import** wizard to import a VHDX/AVHDX file, you can easily migrate your vDisk from VMware to XenServer. For more information, see Migrating from VMware.
- Close TCP port 80 for a pool's management interface by using XenCenter. For more information, see Change Pool Properties.

  You can also view the status of port 80 for a pool or server in its **General** tab in the **Management Interface** section.

This update includes the following improvements:

- XenCenter lists the make and model of the host hardware on the host's **General** tab.
- Improvements to the display of licensing information.
- Improvements to branding information in the **New Conversion** wizard.
- Improvements to NIC labeling. The "FCoE Capable" column is renamed to "Software FCoE Capable".

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Improvements to error handling and threading in the **Conversion Manager** window.
- Improvements to error handling in the **Copy VM** wizard.
- Improvements to error handling in the **New VM** wizard.
- XFS file system type now listed in XenCenter.

Fixed issues

- Some updates that do not include guidance about update tasks are not displayed in the **By update** view. To see these updates, you can look in the **By server** view.
- Customers with a Standard Edition license are not able to do GPU Pass-through to a Windows VM through XenCenter.
- In XenCenter 2024.1.0, when you create a new folder it does not appear until you disconnect and reconnect to the modified pool. Also, when a folder is deleted it remains visible until you reconnect.
- Importing dynamic VHDs results in an error.
- Sometimes, the License Manager can assign a non-selected license and refuse to release the license.

XenCenter 2024.1.0

Released Mar 06, 2024

What's new

NOTE:

You must be using this version XenCenter or later before applying updates released after Mar 06, 2024 to your XenServer pool. Always install the latest version of XenCenter.

This update contains the following new features:

- (XenServer 8.4) **Improved update guidance:** We've added more nuanced guidance for the tasks that are performed as part of updates. These changes are designed to minimize the disruption to your VMs that these update tasks might cause. Tasks are categorized into **Mandatory**, **Recommended**, **Full-effectiveness**, and **Live patch**. These categorizations enable you to judge whether an update task that might cause downtime or minor disruption for your hosts or VMs is necessary for your environment and risk profile. For more information, see Updating your XenServer hosts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- (XenServer 8.4) **SNMP:** You can now use SNMP and any NMS of your choosing to remotely monitor resources consumed by XenServer. With this feature, you can also configure traps to monitor your XenServer hosts, which are agent-initiated messages that alert the NMS that a specific event has occurred in XenServer. For more information, see Monitoring host and dom0 resources with SNMP.
- **Changes to licensing:** If you used XenServer 8.4 during its public preview phase with a Citrix Virtual Apps and Desktops license, this license is now deprecated and will not be supported with XenServer 8.4 in future. XenCenter now alerts you that this license is deprecated and prevents you from upgrading from Citrix Hypervisor 8.2 CU1 to XenServer 8.4 until you apply a XenServer Premium Edition license to your hosts.

  To run Citrix Virtual Apps and Desktops workloads on your XenServer pool, you require a XenServer Premium Edition license. For information about getting a license, see the XenServer website.

  XenServer is now an entitlement of the Citrix for Private Cloud, Citrix Universal Hybrid Multi-Cloud, Citrix Universal MSP, and Citrix Platform License subscriptions for running your Citrix workloads. Read more.

This update includes the following improvements:

- The **Advanced Options** panel has been removed from **VM Properties**. This panel contained obsolete options that are no longer required.
- In the **Virtual Interface Properties** pane, XenCenter now shows the QoS limit in MBit/s.
- The units shown in XenCenter have been corrected to reflect accurately the base of the unit (1000 or 1024). Wherever the unit is calculated with multiples of 1024, XenCenter displays kiB, MiB, GiB, TiB, and so on. Wherever the unit is calculated with multiples of 1000, XenCenter displays kB, MB, GB, TB, and so on.
- Usability improvements to the VM Export wizard.
- XenCenter now shows the object's UUID on the **Properties Dialog > General** tab for all objects accessible through XenCenter.

Fixed issues

- Previously, XenCenter allowed you to rolling pool upgrade your hosts to the same version they are currently running, which left the pool in a broken state. XenCenter now prevents this behavior.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sometimes, in the VM Snapshot Schedule **Properties** dialog, the **Snapshot Schedule** panel doesn't load. (CA-387186)
- XenCenter can incorrectly allow an upgrade to proceed when there are failed pre-checks. (CA-386488)
- Sometimes, VMs are not restored to their original host after exiting maintenance mode. (CA-387197)
- Updates are not made available to users on Standard Edition. (CA-389235)
- XenCenter does not prompt you to save your connection state on first opening. (CA-380853)
- When pinned to the taskbar, the XenCenter taskbar icon disappears after a XenCenter update. (CA-379341)
- XenCenter does not preserve the power state when exporting a suspended VM as an XVA. (CA-368247)
- XenCenter incorrectly blocks pool operators from importing appliances and VM admins from exporting appliances. (CA-389487)

XenCenter 2023.4.0

Released Dec 04, 2023

What's new

This update contains the following improvements:

- (XenServer 8.4) **Monitor host and dom0 resources with NRPE** In XenServer 8.4, users with the Pool Admin role can use any third-party monitoring tool that supports Nagios Remote Plugin Executor (NRPE) to monitor host and dom0 resources. For more information on how to configure NRPE, see Monitoring host and dom0 resources with NRPE.
- (XenServer 8.4) **Support for 64 vCPUs** XenCenter can now support up to 64 virtual CPUs on a Linux or Windows VM.
- If you select the **Click here to create a DVD drive** option, you are now prompted to confirm whether you want to create a new DVD drive.

This update contains the following behavior changes:

- In XenCenter, the performance graph showing the average CPU for a VM has been removed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- When applying updates to hosts by using the **Install Updates** wizard, if you pause WLB by using the wizard, XenCenter fails to automatically resume the running of WLB.
- You cannot live migrate a VM to the local storage of another host in the same XenServer pool.
- On the **XenCenter Setup** wizard, the **Launch XenCenter on exiting the Setup wizard** checkbox disappeared.

XenCenter 2023.3.2

Released Oct 05, 2023

What's new

Fixed issues

- In pools with GFS2 SRs, using XenCenter to generate a server status report (SSR) can fail. (CA-375900)
- If you attempt to load a performance graph on a XenServer host after attempting to load a performance graph on a host with 100% CPU usage, the graph has trouble rendering. (CA-376887)
- XenCenter can fail to start due to a file naming issue in third-party software. (CA-382850)

XenCenter 2023.3.1

Released Aug 24, 2023

What's new

- (XenServer 8.4) A delivery of regular updates to XenServer 8.4 is made available through XenCenter, allowing you to benefit from a more efficient release process that delivers new features and bug fixes at a faster cadence than was previously possible. For more information, see Update your hosts.
- XenCenter updates can be downloaded and applied from within the UI. For more information, see Update XenCenter.
- You can use XenCenter to manage your XenServer 8.4 non-production environments.
- PuTTY is no longer bundled with XenCenter. To launch an SSH console to a XenServer host by using XenCenter, you must install an external SSH console tool and ensure that XenCenter is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configured to use it. For more information, see Configure XenCenter to use an external SSH console.

Fixed issues

This update includes fixes for the following issues:

- On Windows 10 (1903 and later) VMs, there can be a delay of a few minutes after installing the XenServer VM Tools before the **Switch to Remote Desktop** option is available in XenCenter. You can restart the toolstack to make this option appear immediately. (CA-322672)
- XenCenter gives an invalid error when you attempt to create multiple VM disks totaling > 2 TB. (XSI-1467)

XenCenter 8.2.7

For more information, see XenCenter 8.2.7.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Installing XenCenter®

XenCenter must be installed on a Windows machine that can connect to the XenServer® host through your network.

System requirements

In addition, XenCenter has the following system requirements:

- **Operating System:**
  - Windows 10
  - Windows 11
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server 2022
  - Windows Server 2025
- **.NET Framework:** Version 4.8
- **CPU Speed:** 750 MHz minimum, 1 GHz or faster recommended
- **RAM:** 1 GB minimum, 2 GB or more recommended
- **Disk Space:** 100 MB minimum
- **Network:** 100 Mbit/s or faster NIC
- **Screen Resolution:** 1024x768 pixels, minimum

If you want XenCenter to be able to launch an external SSH console that connects to your XenServer host, install one of the following applications on the system:

- PuTTY
- OpenSSH (installed by default on some Windows operating systems)

Install XenCenter

1. Download the XenCenter installation file, `XenCenter.msi`, from the XenServer downloads page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Launch the installer `.msi` file.
3. Follow the **XenCenter Setup** wizard to install XenCenter.

    a. On the introduction panel, click **Next**.

    b. In **Custom Setup**, you can configure the following options:

    - Where to install XenCenter. The default location is `C:\Program Files (x86)\XenServer\XenCenter\`.
    - Whether to make XenCenter available for all users or just the current user. The default value is **Just Me**, which installs XenCenter only for the current user.

    On this panel, you can also click **Disk Usage** to check how much disk space is available on your computer and how much is required to install XenCenter.

    Click **Next** to confirm your choices.
4. Click **Install** to begin the installation. The installation process takes a short time.
5. After XenCenter installation is complete, select whether to **Launch XenCenter on exiting the Setup wizard**. Click **Finish**.

On first startup of XenCenter, you are asked whether you want to periodically check for updates to XenCenter. This capability is enabled by default. You can configure a proxy server that XenCenter goes through to check for and download updates.

For more information, see Update XenCenter.

Connect XenCenter to the XenServer host

If you have not yet installed any version of XenServer on your servers, first complete the steps in Install XenServer.

1. Launch XenCenter. The program opens to the **Home** tab.
2. Click the **Add New Server** icon.
3. Enter the host name or IP address of the XenServer host in the **Server** field. Type the root user name and password that you set during installation of the XenServer host. Click **Add**.

The first time you add a host, the **Save and Restore Connection State** dialog box appears. This dialog enables you to set your preferences for storing your host connection information and automatically restoring host connections.

If you later want to change your preferences, you can do so by using XenCenter:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. From the main menu, select **Tools > Options**. The **Options** dialog box opens.
2. Select the **Save and Restore** tab and set your preferences.
3. Click **OK** to save your changes.

Configure XenCenter to use an external SSH console

XenCenter can launch an external SSH console that connects to a XenServer host. The supported external SSH console tools are PuTTY and OpenSSH. To use an external SSH console, ensure you have one or both of these tools installed on the system that hosts XenCenter.

You can configure the paths to both PuTTY and OpenSSH in XenCenter. However, XenCenter only attempts to use the tool that is selected in the Options dialog. By default, XenCenter selects the installed tool. If both tools are installed, PuTTY is selected.

If you have not configured the path to your external SSH console tool, XenCenter attempts on start to locate your PuTTY or OpenSSH installation and uses the paths it discovers.

To configure your external SSH console tool, complete the following steps:

1. In the XenCenter main menu, go to **Tools > Options**.
2. In the **Options** dialog, go to the **External Tools** tab.
3. In the section **External SSH Client**, you can configure the following options:
   - Select the external tool that you want to use.
   - Browse to or enter the path to the executable for an external tool.
4. To save your changes, click **OK**.

Uninstall XenCenter

To uninstall XenCenter:

1. Open the **Windows Control Panel**.
2. On the **Control Panel**, under **Programs**, select **Uninstall a program**.
3. Select **XenCenter** from the list and then select **Uninstall**.

XenCenter user configuration data and log files are not removed when you uninstall the XenCenter application. The log files and user configuration data are stored in the folder:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
%appdata%\XenServer\XenCenter
```

Starting or Exiting XenCenter®

Starting XenCenter

To start your XenCenter session, do one of the following:

- On the **Start** menu, choose: **Start > All Programs > XenCenter**
- Double-click the **XenCenter** desktop shortcut.

If you previously configured XenCenter to restore your server connections on startup and set a main password, XenCenter prompts you to enter this password before continuing. See Store Your Server Connection State to find out more about how to set your server reconnection preferences.

It is possible to run only one XenCenter session per user.

Exiting XenCenter

To exit the current XenCenter session, on the **File** menu, select **Exit**.

Any servers and VMs that are running when you exit XenCenter continue to run after the XenCenter window closes.

If there are any XenCenter tasks in progress, XenCenter warns you when you try to exit. You can choose to exit anyway, in which case unfinished tasks might not complete successfully. Alternatively, you can wait until the unfinished tasks have completed.

Uninstalling XenCenter®

To uninstall XenCenter:

1. Open the **Windows Control Panel**.
2. On the **Control Panel**, under **Programs**, select **Uninstall a program**
3. Select **XenCenter <version>** from the list and then select **Uninstall**.

XenCenter user configuration data and log files are not removed when you uninstall the XenCenter application. The log files are stored in the folder:

```
%appdata%\XenServer\XenCenter
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The user configuration data are stored in the folder:

```
%appdata%\XenServer\XenCenter.exe_Url_<hash>\<version>\user.config
```

Uninstalling by using `msiexec`

If you installed XenCenter by using `msiexec`, it might not appear in the **Add or Remove Programs** list. In this case, you can instead use `msiexec` to uninstall the program.

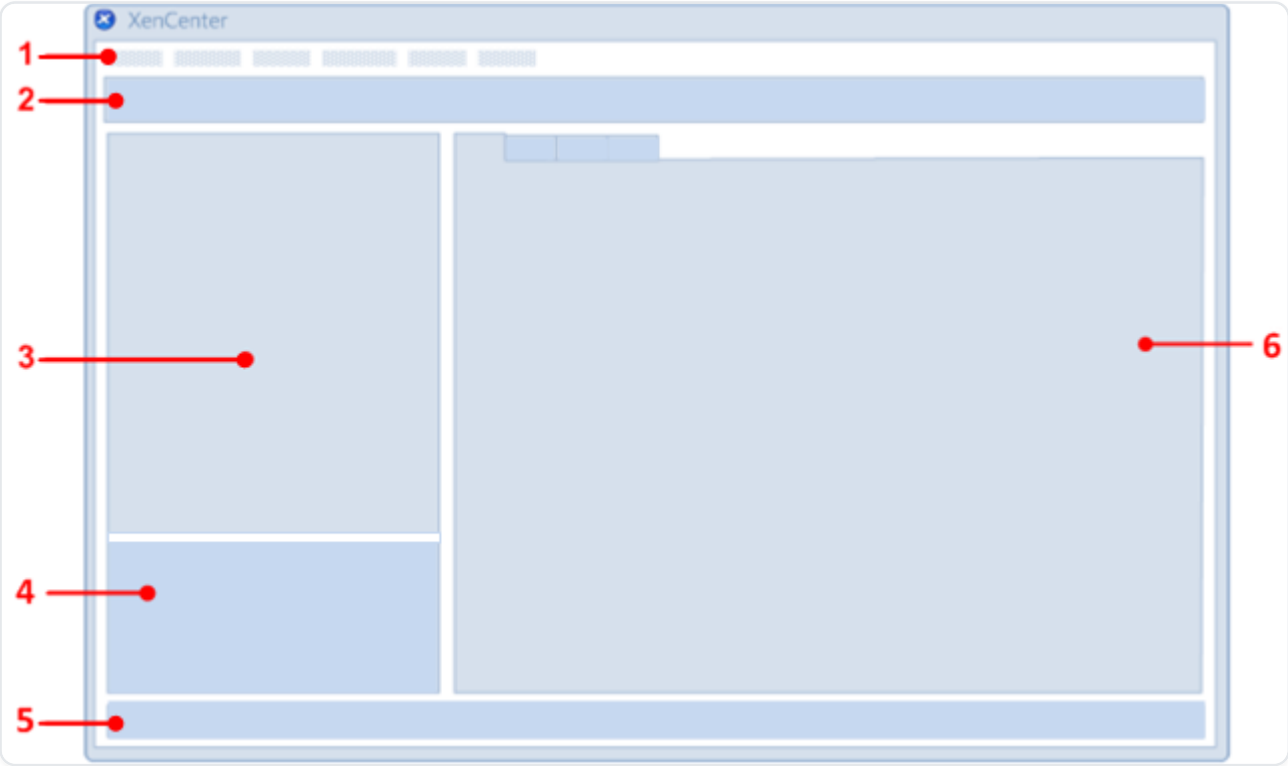
Open a command prompt and run the following command:

```
msiexec /x <xencenter-installation-msi-file-name>
```

Replace `<xencenter-installation-msi-file-name>` with the name of the XenCenter installer `.msi` file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exploring the XenCenter® workspace



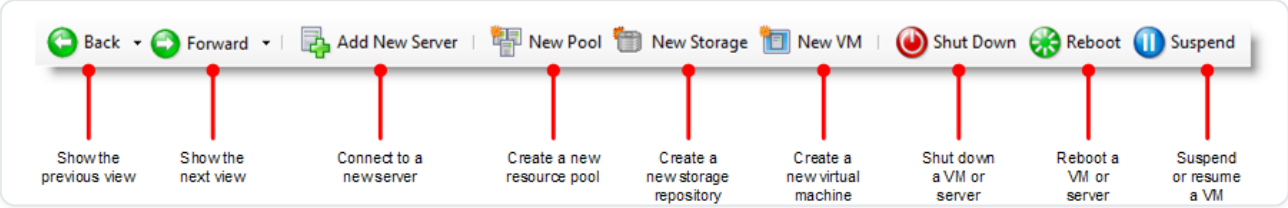
REF #	NAME	DESCRIPTION
1	Menu bar	Includes all the commands you need to manage servers, pools, SRs, VMs, and templates.
2	Toolbar	Provides quick access to a subset of the most frequently used menu commands. See The Toolbar.
3	Resources pane	Lists the servers, pools, VMs, templates, and SRs currently being managed from XenCenter. See The Resources Pane
4	Navigation pane	Lists the navigation buttons. Click a button to see a corresponding view of the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REF #	NAME	DESCRIPTION
		managed resources in the resources pane.
5	Status bar	Displays progress information about the current task.
6	Properties tabs	View and set properties for the selected resource. See The Tabs.

The Toolbar

The XenCenter® toolbar provides quick access to some of the most common XenCenter tasks, for example, to connect to new servers and create VMs.

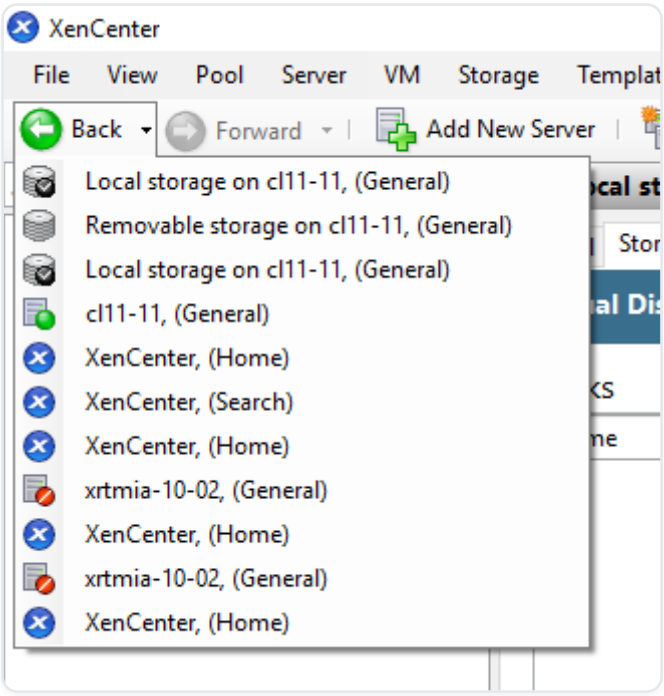


Using the Back and Forward buttons on the Toolbar

The **Back** and **Forward** buttons on the toolbar work like **Back** and **Forward** buttons on a browser and allow you to quickly move between views of your resources.

- To display your previous resource view, select **Back**.
- To display the next resource view (if you have used **Back**), select **Forward**.
- To display one of the resource views you used in this session, select the down arrow next to the **Back** or **Forward** buttons, and then select the view from the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Showing and hiding the Toolbar

The XenCenter window displays the toolbar by default. However, you can hide the toolbar, for example, if you need to make more space in the XenCenter window for the console display. To hide the toolbar, do one of the following:

- Right-click anywhere on the toolbar and, on the shortcut menu, select to remove the **Show Toolbar** check mark.
- On the **View** menu, select to remove the **Toolbar** check mark.

NOTE:

Any changes you make to your XenCenter toolbar visibility are persistent and are saved from session to session.

The Resources Pane

The **Resources pane** displays details about the managed resources - servers, pools, VMs, and storage. You can view your resources by their physical location or by properties such as folders, tags, or custom fields. The view in the **Resources** pane depends on the button you click in the **Navigation** pane. See the table in the following section for information about various buttons in the **Navigation** pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To do a simple text search on resource names, type a word or a phrase in the **Search** box, located above the **Resources** pane. Matching resources are displayed as you type. To remove the query and view all your resources again, click the **x** button at the right of the **Search** box.

You can also apply a previously saved search query to the **Resources** pane. XenCenter includes several useful saved searches. For more information, see Saved searches.

You can also create and add your own custom searches to this list at any time. For more information, see Create a Search Query.

To apply a saved search to the contents of the **Resources** pane, select **Saved Searches** in the **Navigation** pane and select a search query from the list.

The following table lists the various options available in the **Navigation** pane.

NAVIGATION BUTTON	DESCRIPTION
Infrastructure	Displays resources by their physical location, that is, by the host or pool to which they belong
Objects	Displays resources by categories such as pools, servers, VMs, templates.
Organization Views	Displays resources by folders, tags, custom fields, or by vApps
Saved Searches	Displays resources by the selected search criteria
Notifications	Displays the Notifications view which is a one-stop shop for alerts, updates, and events

For detailed information about the navigation buttons, see The Navigation Pane.

The Navigation Pane

The XenCenter® **Navigation** pane provides various options to view and access managed resources. The following navigation buttons provide a quick way to view and manage your resources:

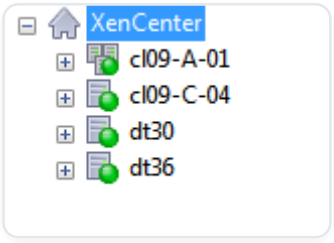
- **Infrastructure**
- **Objects**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Organizations Views**
- **Saved Searches**
- **Notifications**

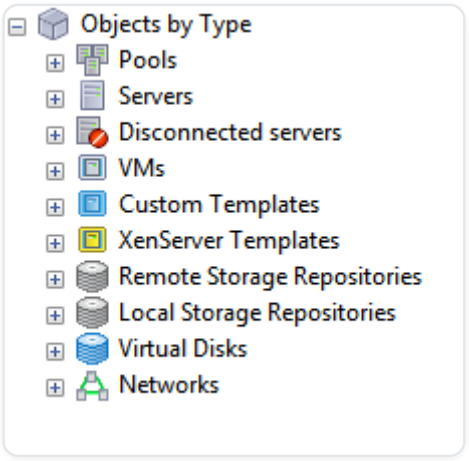
The following sections provide an overview of the buttons in the **Navigation** pane:

Infrastructure



This view is the default view. The **Infrastructure** view displays a tree view of the resources by their physical location. It provides a list of servers, VMs, templates, and storage resources by the pool or the server to which they belong.

Objects



Select **Objects** to see a list of the resources by categories such as pools, servers, VMs. Expand the nodes to view items in each category.

Organization views

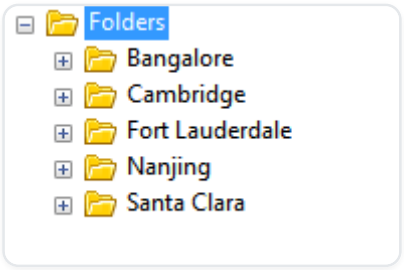
XenCenter allows you to group resources for ease of management. By default, XenCenter provides the following types of Organization Views:

- Objects by Folder
- Objects by Tag
- Objects by Custom Field
- vApps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VM groups

Objects by folder



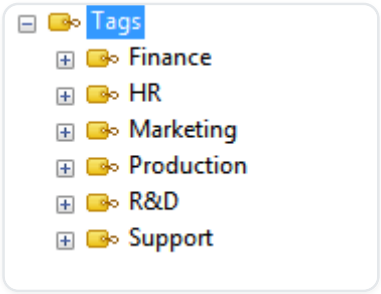
Select this option to view your resources by folders. You can create folders to group your resources by location, function, resource type, and so on

NOTE:

Organizing resources into a folder is conceptual, and not physical. The resources are note physically moved to a folder if you choose to group them by Folders.

For detailed information about creating and managing folders to organize your resources, see Using Folders.

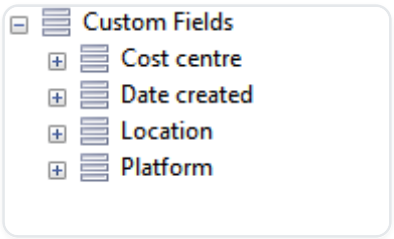
Objects by Tag



Select this option to view your resources by the tags that you have previously defined. Tags are labels that you specify to view resources based on the criteria that you define. A single resource can contain multiple tags. For example, a server with the tag 'Production' can also be tagged as ‘R&D’.

For detailed information about creating and managing tags in XenCenter, see Using Tags.

Objects by Custom Field



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Select this option to view your resources by the customized fields you have previously defined. XenCenter enables you to add custom fields to your resources and provide a value to effectively manage your resources. You simply add a custom field to a server, VM, or any other resource in the pool, then give it a value. You can then use custom field values when building search queries.

For information on creating and using custom fields, see Using Custom Fields.

vApps

Select this option to view your VMs by the vApps they belong to. A vApp is a group of one or more VMs which can be managed as a single entity. For detailed information about vApps, see Managing vApps.

VM groups

Select this option to view your VMs by the VM group they belong to. A VM group is a set of one or more VMs whose placement behavior is defined by the rules of the group. For more information, see Manage VM groups.

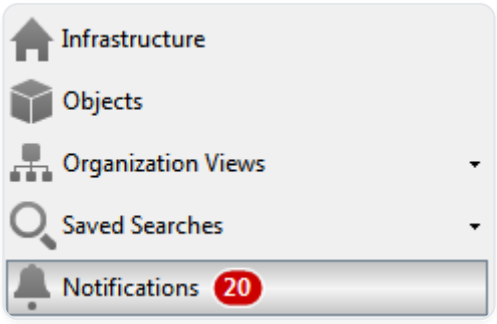
Saved searches



Click this button and select an option from the list to view resources that match the search criteria. By default, XenCenter includes a few saved searches that allow you to search your resources. You can create and add your own query to this list at any time.

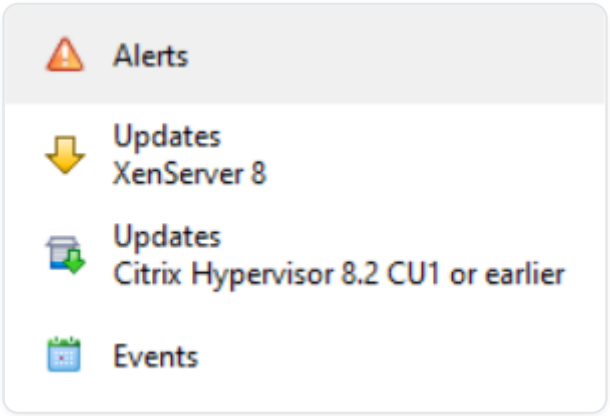
For detailed information about the Search functionality in XenCenter, see Searching Resources.

Notifications



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click this button for the **Notifications** view. The **Notifications** view enables users to see all notifications in a centralized location and perform specific actions to address them. It contains Alerts, Updates, and the Events view.



Alerts

The **Alerts** view displays a list of system alerts generated by XenCenter. You can filter the alerts by various options and take specific actions to address the alerts. For detailed information, see XenCenter Alerts.

Updates

XenCenter issues notifications about available updates for your hosts and pools under the **Updates** tabs. For more information, see Update your XenServer hosts.

Events

Select this option to see a summary of all events in your current XenCenter session. For detailed information, see XenCenter Event Log.

The Tabs

The tab-based navigation in XenCenter® provides quick access to your managed resources without needing to open and close dozens of windows at the same time. The tabs available at any time depend on what you have selected in the **Resources** pane. For example, most resources have a **General** tab. The **HA** and **WLB** tabs are available only when a pool is selected and the **Snapshots** tab is only available when a VM is selected.

Citrix®

When XenCenter has an active connection to a Citrix Virtual Apps and Desktops™ environment, XenCenter shows a **Citrix** tab for the following resources:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VM
- Host
- Pool

Console

On this tab, you can run a console session on a VM or a managed server.

See also Run a Remote Console Session to read about the different types of remote VM console supported in XenCenter.

Switch to Remote Desktop or Switch to Default Desktop

Switches between Windows remote console types

Switch to Graphical Console or Switch to Text Console

Switches between Linux remote console types. You might need to enter your VNC password first when switching to a graphic console.

Open SSH Console

Opens an external SSH console as a pop-up window. This option is available

- On the host's Console tab to access the Control Domain (Dom0) console
- On the Console tab of a Linux VM to access the VM's console.

> **NOTE:**
>
> Ensure that the Linux guest agent is installed on the VM to launch the SSH console.

Send Ctrl+Alt+Del

Sends the Ctrl+Alt+Del key sequence to the remote console.

Most keyboard shortcuts are transmitted to the server or VM when you use a remote console. However, your local system always intercepts the **Ctrl+Alt+Del** key sequence and prevents it from being sent if you type it in directly at the remote console.

Undock (Alt+Shift+U)

Undocks the **Console** tab into a floating window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To shut down or reboot a server, install XenServer® VM Tools, shut down, reboot or suspend a virtual machine from within the floating console window, select the lifecycle icon in the top-left corner of the window and then click a command.



To use a different keyboard shortcut for docking and undocking the console, go to the XenCenter **Options** dialog box: click **Tools > Options**.

Find Console

Opens the floating console window when it has been minimized or brings it to the front if it is hidden behind other windows.

Redock (Alt+Shift+U) or Reattach Console

Docks the floating console window back to the **Console** tab.

Scale

Scales the remote console screen to fit within the **Console** tab or window so that you can easily see everything on the remote console. Clear the check box to display the remote console screen at its normal size.

By default, the scale setting used in the **Console** tab is preserved when you undock the console or switch between console types, but this behavior is configurable. To change this setting, go to the **Console** tab of the **Options** dialog box.

Fullscreen (Ctrl+Enter)

Displays the console in full-screen mode. Press **Ctrl+Alt** to exit full-screen mode; to use a different key sequence, go to the XenCenter Changing XenCenter Options dialog box.).

When you point to the top center of the screen in full-screen mode, the **Connection bar** is displayed. The **Connection bar** shows the name of the VM or server you are working on and including two controls: a **Pin** button to allow you to turn the **Connection bar** on permanently, and a **Restore down** button that you can click to exit full-screen mode.

You can control various console settings in the **Options** dialog box. For example, the text clipboard on your local machine is shared with the remote console by default. Items you cut or copy are placed on the clipboard and made available for pasting on either your local computer or on the remote console. You can turn clipboard sharing off and change various other console settings from the XenCenter **Options** dialog box; see Changing XenCenter Options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

General

View general properties of the selected container, virtual machine, server, resource pool, template, or storage repository on the **General** tab; click **Properties** to set or change properties.

Copy any of the values shown on this pane to the Windows clipboard by right-clicking on the value and clicking **Copy** on the shortcut menu.

More information about the general properties of some types of resource is available in the following articles:

- View VM properties
- View server properties
- View pool properties

GPU

The **GPU** tab allows you to view or edit the GPU placement policy, view the available GPUs and virtual GPU types. The GPUs are grouped based on the supported virtual GPU types. You can modify the virtual GPU types allowed on a particular GPU using the **Edit Selected GPUs** option. The horizontal bar in each group represents a physical GPU and it displays information about VMs running on the GPU.

For more information, see the following articles:

- Configuring Virtual GPU
- Change Pool Properties.

NOTE:

- GPU Pass-through and Graphics Virtualization are available for XenServer Premium Edition customers. The GPU tab is displayed when the pool meets the license requirements and also has GPUs that support various virtual GPU types.
- There is no licensing restriction to use NVIDIA GPU pass-through for Linux VMs.

High availability

On the **HA** tab for a pool, you can:

- Enable high availability using the **Configure HA** button.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Change the pool's high availability configuration using the **Configure HA** button.
- Disable high availability.

When high availability has been enabled, you can see high availability status (failure capacity and server failure limit) and the status of the selected heartbeat storage repositories on the **HA** tab.

For more information, see the following articles:

- Configure high availability
- Disable high availability
- Change high availability Settings

Home

The **Home** tab allows you to add a server to the list of managed servers or open a browser window to find out more about XenServer.

Memory

You can enable Dynamic Memory Control (DMC) and configure dynamic memory limits on the **Memory** tab. VMs can have a static memory allocation or can use DMC. DMC allows the amount of memory allocated to a VM to be adjusted on-the-fly as memory requirements on the server change without having to restart the VM. The **Memory** tab also lets you update the Control Domain (dom0) memory.

For more information, see the following articles:

- Changing the Control Domain Memory
- About VM Memory Configuration

Networking

The **Networking** tab displays a list of networks configured on the pool, server, or the VM you have selected. It provides a centralized location to access or modify your network settings.

For more information, see the following articles:

- About XenServer Networks
- View and Change Network Properties.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NICs

View detailed information about the physical NICs on the selected server and configure NIC bonds on the **NICs** tab.

NIC bonding (or "NIC teaming") can improve server resiliency by using two or more physical NICs as if they were one: if one NIC within the bond fails, the server's network traffic is automatically routed over the second NIC, ensuring server management connectivity. See Configuring NICs.

> **NOTE:**
>
> Use vSwitch as your network stack to bond four NICs. You can only bond two NICs when using Linux bridge (deprecated).

Performance

View performance data for your VMs and managed servers on the **Performance** tab. Full performance data is only available for VMs with XenServer VM Tools installed.

The tab provides real-time monitoring of performance statistics across resource pools and graphical trending of virtual and physical machine performance. By default, graphs showing CPU, memory, network I/O, and disk I/O are displayed on the tab. Click **Actions** to add more performance data and change the appearance of the graphs. For more information, see Configuring Performance Graphs.

Performance alerts can be generated when CPU, memory usage, network, storage throughput, or VM disk activity go over a specified threshold on a managed server, VM, or SR. For more information, see Configuring Performance Alerts.

Search

Select the top-level XenCenter item, pool, or server in the **Resources** pane and then click the **Search** tab to perform complex searches of your managed resources. You can construct queries based on object types, folders, and attributes such as name, description, tags, high availability status or restart priority, and power state.

For more information, see the following articles:

- Create a Search Query
- Filter and Group Search Results
- Saved Searches

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Export and Import Searches

Snapshots

Create, delete and export VM snapshots, revert a VM to a selected snapshot, and use existing snapshots to create VMs and templates on the **Snapshots** tab.

See VM Snapshots.

Storage

View the storage configuration of the selected virtual machine, server, resource pool, or storage repository on the **Storage** tab. The settings shown on this tab depend on the type of resource currently selected in the **Resources** pane.

SELECTED RESOURCE	WHAT'S SHOWN ON THE STORAGE TAB	LEARN MORE
VMs and templates	Information about each virtual disk on the VM is shown. This information includes its size and location (the SR where the virtual disk is located), its data access status, and disk access priority. To edit a virtual disk's settings, select it in the list and click **Properties**. Click **Add** to add a disk or **Attach** to attach an existing disk.	Configuring Virtual Storage
Servers and pools	A list of the available storage repositories (SRs) is shown, with summary information about their type, size, free space, and share status. To edit the name or description of an SR, select it in the list and click **Properties**. Click **Add** to add an SR or **Detach** to detach the selected SR.	Managing Storage Repositories (SRs)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SELECTED RESOURCE	WHAT'S SHOWN ON THE STORAGE TAB	LEARN MORE
Storage repositories	A list of the virtual disks or ISOs on the selected SR is shown. Click **Add** to add a new virtual disk.	Add Virtual Disks

USB

The **USB** tab allows you to pass through individual physical USB devices to a VM so the VM's OS can use it as a local USB device. You can enable or disable pass-through by clicking the **Enable Pass-through** or **Disable Pass-through** button on the **USB** tab. To attach a USB, perform the following steps:

1. Shut down the VM.
2. Right-click the VM and select **Properties**.
3. On the left pane, click **USB**.
4. Click **Attach**.
5. In the Attach USB dialog box, click **Attach**.
6. Start the VM. The USB is now attached to the VM.
7. In the same way, click **Detach** to detach the USB from the VM.

USB pass-through support has the following restrictions:

- USB pass-through is supported for the following USB versions: 1.1, 2.0, and 3.0.
- USB pass-through supports a maximum of 6 USBs to be passed through to a single VM.
- Snapshot/Suspend/ Pool Migrate/ Storage Migrate operations are not supported when USB is passed through to VM.
- USB pass-through feature is available for XenServer Premium Edition customers.
- Plugging in untrustworthy USB devices to your computer might put your computer at risk. Assign USB devices with modifiable behavior only to trustworthy guest VMs.
- Do not boot BIOS from USB devices.
- Ensure that the USB device to pass-through is trustworthy and can work stably in normal Linux environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- USB device pass-through is blocked in a VM if high availability is enabled on the pool and the VM has restart priority as **Restart**. The USB attach button is disabled and the following message is displayed: **The virtual USB cannot be attached because the VM is protected by HA**. When configuring high availability for a pool, if a VM is not agile, the **Restart** option is disabled with the following tooltip: **The VM has one or more virtual USBs. Restart cannot be guaranteed**.

Users

Configure role-based access to XenServer users and groups through AD user account provisioning and Role Based Access Control (RBAC) on the **Users** tab. In this tab you can do the following tasks:

- Join a pool or server to an Active Directory (AD) domain
- Add an AD user or group to a pool
- Assign roles to users and groups.

For more information, see Managing Users.

WLB

Access key Workload Balancing features, including configuration, optimization recommendations, and status on the **WLB** tab.

NOTE:

WLB is available for XenServer Premium Edition customers. For more information about licensing, see About XenServer Licensing.

Resource Status Icons

The status of managed resources - servers (hosts), virtual machines, storage, and templates - is represented using different icons in the **Resources** pane and elsewhere in XenCenter®:

Pools

ICON	DESCRIPTION
	A pool that is connected and is up and running normally.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ICON	DESCRIPTION
	A mixed-mode pool with hosts in different upgrade states. This icon appears if one or more of your hosts are in a less upgraded state than the pool coordinator. For example, if your host is running an older version of XenServer or Citrix Hypervisor than your pool coordinator.
	A mixed-mode pool with hosts in different update states. This icon appears if one or more of your hosts are in a less updated state than the pool coordinator. For example, if you haven't applied the latest updates to all hosts in the pool.
	A pool that is unlicensed.

Servers

ICON	DESCRIPTION
	A host that is connected and is up and running normally.
	A host that is temporarily not connected to XenCenter, for example because it is being rebooted or is in the process of connecting.
	A host that is disconnected, for example because it has been shut down.
	A host that is currently in maintenance mode. See Run in maintenance mode.
	A host on which a crash dump file has been created as a result of a system failure. Crash dump files are located in a folder named crash under the `/var` directory on the host. Crash dump files can provide invaluable information to your support engineer to aid in diagnosing XenServer-related problems. This file can be included in host status reports generated in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ICON	DESCRIPTION
	XenCenter using the **Get Server Status Report** utility. See Creating a Server Status Report for more information on using this feature. When you remove the crash dump file from the `/var` directory on the host, the host status icon shown in XenCenter is restored to normal.
	A host that requires *updating* because it is less updated than the pool coordinator. See Update your XenServer hosts.
	A host that requires *upgrading* because it is running an older version of XenServer than the pool coordinator. See Upgrade your hosts.
	A host that is unlicensed.

Virtual machines, VM templates, and vApps

ICON	DESCRIPTION
	A virtual machine that is up and running normally.
	A virtual machine that is currently suspended.
	A virtual machine that is currently unavailable, for example because it is being rebooted or suspended.
	A virtual machine that is not running, for example because it has been shut down.
	A virtual machine that is currently migrating. See Migrate Virtual Machines.
	XenServer VM template.
	A custom (user-defined) VM template.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ICON	DESCRIPTION
	XenServer vApps. See Managing vApps.

VM snapshots

ICON	DESCRIPTION
	A disk-only VM snapshot.
	A scheduled disk-only VM snapshot.
	A disk and memory VM snapshot.
	A scheduled disk and memory VM snapshot.

Storage

ICON	DESCRIPTION
	A storage repository.
	The default storage repository for a pool.
	A storage repository that is not currently connected.
	A storage repository that is currently unavailable. See Resolving SR Connectivity Problems.
	A virtual disk.
	A virtual disk snapshot. This object is a snapshot of a VM's disks, and is created when a snapshot is made of the VM. See VM Snapshots for information about taking VM snapshots, and see Snapshots to find out more about disk snapshots.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Keyboard Shortcuts

In addition to the mouse, you can use the keyboard to navigate and perform tasks in XenCenter. For example, you can use the arrow keys to navigate between the items in the **Resources** pane and around the menus.

Navigating XenCenter

XenCenter provides many of the standard Windows shortcuts to navigate through the user interface. For more information, see Keyboard shortcuts in Windows.

To toggle menu mode on and off, press **F10** or **Alt**. When menu mode is enabled, letters in the menus are underlined to indicate that they are Access Keys that you can use to select specific menus and menu commands.

In menu mode, you can use the keyboard to navigate menus. The following table lists some of the basic navigation commands:

KEY	ACTION
Tab	Navigate to the next UI item and give it focus.
Right Arrow, **Left Arrow**	Navigate across the menu bar, selecting each menu in turn.
Up Arrow, **Down Arrow**	Select each menu command in turn.
Enter	Activate the selected command.
Space	Select the UI item that has focus.
Esc	Cancel the selected command and close the menu.

Shortcut keys

Use shortcut key combinations to activate specific menu commands. For example, pressing **Ctrl+N** opens the **New VM** wizard, just like clicking **New VM** on the **VM** menu of the main toolbar.

For numeric keypad keys, ensure that **Num Lock** is off.

Some shortcut keys are shown on the menus and in toolbar tooltips. The following table lists shortcuts for common XenCenter tasks:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KEY	ACTION
F1	Display the online Help
Alt+F4	Exit XenCenter and close the XenCenter window
Ctrl+Enter	Toggle the console display between full screen mode and window mode
Ctrl+B	Start the selected VM
Ctrl+C	Copy the selected text to the Windows clipboard
Ctrl+E	Shut down the selected VM
Ctrl+N	Open the **New VM** wizard
Ctrl+R	Reboot the selected VM
Ctrl+V	Paste the selected text from the Windows clipboard
Ctrl+X	Cut the selected text to the Windows clipboard
Ctrl+Y	Suspend or resume the selected VM
Ctrl+Z	Undo the last text edit action

Keyboard shortcuts are also available for working with VM consoles. These shortcuts are configurable. For more information, see Console Settings.

Changing XenCenter® Options

You can change various settings that affect your XenCenter working environment. On the **Tools** menu, click **Options**, click a tab and change the setting, and then click **OK** to save your changes.

Save and restore settings

By default, XenCenter remembers the address of each of the managed servers you connect to. Use the settings on this tab to specify whether to store your login credentials for the servers. Stored login credentials can be used to reconnect to your servers on demand or automatically at

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the start of each XenCenter session. You can also set a main password here to protect your stored login credentials.

OPTION	DESCRIPTION	DEFAULT
Save server login credentials	Login credentials - your user name and password - for all your managed servers can be stored between XenCenter sessions. When this check box is selected, XenCenter remembers your login credentials at the start of each new session. You can then reconnect to your servers on demand without having to re-enter your login credentials.	Off
Automatically restore server connections on startup	Stored login credentials can be used to automatically reconnect to your managed servers at the start of each new XenCenter session. When this check box is selected, XenCenter remembers the connection state of all your managed servers at the end of each session. XenCenter attempts to restore the connection state of your servers at the start of your next session using your stored login credentials.	Off
Require a main password	When **Save and restore server connection state on startup** is enabled, you can protect your stored login credentials with a main password to ensure they remain secure. At the start of	Off

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPTION	DESCRIPTION	DEFAULT
	each session, you are prompted to enter this main password before connections to your managed servers are automatically restored.	
Change main password	Select to change the current main password. You are prompted to enter the current password then to enter and confirm the new main password.	

Security settings

OPTION	DESCRIPTION	DEFAULT
Warn me when a new certificate is found	Select this check box to have XenCenter display a warning whenever a new TLS security certificate is found on a managed server. Clear the check box if you do not want to see warnings about new certificates found on your managed servers when connecting to them.	Off
Warn me when a certificate changes	Clear this check box if you do not want to see warnings about modified certificates found on your managed servers when connecting to them. Select the check box to have XenCenter display a warning whenever a modified certificate is found on a managed server.	On

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPTION	DESCRIPTION	DEFAULT
Remind me to change the server root password when I rotate the pool secret	Clear this check box if you do not want to be prompted to change your root password after rotating the pool secret. Select the check box to be prompted to change your root password after the pool secret is rotated.	On

See also: Connecting and disconnecting servers.

XenCenter Updates settings

OPTION	DESCRIPTION	DEFAULT
Check for new versions of XenCenter	Select this check box to have XenCenter periodically check and notify you when new versions of XenCenter are available. Clear the check box to disable the periodic check.	On

See also:

- Update XenCenter

Confirmations settings

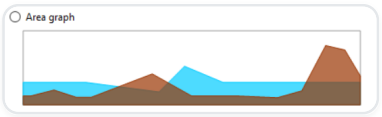
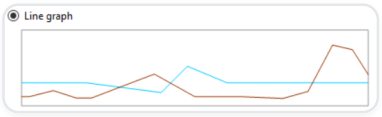
Use the settings on this tab to configure whether to display a confirmation dialog in the following cases:

- When you dismiss an alert
- When you dismiss an update
- When you dismiss an event
- When validating an OVF/OVA package

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Display settings

This tab enables you to configure how graphs are displayed in the **Performance** tab.

OPTION	DESCRIPTION	DEFAULT
Area graph	Choose this radio button if you want to view the performance data shown on the **Performance** tab as area charts. For example: 	No
Line graph	Choose this radio button if you want to view the performance data shown on the **Performance** tab as line charts. For example: 	Yes
Remember the last selected Tab for a resource	Select this option to display your last viewed tab for a resource when you next click on that resource.	On
Show timestamps in the update and upgrade log consoles	Select this option to include timestamp information in the update and upgrade logs.	On

See also: Monitoring system performance.

You can also use this tab to configure whether XenCenter remembers the last selected tab for a resource.

Console settings

OPTION	DESCRIPTION	DEFAULT
Share clipboard contents with remote console	Select this check box to share your local text	On

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPTION	DESCRIPTION	DEFAULT
	clipboard contents with the remote console. Items cut or copied are placed on the clipboard and made available for pasting on either your local computer or on the remote console.	
Full-screen mode	The keyboard shortcut to switch the console to and from full-screen mode.	Ctrl+Enter
Dock/Undock	The keyboard shortcut to undock the **Console** tab from the XenCenter window and to redock it.	Alt+Shift+U
Release keyboard and mouse	When the operating system on a VM captures your keyboard and mouse cursor for use within the guest OS. All the keystrokes, mouse moves, and button clicks that you make go to the VM. To return ownership of the keyboard and mouse to your host operating system, XenCenter reserves a special key on your keyboard: this key is the host key. By default, the host key is the right Ctrl key on your keyboard. You can change this default here.	Right Ctrl
Preserve current scale setting when console is undocked	Select this check box to use the same console scale setting when the console is docked and when it is undocked.	On

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPTION	DESCRIPTION	DEFAULT
Preserve current scale setting when switching back to the default console	Select this check box to keep the same console scale setting when switching between console types (for example, VNC/text console).	On
Send Windows Key combinations to the Remote Desktop console	Select this check box to have XenCenter send any Windows Key combinations entered on your keyboard to the Remote Desktop console.	On
Receive sound from the Remote Desktop console	Select this check box to have XenCenter play sounds from applications running on the Remote Desktop console on your local computer (the computer where you run XenCenter).	On
Automatically switch to the Remote Desktop console when it becomes available	Select this check box to have XenCenter automatically switch from using the standard graphical console to using the Remote Desktop console whenever it is available.	On
Connect directly to the server's console session	Select this check box to have XenCenter connect to the existing console session on the remote server. When opening a Remote Desktop console session, XenCenter uses this session instead of creating a new virtual console session.	On

Any changes you make to the Windows Remote Desktop console settings apply when you restart XenCenter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

See also: Run a remote console session.

Connection settings

Proxy server

XenCenter can be configured to connect directly to your managed servers or to use a proxy server. You can use your operating system's proxy server settings, or you can specify a proxy server.

- Select **Don't use a proxy server** to have XenCenter connect directly to managed servers without using a proxy server.
- Select **Use your operating system's proxy server settings** to use the same proxy settings that are set in your OS.
- Select **Use this proxy server** if you want XenCenter to connect to the specified proxy server. Use HTTP CONNECT to establish a secure TLS tunnel to your servers. Enter the address of the proxy server and the port number to use.

To have **XenServer®** connection requests made directly and not through the proxy server, select the **Bypass proxy server for XenServer connections** check box. To have all connection requests made through the proxy server, clear the check box.

XenServer connection is any connection which provides communication between XenCenter and the XenServer system, such as sending commands and using the console. A non-XenServer connection is something such as checking for updates.

Select the **Provide credentials** check box and enter the **Username** and **Password** that corresponds to a user account that is set up on the specified proxy server.

Select the desired authentication method: Basic or Digest (default).

Authentication method is used to authenticate to the proxy server. Select the same authentication method as the one the proxy server is set for.

For example, if the proxy server requests XenCenter to authenticate using Digest, then XenCenter fails to authenticate if the Basic authentication method is selected.

Default: Don't use a proxy server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connection timeout

You can specify how long to wait when establishing a connection with a managed server by adjusting the number of seconds to wait for a connection timeout. Do not set this value too low if you don't want to receive many false alerts due to network-related problems.

Default: 20 seconds

See also: Connecting and disconnecting servers.

Active Directory

When you initiate connections to multiple systems simultaneously, XenCenter also performs the logins simultaneously. This option can be disabled for logins that use the same Active Directory account if it leads to account lockouts.

Default: Allow simultaneous logins

External Tools settings

XenCenter can launch an external SSH console that connects to a XenServer host. The supported external SSH console tools are PuTTY and OpenSSH. To use an external SSH console, ensure you have one or both of these tools installed on the system that hosts XenCenter.

You can configure the paths to both PuTTY and OpenSSH in XenCenter. However, XenCenter only attempts to use the tool that is selected in this dialog. By default, XenCenter selects the installed tool. If both tools are installed, PuTTY is selected.

Hidden Objects

Hide networks, PIFs, and VMs from XenCenter by adding the key `HideFromXenCenter=true` to the `other_config` parameter for the object in the XenServer Management API. For example, certain VMs can be hidden to prevent them being used directly by general users in your environment. Objects flagged with this key are hidden objects, and by default they do not appear anywhere in XenCenter.

To make hidden objects visible in XenCenter®, on the **View** menu, click to select **Hidden Objects**. To hide them again, on the **View** menu, clear the **Hidden Objects** check mark.

See the developer documentation to find out more about flagging objects using the `HideFromXenCenter` key.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Organizing Resources

XenCenter® provides various different ways of organizing your physical and virtual resources, allowing you to use the method that works best for you.

- Using Folders
- Using Tags
- Using Custom Fields

Using Folders

A folder is a container that groups managed resources in whatever manner makes sense for your environment. For example, you might create a folder for each branch office in your organization. Folders can contain any type of resource from anywhere in your XenServer® environment. Resources can be accessed independently of the folder in which they are referenced.

The organization of folders in XenCenter® is conceptual, not physical. The resources are not physically located in the folder. Therefore, you can place resources into folders independently of their physical location. For example, placing a VM into a folder does not place its host server in the folder as well. Placing a server into a folder does not place all the VMs and storage resources on that server into the folder as well.

Folders can also be used in search queries. For example, you can search by folder with a "contained in" or "not contained in" relation and a list hierarchy of folders. For more information, see Create a Search Query.

The folder in which a resource is located is shown on the resource's **General** tab and in its **Properties** dialog box. You can always see folder information for a resource. You can also move a resource into a different folder or remove it from a folder from the **General** tab.

To create a folder

The simplest way to create a folder is through Resources pane. Click **Organization Views** in the **Navigation** pane, and then select **Objects by Folder**. In the **Resources** pane, click the **Folders** group, right-click, and select **New Folder** from the shortcut menu. Type a name for the new folder, select the server where your folder metadata is stored, and then click **Create**.

You can also create folders from the **General** tab for any resource:

1. In the **Resources** pane, select a pool, server, SR, virtual machine, or template, then click the **General** tab and click **Properties**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. On the **General** tab of the **Properties** dialog box, click **Change** in the **Folder** box.
3. In the **Change Folder** dialog box, click **In this folder** button and then click **New Folder**.
4. Type a name for the new folder and select the server where your folder metadata is stored, then click **Create**.
5. Click **Move** to apply the change and click **OK** on the **Properties** dialog box.

To move resources into and out of folders

Move a resource into a folder by dragging it from the **Resources** pane or **Search** tab and to the folder. Resources can only be in one folder. If the resource is already in another folder, it is moved when you drag in onto a different folder.

You can also move a resource into a different folder or remove it from a folder from the **General** tab:

1. In the **Resources** pane, select the pool, server, SR, virtual machine, or template you want to place in a folder.
2. Select the **General** tab and click **Properties**.
3. On the **General** tab of the **Properties** dialog box, click **Change** in the **Folder** box.
   - To remove the resource from its current folder, select **Not in any folder**.
   - To move the resource into a different folder, select **In this folder** and choose a folder or a subfolder from the list.
   - To place the resource in a new folder, click **New Folder**. Type a name for the new folder and select the server where your folder metadata is stored, and then click **Create**.
4. Click **Move** to apply the change and click **OK** on the **Properties** dialog box.

To rename a folder

1. In the **Resources** pane, select the folder then right-click and select **Rename Folder** on the shortcut menu.
2. Type the new name.

To delete a folder

You do not actually delete the resources in the folder when you delete the folder. The resources return to the general collection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In the **Resources** pane, select the folder, then right-click and select **Delete Folder** on the shortcut menu.
2. Click **Yes** to confirm.

All the contents are moved out of the folder and then the folder is deleted.

Using Tags

Tags enable you to identify your resources in new ways. Tags are like keywords or labels. They allow you to rearrange your view of resources within XenCenter® depending on criteria that are important to you. For example, you can use criteria such as application, location, cost center, owner, or lifecycle stage.

You make up tags when you need them and you can use as many as you like. You can also build searches based on your tags, for example, "all Windows 10 test machines located in Cambridge".

Select the **General** tab for a resource to see the tags currently assigned to that resource and to add and remove tags.

To create a tag

1. In the **Resources** pane, select a resource.
2. Select its **General** tab and then select **Properties**.
3. On the **General** tab of the **Properties** dialog box, select **Edit tags**.
4. Type a word or phrase in the **New Tag** box and then select **Create**.
5. The new tag is automatically assigned to the selected resource. To remove the tag, clear the check box.
6. Select **OK**.
7. On the **Properties** dialog box, select **OK** to apply your changes.

To delete a tag

1. In the **Navigation** pane, select **Organization Views** and then **Objects by Tag**. The **Tags** group is displayed on the **Resources** pane.
2. Select the tag you want to delete, right-click, and then select **Delete Tag**. The tag is removed from all resources that are currently tagged with it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To tag a resource

The simplest way to assign an existing tag to a resource is by dragging it onto the tag in the **Resources** pane. You can drag resources from within the **Resources** pane on the **Tags** group or from the search results list on the **Search** tab.

You can also assign an existing tag or a new tag to a resource using the **Edit tags** dialog box:

1. In the **Resources** pane, select the pool, server, SR, virtual machine, or template you want to tag.
2. Select the **General** tab and then select **Properties**.
3. On the **General** tab of the **Properties** dialog box, select **Edit tags**.
   - To create a tag and add it to the selected resource, type a word or phrase in the **Edit Tags** box. Click **Create**.
   - To add an existing tag, select to select the tag's check box in the **Tags** list. Click **OK**.
4. On the **Properties** dialog box, select **OK** to apply your changes.

To untag a resource

To untag (remove a tag from) a resource, in the **Navigation** pane, select **Organization Views** and then select **Objects by Tag**. Select the resource that you would like to untag, right-click, and then select **Untag object**.

You can also untag a resource using the **Edit Tags** dialog box:

1. In the **Resources** pane, select the pool, server, SR, virtual machine, or template you want to untag.
2. Select its **General** tab and then select **Properties**.
3. On the **General** tab of the **Properties** dialog box, select **Edit tags**.
4. Clear the check box for the tag in the **Tags** list and select **OK**.
5. On the **Properties** dialog box, select **OK** to apply your changes.

Using Custom Fields

Custom fields allow you to add structured information to your resources, which can help you find and manage them more effectively.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, you might identify all hosts with their physical location. Alternatively, you might label the cost center and applications running on all of your VMs. You simply add a custom field to a server, VM, or any other resource in the pool, then give it a value. You can then use custom field values when building search queries.

Custom fields are shared at the pool level. If you set a custom field on any resource in a pool, this field is available to all resources in the pool. You can access custom fields on the **General** tab and in the **Custom Fields** tab of the resource's **Properties** dialog box.

In the **Navigation** pane, click **Organization Views** and then select **Objects by Custom Field** to see your managed resources by the custom fields.

To create a custom field

1. In the **Resources** pane, select any resource.
2. Select the **General** tab and then click **Properties**.
3. On the **Custom Fields** tab, click **Edit Custom Fields**.
4. Click **Add**, type a name for the custom field and select the field type.
5. Click **OK** to apply your changes.

To assign a value to a custom field on a resource

1. In the **Resources** pane, select the resource.
2. Select the **General** tab and then click **Properties**.
3. On the **Custom Fields** tab in the **Properties** dialog box, enter a value for the custom fields.
4. Click **OK**.

The **General** tab for the resource displays all the Custom Fields set for that resource.

To delete a custom field

1. In the **Resources** pane, select the resource.
2. Select the **General** tab and then click **Properties**.
3. On the **Custom Fields** tab in the **Properties** dialog box, click **Edit Custom Fields**.
4. Select the custom field in the list and then click **Delete**.
5. Click **Yes** to confirm.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Searching Resources

XenCenter® enables you to perform complex searches of your managed resources. By default, XenCenter includes several searches. These searches allow you to search resources by tag. They also enable you to search VMs by network, operating system, power state, vApp, and XenServer VM Tools status.

You can also create and add your own custom searches to this list at any time. The view on the **Search** tab depends on the option you select in the **Navigation** pane. Select a view from the **Navigation** pane and then select the **Search** tab to start your search query. The **Search** tab also displays a title that highlights the selection of resources for your search query.

You can also do a simple text search on resource names by typing a word or a phrase in the **Search** box. The **Search** box is located above the **Resources** pane. Matching resources are displayed as you type. To remove the query and view all your resources again, select the **x** button at the right of the **Search** box. For more information, see the following topics:

- Create a Search Query
- Filter and Group Search Results
- Export and Import Searches
- Saved Searches

Create a Search Query

Using the **Search** tab, you can construct queries based on object types, folders, and attributes. Attributes can include name, description, tags, high availability status, restart priority, and power state.

To create a search query

1. On the **Search** tab, click **New Search**.
2. Under **Search for**, select the type of resource or combination of resources you want to search for. In addition to resource types such as servers, VMs, and SRs, this list also contains some common combinations of resource types. It also provides options to search all resources.

   To define your own search category, click **Custom** and select the resource types you want to search for.

   The search is applied when you select an option under **Search for**. The results are displayed immediately in the bottom half of the **Search** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click **Save** to save the search query.
4. Type a title for your search query in the **Name** box.
5. Click the **Location** list to choose the server where the search query metadata is saved.
6. Click **Save**.

Notes:

- Double-click a search result on the **Search** tab to display the **General** tab for that resource.
- To refine the search further, you can apply filters to the results. For more information, see Filter and Group Search Results. Filters are applied when you select a filter option, and the results are updated immediately.
- To quickly place search results into folders, select **Organization Views** and then **Objects by Folder**. Perform a search query, select the search results, and drag them onto folders in the **Resources** pane. Resources can only be in one folder, so if the resource is already in another folder it is moved. See Using folders to find out more.
- To quickly tag search results, select **Organization Views** and then **Objects by Tag**. Perform a search query, select the search results, and drag them onto tags in the **Resources** pane. For more information on using tags, see Using tags.

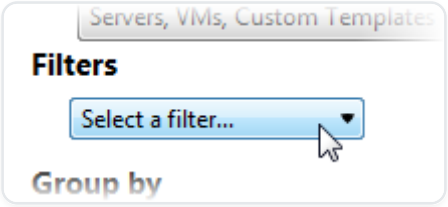
Filter and Group Search Results

You can apply filters to a selected search category to further refine the search. The filters that are available are appropriate to the type of resource you are searching for.

For example, when you search for servers, you can filter the results by server name, server IP address, its resource pool, and the VMs on it. When you search for virtual disks, you can filter the results using criteria such as whether they are shared or the storage repository they are on.

To filter your search results

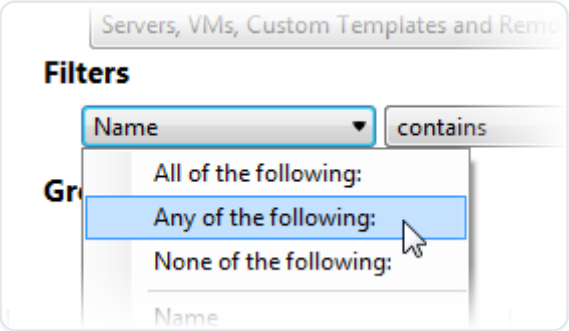
1. Click the filter button and choose a filter category from the list:



You can only select filters that are applicable to the resources you are searching for.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. If applicable, select an operator, such as **Is**, **Contains**, or **Start Time** and then enter a value. The filter applies to the search result when you select an option here. The results are updated immediately.
3. To add more filters, click the filter button and choose a multi-filter category from the list:



4. To remove a filter, click the **Remove** button on the right of the **Search** tab.

To group search results

1. Under **Group by**, select the grouping options you want to apply from the list. The grouping is applied when you select an option here. The results are updated immediately.
2. To add another grouping category to the search results, click **More** and then select a group category you want to add.
3. To remove a grouping, click the group button and select **Remove Grouping**.

Saved Searches

XenCenter® includes several useful saved searches. These searches allow you to search resources by tag. They also enable you to search VMs by network, operating system, power state, vApp, and XenServer VM Tools status. Modify these search queries by clicking the **Edit Search** button on the **Search** tab.

You can create and add your own custom searches to this list at any time. For more information, see Create a Search Query. Custom searches appear at the top of the **Saved Searches** list in the **Navigation** pane.

To apply a saved search

- To run a saved search in the **Resources** pane, select a search from the **Saved Searches** list in the **Navigation** pane. Search results are listed in the **Resources** pane.
- To run a saved search on the **Search** tab, click **Saved Searches** and then select a saved search query from the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To delete a saved search

On the **Search** tab, click **Saved Searches** and then **Delete** and select a saved search query from the list. Click **Yes** to confirm.

Export and Import Searches

XenCenter enables you to save search queries as `.xensearch` files. When you export and save a search query, only the search query is saved, and not the results.

To export the current search

1. On the **Search** tab, select **Export**.
2. Enter a file name and location.
3. Click **Save** to confirm.

To import a search

1. On the **Search** tab, select **Import**. Alternatively, on the XenCenter® **File** menu, select **Import Search**.
2. Browse to locate the exported search file (file name extension `.xensearch`) and then click **Open**. The imported search is performed immediately, displaying results on the **Search** tab.

To save the imported search as a new custom search

1. Click **Save**.
2. Specify a **Name** for the search query.
3. Choose the **Location** where to store the search query metadata.
4. Click **Save** to confirm.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

About XenServer® Licensing

XenServer requires a Citrix License Server to connect to the License Activation Service in Citrix Cloud and verify your XenServer entitlements. For information about how to install and run Citrix Licensing, see Citrix Product Documentation.

If you are using XenServer to run your Citrix Virtual Apps and Desktops or Citrix DaaS workloads, XenServer is now an entitlement of the Citrix for Private Cloud, Citrix Universal Hybrid Multi-Cloud, Citrix Universal MSP, and Citrix Platform License subscriptions for running your Citrix workloads. Read more.

To use XenServer Trial Edition, you do not require a license or a Citrix License Server. For more information, see XenServer Licensing.

For more information about licensing, see:

- Licensing Overview
- Managing XenServer Licenses

Related documentation

XenServer Current Release

- Licensing overview
- Licensing FAQ

Licensing Overview

XenServer is available in the following editions:

- Trial Edition
- Premium Edition

The **Premium Edition** is our premium offering, optimized for both server, desktop and cloud workloads. It offers the following features:

- Dynamic Workload Balancing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- GPU virtualization with NVIDIA vGPU
- Thin provisioning for shared block storage devices
- Support for SMB storage
- Direct Inspect APIs
- Export pool resource data
- In-memory read caching
- PVS-Accelerator
- Enablement for Citrix Virtual Desktops™ tablet mode
- Changed block tracking
- IGMP snooping
- USB pass-through
- SR-IOV network support
- Monitor host and dom0 resources with NRPE
- Monitor host and dom0 resources with SNMP

  If you use XenServer to run your Citrix Virtual Apps and Desktops or Citrix DaaS workloads, you must have a Premium Edition license. XenServer is now an entitlement of the Citrix for Private Cloud, Citrix Universal Hybrid Multi-Cloud, Citrix Universal MSP, and Citrix Platform License subscriptions for running your Citrix workloads. Read more.

The **Trial Edition** gives you access to all Premium Edition features in a restricted pool of 3 or fewer hosts. You can use Trial Edition for 90 days before it expires. After this 90-day period expires, you cannot start VMs on your Trial Edition host or pool.

Citrix® Licensing

XenServer uses the same licensing process as other Citrix products and as such requires a valid license or entitlement to be available in the License Activation Service. Use the Citrix License Server to connect to the License Activation Service and verify your entitlement. You can download the License Server from Citrix Licensing.

When you assign a license to your XenServer® host, XenServer contacts the specified Citrix License Server and requests a license for the specified servers. If successful, a license is checked out. The **License Manager** displays information about the license the hosts are licensed under.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you request or apply licenses, information about the XenServer version and license type might be transmitted to Citrix. No other information relating to users, VMs, or the XenServer environment is collected or transmitted to Citrix. The limited information transmitted to Citrix during the licensing process is handled in accordance with our privacy policy. For more information, see our privacy policy.

Licensing XenServer servers

XenServer does not support partial licensing, all servers in a pool must be licensed. If your XenServer pool contains servers that are licensed with different license types, the lowest license applies to the whole pool. Mixed pools of licensed and unlicensed hosts behave as if all hosts were unlicensed. For information on managing licenses in XenServer, see Managing XenServer Licenses.

License expiry

XenCenter® notifies you when your license is due to expire. Purchase a license before it expires. When your XenServer license expires:

- XenCenter License Manager displays the status as **Unlicensed**.
- You cannot access licensed features or receive Technical Support for any server within the pool until you purchase another license.
- You are running Trial Edition and can use the features provided by that edition for 90 days before your Trial Edition license expires.

License grace period

If your licensed XenServer host cannot contact the License Server, the server lapses into a 15-day licensing grace period. During the grace period, XenServer licenses itself through cached information. The servers are allowed to continue operations as if they are still in communication with the License Server. The grace period is 15 days and when the grace period runs out, XenServer reverts to an unlicensed state. After communication is re-established between XenServer and the License Server, the grace period is reset.

If your License Server cannot contact the License Activation Service, the server lapses into a 30-day licensing grace period. During the grace period, XenServer licenses itself through cached information. The servers are allowed to continue operations as if the License Server is still in communication with the License Activation Service. The grace period is 30 days and when the grace period runs out, XenServer reverts to an unlicensed state. After communication is re-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

established between the License Server and the License Activation Service, the grace period is reset.

Related documentation

XenServer Current Release

- Licensing overview
- Licensing FAQ

Managing XenServer® Licenses

This topic contains information about managing licenses in XenServer.

All hosts in a pool must be licensed. You can manage your XenServer license using the **License Manager** dialog box in XenCenter. The License Manager allows you to:

- **Assign** XenServer license to managed servers. When you assign a license, XenServer contacts the Citrix® License Server and requests the specified type of license. If a license is available, it is then checked out from the Citrix License Server.
- **Release** XenServer licenses. When you release a license, XenServer contacts the Citrix License Server and checks the license back in.

The **License Manager** dialog also provides information about the licenses that are applied to your hosts. It lists the following information:

- The license type.
- The number of sockets.
- The license expiry date.
- The license server host and port.
- The level of features that the license enables. For more information, see Licensing Overview.
- Whether the host is eligible for support. A host is eligible for support if the license has an active Customer Success Services subscription associated with it.
- Whether the license is deprecated. For information about getting a license, see the XenServer website.

Available licenses

XenCenter displays the XenServer Premium Per-Socket licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenServer is an entitlement of the Universal Hybrid Multi-Cloud, Citrix Platform, Citrix® Platform Flex and Citrix for Private Cloud offerrings. For information about getting a license, see the Citrix website.

To discover the license status of servers and pools

To see the license type of a server or pool, select that server or pool in the tree view. XenCenter displays the license status in the title bar for that server or pool, after the server or pool name.

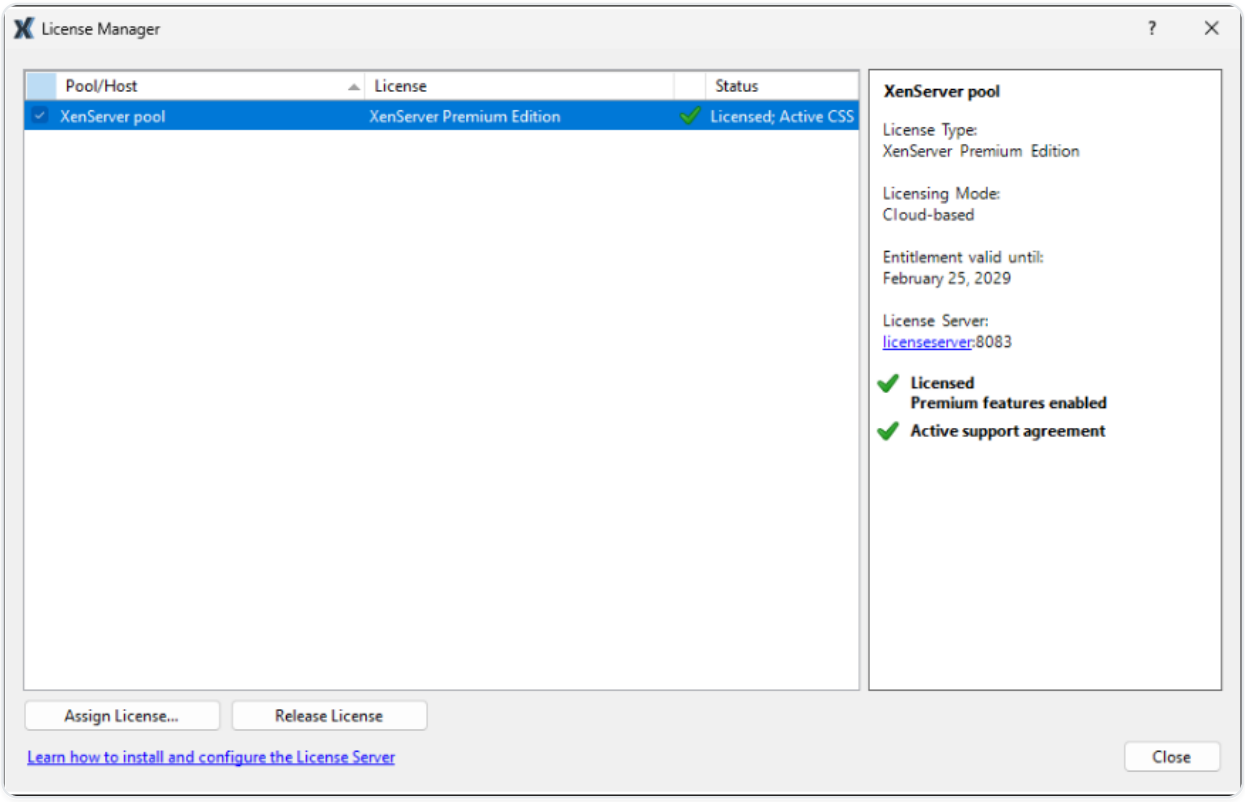
You can also go to the **General** tab of the server and find the license type in the **License Details** section.

Mixed pools of licensed and unlicensed hosts behave as if all hosts were unlicensed. In the tree view XenCenter displays unlicensed pools with a warning triangle icon.

Check licensing details

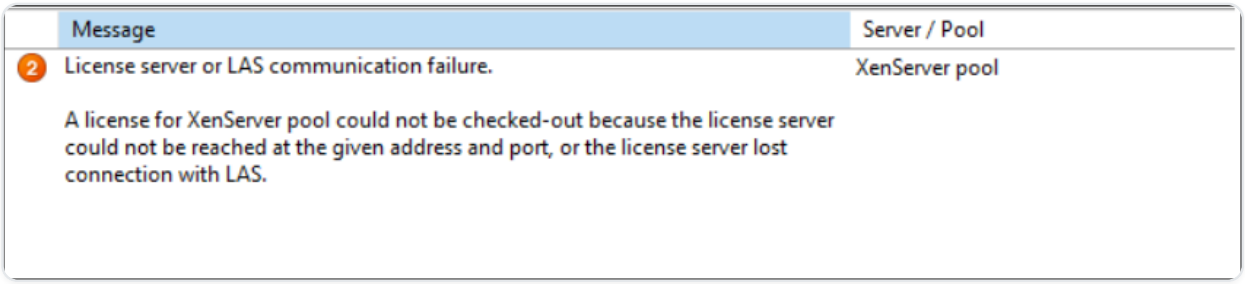
After you have configured the license, you can check the licensing details using XenCenter.

1. In XenCenter, on the Tools menu, select License Manager.
2. On the License Manager, click the pool or host in the list; if the XenServer has been activated using LAS, the entitlement validation status will be displayed in the right panel.

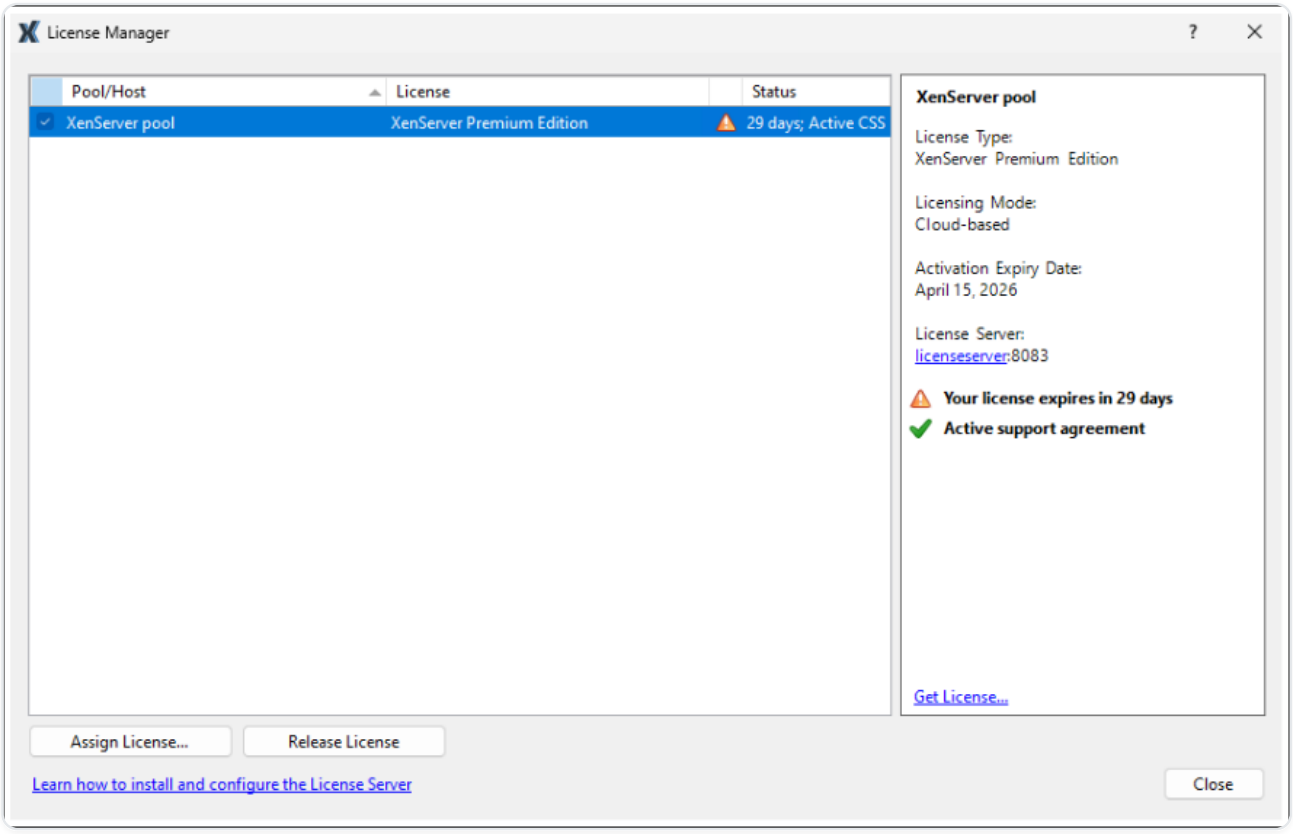


© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. If the License Server is unavailable or unable to communicate with LAS, you may see an alert in XenCenter stating “License server or LAS communication failure”. In this situation, XenServer will enter a grace period.



In the License Manager, this grace period is reflected as a license expiry date, and you will see a warning indicating that the license will expire in a specified number of days.



To assign a XenServer license

1. From the **Tools** menu, select **License Manager**.
2. Select one or more hosts or pools that you want to assign a license and then select **Assign License**.
3. In the **Apply License** dialog box, select the license you want to request from the License Server. For more information about various XenServer licenses, see Licensing Overview.
4. Enter the License Server details and then click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> By default, the License Server uses the port **8083** for communication with Citrix Cloud™ License Activation Service.

XenCenter contacts the specified Citrix License Server and requests a license for the specified servers.

- If successful, a license is checked out and the information displayed in the XenCenter License Manager is updated.
- If the connection fails, the **License Manager** shows a dialog that enables you to enter additional information about the License Server. For example, if you changed the default port on the License Server, enter the appropriate number in the port number box. For more information about changing port numbers due to conflicts, see the licensing topics in the Citrix Product Documentation website.

To release a XenServer license

1. On the **Tools** menu, select **License Manager**.
2. Select the servers or pools and then select **Release License**.

Related documentation

XenServer Current Release

- Licensing overview
- Licensing FAQ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix® integration

This feature bridges the gap between the different management models of XenServer and Citrix Virtual Apps and Desktops. It shows you the impact of changes to your XenServer pool on your Citrix Virtual Apps and Desktops sessions and enables you to manage your environment with confidence and efficiency.

We currently provide the following integrations with Citrix:

- View how VMs hosted on XenServer® map to your Citrix environment.
- Receive warnings when actions that you are taking in your XenServer pool might affect Citrix Virtual Apps and Desktops sessions.

<iframe src="https://www.youtube.com/embed/Vz_lHc0xdWM" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Feedback

Let us know what you think of this feature by emailing mailto:feedback@xenserver.com. Help us understand the full context of your situation by including as much information as possible about your XenServer and Citrix Virtual Apps and Desktops deployment.

Compatibility

This feature has been tested with Citrix Virtual Apps and Desktops 2407 and Citrix Virtual Apps and Desktops 2411.

Your Delivery Controller™ must be located on-premises and be accessible to XenCenter. XenCenter uses port 443 to request information from the HTTPS REST endpoint of the Delivery Controller.

For information about other connectivity requirements for your Citrix and XenServer environment, see Connectivity requirements and Communication Ports used by Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitations

- You can only connect one site per pool. If your XenServer pool hosts two Citrix Virtual Apps and Desktops installations, you can only integrate with one.
- You can only connect to one Delivery Controller per site. If you have multiple Delivery Controllers in your environment, choose just one of them to create a connection to.

Citrix Virtual Apps and Desktops permissions

To get the full benefit of this feature, ensure that the account you use to connect to your Citrix environment has the following permissions:

- **Read only admin** - A non-disabled, read-only Citrix Virtual Apps and Desktops admin is the minimum role that is supported with this integration.
- **VM scope** – Ensure that the account is scoped to view the VMs that you want to view and manage through the XenCenter® Citrix integration.

Connect to Citrix

To connect XenCenter to your Citrix Virtual Apps and Desktops environment:

1. Go to **Tools > Manage Citrix Connections...**. The **Configure Citrix Connections** dialog opens.
2. Click **Add Connection**.
3. Specify a display name for your connection in the **Name** field.
4. In **Connection Details** provide the connection information for your Citrix Virtual Apps and Desktops environment:
    - In **Controller Address**, enter the IP address or host name of your Delivery Controller.
    - (Optional) From the **Pre-fill with XenServer Credentials** list, choose a set of Active Directory credentials to use to connect to your Delivery Controller. This selection populates the following fields with your saved credential information.
    - In **Username** and **Password**, enter a set of valid credentials for your Citrix environment. The user account that you choose must have the required Citrix Virtual Apps and Desktops permissions.
5. Click **Test Connection** to verify that the values you entered are correct and that XenCenter can connect to your Citrix environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. If the connection succeeds, you can click **OK** to save the connection.

XenCenter shows the Citrix icon (

) in the status bar when it is connected to a Citrix environment.

When at least one connection has been saved, XenCenter shows a **Citrix** tab for the following resources:

- VM
- Host
- Pool

Remove a Citrix connection

To remove a Citrix connection from XenCenter:

1. Go to **Tools > Manage Citrix Connections...**. The **Configure Citrix Connections** dialog opens.
2. Find the connection in the left-hand panel.
3. Click the **Remove** icon (X) for the connection.
4. Click **OK** to exit the dialog.

Pools and Citrix®

Citrix tab

The **Citrix** tab for a pool in XenCenter shows information about the Citrix Virtual Apps and Desktops™ environment this pool is powering and the machines and sessions hosted in the pool. Information shown on this tab is updated every 10 seconds.

If the selected pool cannot be associated with a Citrix Virtual Apps and Desktops deployment, the tab shows a message. If the pool is part of your Citrix Virtual Apps and Desktops environment, this might be caused by incorrect permissions.

Overview

The **Overview** section of this tab shows high-level information about the sessions, machines, Machine Catalogs, and Delivery Groups in the connected Citrix Virtual Apps and Desktops environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

General

This section shows the following information:

- **Name:** The name of the Citrix Virtual Apps and Desktops site.
- **ID:** The ID of the Citrix Virtual Apps and Desktops site.
- **Sessions:** The total number of sessions in the pool and how many of them are disconnected.
- **Machines:** The total number of machines present in the site. This field also shows how many machines are marked as in maintenance mode in Citrix Virtual Apps and Desktops.
- **Delivery Groups:** The total number of Delivery Groups present in the site. This field also shows how many Delivery Groups are marked as in maintenance mode in Citrix Virtual Apps and Desktops.
- **Machine Catalogs:** The total number of Machine Catalogs present in the site. This field also shows how many Machine Catalogs exist in the site for each provisioning type: MCS, PVS, or manual.

Sessions

The **Sessions** section of this tab lists all Citrix Virtual Apps and Desktops sessions on all VMs in this pool. For each session, the following information is shown:

- **VM:** The VM this session is on.
- **User:** The full user name of the user of the session.
- **State:** Whether the session is active.
- **Type:** The type of session: Desktop or Application.
- **Session Started:** The start time of the session.
- **Session Established:** The last time the session was actively used by a user.

Machine Catalogs

The **Machine Catalogs** section of this tab lists all the Machine Catalogs in the connected Citrix Virtual Apps and Desktops environment. For each Machine Catalog, the following information is shown:

- **Name:** The name of the Machine Catalog.
- **Machine Type:** The type of the machine: virtual or physical.
- **Provisioning Type:** The provisioning type used by the Machine Catalog: MCS, PVS, or manual.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Allocation Type:** How machines are allocated by the Machine Catalog: random or static.
- **Total Machine Count:** The total number of machines in this Machine Catalog.
- **Machines Allocated to Server:** The total number of machines in this Machine Catalog that are allocated to this pool.

Delivery Groups

The **Delivery Groups** section of this tab lists all the Delivery Groups in the connected Citrix Virtual Apps and Desktops environment. For each Delivery Group, the following information is shown:

- **Name:** The name of the Delivery Group.
- **Machine Count:** The total number of machines in this Delivery Group in this pool.
- **Active Sessions:** The number of active sessions running under the Delivery Group in this pool.
- **Disconnected Sessions:** The number of disconnected sessions running under the Delivery Group in this pool.

Machines

The **Machines** section of this tab lists all the machines in the connected Citrix Virtual Apps and Desktops environment. For each machine, the following information is shown:

- **Name:** The name of the Citrix Virtual Apps and Desktops machine.
- **VM:** The VM that the machine is running on and the host where that VM is running.
- **User Changes Persistence:** Whether changes made by end users are discarded.
- **Delivery Group:** The Delivery Group the machine is assigned to.
- **Machine Catalog:** The Machine Catalog the machine is assigned to.
- **Active Sessions:** The number of active sessions running on this machine.
- **Disconnected Sessions:** The number of disconnected sessions running on this machine.

Hosts and Citrix®

Citrix tab

The **Citrix** tab for a host in XenCenter shows information about the Citrix Virtual Apps and Desktops environment this host is powering and the machines and sessions hosted in the host. Information shown on this tab is updated every 10 seconds.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the selected host cannot be associated with a Citrix Virtual Apps and Desktops deployment, the tab shows a message. If the host is part of your Citrix Virtual Apps and Desktops environment, this might be caused by incorrect permissions.

Overview

The **Overview** section of this tab shows high-level information about the sessions, machines, Machine Catalogs, and Delivery Groups in the connected Citrix Virtual Apps and Desktops environments.

General

This section shows the following information:

- **Name:** The name of the Citrix Virtual Apps and Desktops site.
- **ID:** The ID of the Citrix Virtual Apps and Desktops site.
- **Sessions:** The total number of sessions in the host and how many of them are disconnected.
- **Machines:** The total number of machines present in the site. This field also shows how many machines are marked as in maintenance mode in Citrix Virtual Apps and Desktops.
- **Delivery Groups:** The total number of Delivery Groups present in the site. This field also shows how many Delivery Groups are marked as in maintenance mode in Citrix Virtual Apps and Desktops.
- **Machine Catalogs:** The total number of Machine Catalogs present in the site. This field also shows how many Machine Catalogs exist in the site for each provisioning type: MCS, PVS, or manual.

Sessions

The **Sessions** section of this tab lists all Citrix Virtual Apps and Desktops sessions on all VMs on this host. For each session, the following information is shown:

- **VM:** The VM this session is on.
- **User:** The full user name of the user of the session.
- **State:** Whether the session is active.
- **Type:** The type of session: Desktop or Application.
- **Session Started:** The start time of the session.
- **Session Established:** The last time the session was actively used by a user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Machine Catalogs

The **Machine Catalogs** section of this tab lists all the Machine Catalogs in the connected Citrix Virtual Apps and Desktops environment. For each Machine Catalog, the following information is shown:

- **Name:** The name of the Machine Catalog.
- **Machine Type:** The type of the machine: virtual or physical.
- **Provisioning Type:** The provisioning type used by the Machine Catalog: MCS, PVS, or manual.
- **Allocation Type:** How machines are allocated by the Machine Catalog: random or static.
- **Total Machine Count:** The total number of machines in this Machine Catalog.
- **Machines Allocated to Server:** The total number of machines in this Machine Catalog that are allocated to this server.

Delivery Groups

The **Delivery Groups** section of this tab lists all the Delivery Groups in the connected Citrix Virtual Apps and Desktops environment. For each Delivery Group, the following information is shown:

- **Name:** The name of the Delivery Group.
- **Server Machine Count:** The total number of machines in this Delivery Group on this server.
- **Server Active Sessions:** The number of active sessions running under the Delivery Group on this server.
- **Server Disconnected Sessions:** The number of disconnected sessions running under the Delivery Group on this server.

Machines

The **Machines** section of this tab lists all the machines in the connected Citrix Virtual Apps and Desktops environment. For each machine, the following information is shown:

- **Name:** The name of the Citrix Virtual Apps and Desktops machine.
- **VM:** The VM that the machine is running on.
- **User Changes Persistence:** Whether changes made by end users are discarded.
- **Delivery Group:** The Delivery Group the machine is assigned to.
- **Machine Catalog:** The Machine Catalog the machine is assigned to.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Active Sessions:** The number of active sessions running on this machine.
- **Disconnected Sessions:** The number of disconnected sessions running on this machine.

Warnings

If you attempt to shutdown or reboot a XenServer host with VMs that host Citrix Virtual Apps and Desktops sessions, XenCenter displays a warning pop up that lists the affected sessions and asks if you want to proceed.

VMs and Citrix®

Citrix tab

The **Citrix** tab for a VM in XenCenter shows information about the Citrix Virtual Apps and Desktops environment this VM is part of and the sessions on this VM. Information shown on this tab is updated every 10 seconds.

If the selected VM cannot be associated with a Citrix Virtual Apps and Desktops deployment, the tab shows a message. If the VM is hosting Citrix Virtual Apps and Desktops sessions, this might be caused by incorrect permissions.

Overview

The **Overview** section of this tab shows General, Machine Catalog, and Delivery Group information related to the Citrix Virtual Apps and Desktops machine powered by the VM.

General

This section shows the following information about the Citrix Virtual Apps and Desktops machine powered by the VM:

- **Name:** The name of the Citrix Virtual Apps and Desktops machine powered by the VM.
- **ID** The ID of the machine powered by the VM. This ID is not the same as the VM UUID.
- **In Maintenance Mode:** Whether the machine is marked as in Citrix Virtual Apps and Desktops maintenance mode.
- **User Changes Persistence Mode:** Whether changes made by end users are discarded.
- **Sessions:** The total number of sessions on this VM and how many of them are disconnected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Machine Catalog

This section shows the following information about the Machine Catalog the machine is assigned to:

- **Name:** The name of the Machine Catalog.
- **ID:** The ID of the Machine Catalog.
- **Description:** A description of the Machine Catalog.
- **Provisioning Type:** The provisioning type used by the Machine Catalog: MCS, PVS, or manual.
- **Allocation Type:** How machines are allocated by the Machine Catalog: random or static.
- **Machine Type:** The type of the machine: virtual or physical.
- **Total Machine Count:** The total number of machines in this Machine Catalog.
- **Machines:** A comma-separated list of all machines in the Machine Catalog, including the currently selected one.

Delivery Group

This section shows the following information about the Delivery Group the machine is assigned to:

- **Name:** The name of the Delivery Group.
- **ID:** The ID of the Delivery Group.
- **Description:** A description of the Delivery Group.
- **In Maintenance Mode:** Whether the Delivery Group is marked as in Citrix Virtual Apps and Desktops maintenance mode.
- **Total Machine Count:** The total number of machines in this Delivery Group.
- **Machines:** A comma-separated list of all machines in the Delivery Group, including the currently selected one.

Sessions

The **Sessions** section of this tab lists all Citrix Virtual Apps and Desktops sessions on this machine. For each session, the following information is shown:

- **User:** The full user name of the user of the session.
- **State:** Whether the session is active.
- **Type:** The type of session: Desktop or Application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Session Started:** The start time of the session.
- **Session Established:** The last time the session was actively used by a user.

Warnings

If you attempt to shutdown, reboot, or suspend a VM that hosts a Citrix Virtual Apps and Desktops session, XenCenter displays a warning pop up that lists the affected sessions and asks if you want to proceed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Managing Servers

Connecting and disconnecting

- Add a server
- Disconnect a server
- Reconnect a server
- Reboot a Server
- Shut Down a Server
- Restart Toolstack
- Configuring Host Power On
- Power on a server remotely
- Run in maintenance mode
- Store Your Server Connection State
- Back up and Restore a Server
- Remove a Server From XenCenter

Configuring networking

- XenServer Networks
- Add a New Network
- Remove a Network
- View and Change Network Properties
- Configuring NICs
- Configuring IP Addresses

More information

- Changing Server Properties
- Changing the Control Domain Memory
- Exporting and Importing a List of Managed Servers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connecting and Disconnecting Servers

- Add a New Server
- Disconnect a Server
- Reconnect a Server
- Reboot a Server
- Shut Down a Server
- Restart Toolstack
- Configuring Host Power On
- Power on a server remotely
- Run in maintenance mode
- Install a TLS Certificate
- Store Your Server Connection State
- Back up and Restore a Server
- Remove a Server From XenCenter

Add a server

To monitor and manage activities on a server from XenCenter®, first identify the server as a managed resource. When you first connect to a server, the server appears in the **Resources** pane on the left of the XenCenter window. The default storage repository for the server (if configured) and any physical CD or DVD drives on the server can also appear here. A managed server can then be disconnected, reconnected, shut down or put into maintenance mode. It remains accessible from the **Resources** pane until you remove it from XenCenter.

The first time you connect to a server using XenCenter, the **Save and Restore Connection State** dialog box appears. By using this dialog, you can set your preferences for storing connection information and restoring server connections at the start of each XenCenter session. For more information, see Store Your Server Connection State.

To add a server to XenCenter

1. Click **Add New Server**. Alternatively:
    - On the **Server** menu, click **Add**.
    - In the **Resources** pane, select the top-level XenCenter entry, right-click and then click **Add** on the shortcut menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On the XenCenter Home page, click the **Add New Server** button:

2. Enter the IP address or DNS name of the server you want to add in the **Server** box. For example: `203.0.113.28` or `server.example.com`.

   TIP:

   You can add multiple servers with the same login credentials by entering the names or IP addresses separated by semicolons in the **Server** box.

3. Type the user name and the password set up during XenServer installation. If Active Directory (AD) authorization has been enabled in your XenServer environment, you can enter your AD credentials here. For more information, see RBAC overview.
4. Click **Add**. A connection progress monitor is displayed: to cancel the connection, click **Cancel**.

Security Certificates

You can configure XenCenter to display a warning message whenever it finds a new or modified TLS security certificate while connecting to a managed server. Click **View Certificate** to view the security certificate. To prevent TLS certificate warnings from being generated, use the **Security Settings** tab in the XenCenter **Options** dialog box.

Disconnect a Server

A disconnected server remains a managed server and remains available in the **Resources** pane with this status icon:


To see which of your servers are currently disconnected, switch to the **Objects** view in the **Navigation** pane and click **Disconnected servers**.

To disconnect a server:

1. Select the server in the **Resources** pane.
2. On the **Server** menu, click **Connect/Disconnect** and then **Disconnect**.

You can reconnect to a disconnected server at any time. For more information, see Reconnect a server.

To remove a disconnected server from the **Resources** pane, see Remove a server from XenCenter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Reconnect a Server

After you have added a server to XenCenter®, it remains accessible in the **Resources** pane throughout the current XenCenter session. It is accessible regardless of the server status: connected or disconnected, running normally or in maintenance mode.

To reconnect to a disconnected server, select it in the **Resources** pane, or right-click and then select **Connect** on the shortcut menu. Connection information for the server is remembered for the current XenCenter session. You do not need to enter the same login credentials more than once in the same XenCenter session if you want to reconnect using the same user account.

You can also reconnect to a connected server using different login credentials, for example, using your AD login instead of your local root account.

To reconnect to a connected server using different login credentials

1. Select the server in the **Resources** pane.
2. Do one of the following:
   - Right-click in the **Resources** pane and select **Reconnect As** on the shortcut menu.
   - On the **Server** menu, select **Connect/Disconnect** and then **Reconnect As**.
3. Enter the new user name and password. If Active Directory authorization has been enabled in your XenServer environment, you can enter your AD credentials here. See RBAC overview.
4. Click **OK**.

Reboot a Server

When you reboot a server in XenCenter®, the server shuts down any VMs running on it. After the VMs shut down, the server is disconnected and rebooted. If the server is a member of a pool, the loss of connectivity on shutdown is handled and the pool recovers when the server returns. If you shut down another pool member (not the pool coordinator), the other pool members and the pool coordinator continue to function. If you shut down the pool coordinator, the pool is out of action until the pool coordinator is rebooted and back on line. When the pool coordinator restarts, the other members reconnect and synchronize with the pool coordinator. Alternatively, you can make one of the other members into the pool coordinator by using the xe CLI.

VMs with XenServer VM Tools installed are shut down gracefully when you reboot the host server. However, VMs without XenServer VM Tools installed are shut down using a forced shutdown. To

© 1997–2026 Citrix Systems, Inc. All rights reserved.

avoid forced shutdowns, install the XenServer VM Tools on your VMs. For more information, see Installing XenServer VM Tools.

After a server reboot, XenCenter attempts to reconnect to the server automatically. After the server reconnects, restart any VMs that were running on it unless they are configured to start automatically on server reboot. For more information, see Change VM properties.

To reboot a server

Select the server in the **Resources** pane and then click **Reboot** on the Toolbar.

Shut Down a Server

When you shut down a server in XenCenter®, the server shuts down any VMs running on it, and then the server is disconnected and powered off. If the server is a member of a pool, the loss of connectivity on shutdown is handled and the pool recovers when the server returns. If you shut down another pool member (not the pool coordinator), the other pool members and the pool coordinator continue to function. If you shut down the pool coordinator, the pool is out of action until the pool coordinator is rebooted and back on line. At which point the other members reconnects and synchronizes with the pool coordinator. Alternatively, you can make one of the other members into the pool coordinator, which you can do by using the xe CLI.

VMs with XenServer VM Tools installed are shut down gracefully. However, VMs without XenServer VM Tools installed are shut down using a forced shutdown. To avoid forced shutdown, install the XenServer VM Tools on all VMs. For more information, see Install XenServer VM Tools.

After you power the server back on, you must connect to it again. For more information, see Reconnect a server.

To shut down a server

Select the server in the **Resources** pane and then select **Shut Down** on the toolbar.

When the server has been shut down, its status in the **Resources** pane changes to **Disconnected**.



Restart Toolstack

The **Restart Toolstack** option allows you to restart the XenServer® management toolstack. This toolstack controls VM lifecycle operations, host and VM networking, VM storage, and user authentication. It allows the management of XenServer resource pools. The toolstack provides the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

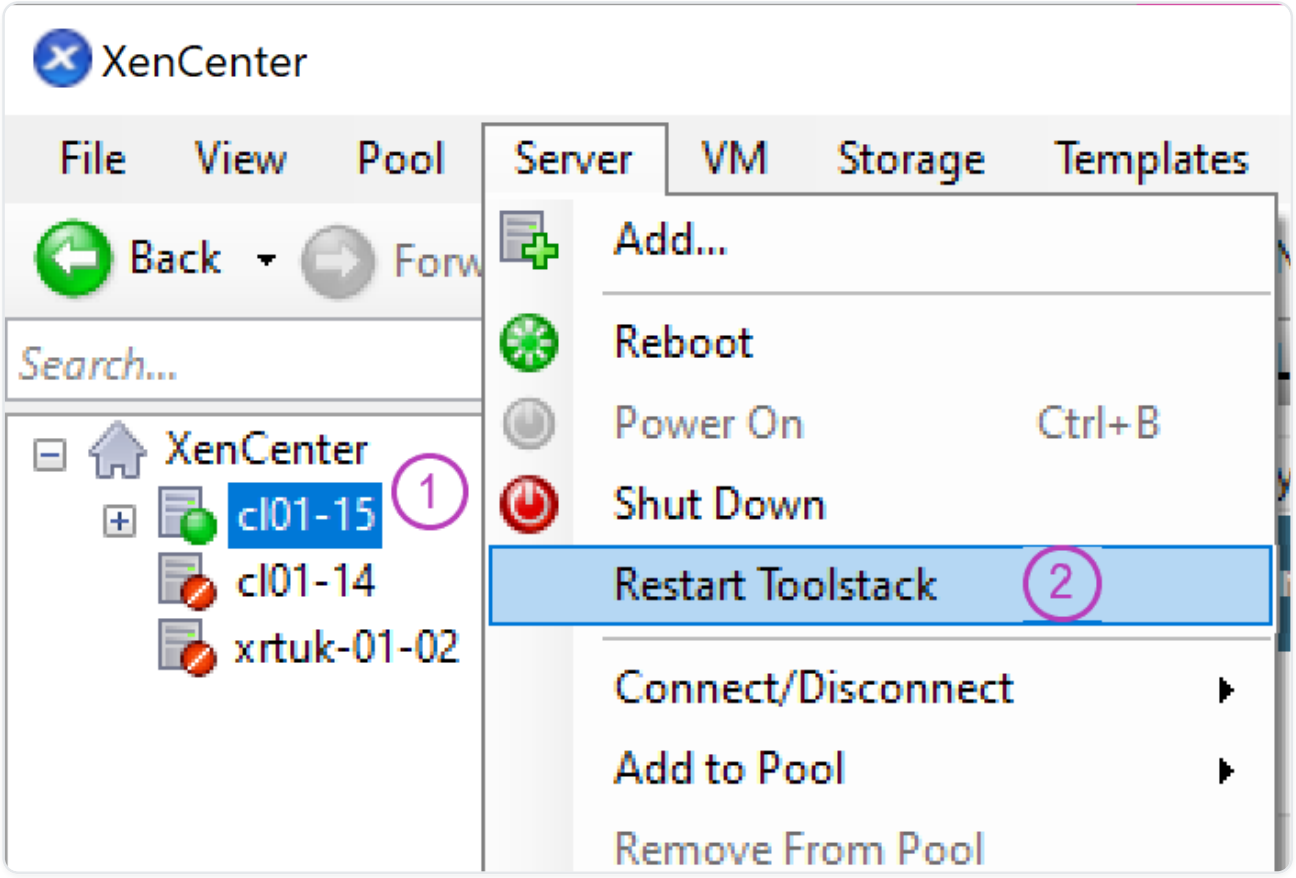
publicly documented Management API, which is used by all tools that manage VMs and resource pools.

NOTE:

Sometimes, the **Restart Toolstack** option can be used for troubleshooting XenServer issues. However, be cautious when using this option, as incorrect usage can cause unexpected results.

Do not restart the toolstack while HA is enabled. If possible, temporarily disable HA before restarting the toolstack.

To restart the toolstack



1. Select the server in the **Resources** pane.
2. On the **Server** menu, click **Restart Toolstack**.
3. Click **Yes** to confirm.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

When you run the **Restart Toolstack** option on the pool coordinator, XenCenter® loses connection to the pool and then automatically attempts to reconnect.

Configuring Host Power On

The XenServer® Host Power On feature allows you to manually turn a remote host (server) on and off. To use this feature, you need to carry out the following steps:

1. Ensure that the server supports remote power control. That is, the server has one of the following capabilities:
   - Wake on LAN functionality
   - IPMI support
   - A custom script
2. Enable the Host Power On functionality.

   To perform this procedure for DRAC processors, you need the credentials for the processor, which are set in its firmware.

After Host Power On has been configured on a server, you can power the server on from XenCenter. Select the server and then, on the **Server** menu, click **Power On**.

If you have installed and configured Workload Balancing, you can also configure XenServer to turn hosts on and off as VMs are consolidated or brought back online. This feature is known as Power Management.

Prerequisites for Host Power On

To enable the Host Power On feature, the host server must have one of the following power control solutions:

- A network card that supports **Wake On LAN (WOL)**.
- **Intelligent Platform Management Interface (IPMI)** support.
- A custom power-on script based on the Management API that enables you to turn the power on and off through XenServer. For more information, see Hosts and Resource Pools.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To enable or disable Host Power On

You can enable Host Power On for an individual server by using the server **Properties** window, or on multiple servers by using the pool **Properties** window.

1. Select the server or pool and open its **Properties** dialog box: on the **Server** or **Pool** menu, click **Properties**.
2. Click the **Power On** tab and under **Power On mode**, select the option you want:
   - **Disabled** Select this option to disable the Host Power On feature.
   - **Wake on LAN (WOL)** To use this option, the host must have a Wake on LAN-enabled network card.
   - **Intelligent Platform Management Interface (IPMI)** To use this option, your server must support power management through IPMI.
   - **Custom power-on script** You can use a custom Python 3 Linux script to turn on the power on the XenServer host from a remote location. For information about creating the script, including a list of supported key/value pairs, see the Hosts and resource pools.
3. If you selected IPMI, enter the following information:
   - **IP Address** The IP address you specified configured to communicate with the IPMI controller.
   - **User name** This is the user name that is associated with the management processor. You might have changed this value from its factory default settings.
   - **Password** This is the password associated with that user name.
4. If you selected **Custom power-on script**, enter the file name and path to the custom script you created. Under **Configuration options**, enter the key/value pairs you want to use to configure the script. Move between fields by clicking or tabbing.

   You do not need to specify the .py extension when you specify the file name of the custom script.
5. Click **OK** to save your configuration changes and close the **Properties** window.

After configuration, you can configure and run the Workload Balancing Automation and Host Power On features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- Host power-on

Power on a server remotely

The Host Power On feature allows you to remotely power on managed servers from XenCenter. For servers to use this feature, they must fulfill the following criteria:

- The server has remote power control support: Wake-on-LAN functionality, IPMI, or a custom power-on script.
- You have enabled Host Power On in the server **Properties** settings. This feature can be enabled once for multiple servers at pool-level. For more information, see Configuring Host Power On.

After Host Power On has been configured, select the server or servers and then do one of the following:

- On the **Server** menu, select **Power On**.
- Right-click and select **Power On**.

Related documentation

XenServer Current Release

- Host power-on

Run in maintenance mode

You might want to take a managed server offline for various reasons. For example:

- To do a rolling upgrade of virtualization software
- To add or test connectivity to a new network
- To diagnose an underlying hardware issue
- To add connectivity to a new storage system.

Use XenCenter® to take a server offline temporarily by placing it into *maintenance mode*. When you place a server in a resource pool into maintenance mode, all running VMs on it are

© 1997–2026 Citrix Systems, Inc. All rights reserved.

automatically migrated to another server in the same pool. If the server is the pool coordinator, a new pool coordinator is also selected for the pool.

When Workload Balancing is enabled, it migrates the running VMs on that server to their optimal servers when available. These migrations are based on Workload Balancing recommendations: performance data, your placement strategy, and performance thresholds.

While a server is maintenance mode, you cannot create or start any VMs on it.

To place a server in maintenance mode

In the **Infrastructure** view of the XenCenter resources pane (left pane), select the server and then do one of the following:

- Right-click the server name and choose **Enter Maintenance Mode** from the shortcut menu.
- On the **Server** menu, select **Enter Maintenance Mode**.

After all running VMs successfully migrate off the server, the server's status in the **Resources** pane changes to show the server maintenance mode icon.



To take a server out of maintenance mode

In the **Infrastructure** view of the XenCenter resources pane (left pane), select the server and then do one of the following:

- Right-click the server name and choose **Exit Maintenance Mode** on the shortcut menu.
- On the **Server** menu, select **Exit Maintenance Mode**.

Related documentation

XenServer Current Release

- Prepare a pool of XenServer hosts for maintenance

Install a TLS certificate on your server

The XenServer host comes installed with a default TLS certificate. However, to use HTTPS to secure communication between XenServer and Citrix Virtual Apps and Desktops™, install a certificate provided by a trusted certificate authority.

This article contains information about how to use certificates in XenCenter. For information about working with certificates by using the xe CLI, see Hosts and resource pools.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements

Ensure that your TLS certificate and its private key meet the following requirements:

- The certificate and key pair are an RSA key
- The key matches the certificate
- The key is provided in a separate file to the certificate
- The certificate is provided in a separate file to any intermediate certificates
- The key file must be one of the following types: `.pem` or `.key`
- Any certificate files must be one of the following types: `.pem`, `.cer`, or `.crt`
- The key is greater than or equal to 2,048 bits and less than or equal to 4,096 bits in length
- The key is an unencrypted PKCS #8 key and does not have a passkey
- The key and certificate are in base-64 encoded 'PEM' format
- The certificate is valid and has not expired
- The signature algorithm is SHA-256 or SHA-512

XenCenter® warns you when the certificate and key you choose do not meet these requirements.

Install a certificate

You can use XenCenter to install a certificate that is in a location accessible from XenCenter into a XenServer® host.

To install a certificate on a XenServer host, you must have the Pool Admin role and the XenServer host must not have HA enabled.

1. Go to the **Install Certificates** dialog. You can get to this dialog in one of the following ways:
   - In the **Server** menu, select **Install Certificates**.
   - Right-click on the host in the resources pane and choose **Install Certificates** from the context menu.
   - In the **General** tab of the host, right-click on the **Certificates** section and choose **Install Certificates** from the context menu.
2. In the **Install Certificates** dialog, browse to the location of the private key file and select it.
3. Browse to the location of the server certificate file and select it.
4. You can choose to add any number of intermediate certificates from the certificate chain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Click **Add**

b. Browse to the location of one or more intermediate certificates and select them.

5. Click **Install**.

   XenCenter validates and installs the certificates.

   - If there is a problem with a certificate, XenCenter shows an error message. Attempt to correct the problem and click **Install** again.
   - If the certificate is installed successfully, XenCenter shows a success message. You can now click **Close** to close the dialog.

When the certificate on a XenServer host is changed, the host closes any open connections. XenCenter expects this behavior and reopens the connection with the XenServer host. However, you might have to manually reopen any other connections that were previously open to the host - for example, from another API client or the remote xe CLI.

View certificate information

In the **General** tab for a XenServer host, a section called **Certificates** displays the following information for the host:

- The certificate validity period. This text appears red when the certificate is approaching its expiry date.
- The certificate thumbprint

The **General** tab for a XenServer pool displays the following information for the pool:

- The **General** section has an entry for **Certificate Verification** which shows whether certificate verification is enabled or disabled.
- The **Certificates** section lists the name, validity, and thumbprint for the CA certificates.

Enabling certificate verification for your pool

Certificate verification is enabled by default on fresh installations of XenServer. For more information, see Certificate verification.

If you upgrade from an earlier version of XenServer, certificate verification is not enabled automatically and you must enable it. XenCenter prompts you to enable certificate verification the next time you connect to the upgraded pool.

Before enabling certificate verification on a pool, ensure that no operations are running in the pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenCenter provides several ways to enable certificate verification.

- When first connecting the XenCenter to a pool without certificate verification enabled, you are prompted to enable it. Click **Yes, Enable certificate verification**.
- In the **Pool** menu, select **Enable Certificate Verification**.
- On the **General** tab of the pool, right-click the entry **Certificate Verification** and choose **Enable Certificate Verification** from the menu.

Reset server identity certificates

You can reset the server identity certificate from XenCenter or the xe CLI. Resetting a certificate deletes the certificate from the host and installs a new self-signed certificate in its place.

To reset a certificate in XenCenter:

1. Go to the **General** tab for the host.
2. In the **Certificates** section, right-click on the certificate you want to reset.
3. From the menu, select **Reset Certificate**.
4. In the dialog that appears, click **Yes** to confirm the certificate reset.

Alternatively, in the **Server** menu, you can go to **Certificate > Reset Certificate**.

When you reset a certificate, any existing connections to the XenServer host are disconnected — including the connection between XenCenter and the host.

For information about resetting a certificate by using the xe CLI, see Certificate verification.

Certificate alerts

When your certificates are nearing their expiry date, XenCenter shows alerts in the **Alerts** section of the **Notifications** tab. You can choose to open the **Install Certificates** dialog from the action menu of these alerts.

For more information about alerts, see XenCenter Alerts.

Related documentation

XenServer Current Release

- Install a TLS certificate on your host
- Certificate verification

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Store Your Server Connection State

Login credentials - your user name and password - for all your managed servers can be stored between XenCenter® sessions and used to automatically reconnect to them at the start of each new XenCenter session. When you enable this feature, XenCenter remembers the connection state of all your managed servers at the end of each session. XenCenter attempts to restore the servers at the start of your next session. If a server was connected at the end of your previous session, it is reconnected automatically without prompting you for your server login details. If a server was disconnected at the end of your previous session, it is not reconnected automatically.

If you disable the automatic reconnection feature, you must reconnect to all your managed servers each time you open XenCenter. You then enter your user name and password for each server.

NOTE:

Your system administrator can disable the saving of server login credentials, so this feature might not be available.

You can optionally protect your stored login credentials with a main password to ensure they remain secure. At the start of each session, you are prompted to enter this main password before connections to your managed servers are restored.

To turn automatic reconnection on or off

1. Open the XenCenter **Options** dialog box: on the **Tools** menu, click **Options**.
2. Click the **Save and Restore** tab.
3. Select or clear the **Save and restore server connection state on startup** check box.

Using a main password

When you choose to store login credentials in XenCenter, you can also set a main password. You must enter this main password before connections to your managed servers are automatically restored. You set, remove, and change the main password from the **Save and Restore** tab in the XenCenter **Options** dialog box.

If you lose or forget the main password, it cannot be recovered. You must connect to each managed server again and then set a new main password.

To set a main password:

1. Open the XenCenter **Options** dialog box: on the **Tools** menu, click **Options**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click the **Save and Restore** tab.
3. Ensure that the **Save and restore server connection state on startup** check box is selected.
4. Under **Main password**, select the **Require a main password** check box, then enter and confirm the password, and click **OK**. Remember that passwords are case-sensitive.

To change the main password:

1. Open the XenCenter **Options** dialog box: on the **Tools** menu, click **Options**.
2. Click the **Save and Restore** tab.
3. Under **Main password**, click **Change main password**.
4. Enter the existing main password, then enter and confirm the new main password, and then click **OK**.

To clear the main password:

1. Open the XenCenter **Options** dialog box: on the **Tools** menu, click **Options**.
2. Click the **Save and Restore** tab.
3. Under **Main password**, clear the **Require a main password** check box.
4. When prompted, enter and confirm the current main password, then click **OK**.

Back up and Restore a Server

You can back up a managed server to one XenServer backup file (`.xbk`). This backup file can be used to restore the server if there is a hardware failure.

NOTE:

This file backs up just the server itself, but not any VMs that might be running on it.

We recommend that you back up your servers frequently to enable you to recover from possible server or software failure. When backing up servers in XenCenter®, note the following points:

- Do not create the backup on XenServer control domain (dom0). For more information about XenServer control domains, see the product documentation.
- XenServer® backup files can be large.

To restore a server, you can select and restore the backup file within XenCenter. Reboot the server from XenServer installation ISO to complete the restore.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To back up your server configuration and software

1. Select the server in the **Resources** pane.
2. On the **Server** menu, click **Back Up**.
3. Browse to locate the folder where you want to create the backup file and enter the file name.
4. Click **Save** to begin the backup.

The backup might take some time. You can select the **Notifications** and then **Events** to view the progress.

To restore server software and configuration from backup

1. Select the server in the **Resources** pane.
2. On the **Server** menu, click **Restore From Backup**.
3. Browse to locate the backup file.
4. Click **Open** to begin the restore.
5. On the server, reboot to the installation CD and select **Restore from backup**.

Related documentation

XenServer Current Release

- Back up and restore hosts and VMs

Remove a Server From XenCenter®

Removing a managed server from XenCenter stops all managing and monitoring activities for that server. It does not affect the activities running on the server itself or remove any VMs installed on it. Removing a server breaks the connection between XenCenter and the server and its VMs. The server is no longer displayed in XenCenter.

To remove a server, select it in the **Resources** pane. In the **Server** menu, select **Remove from XenCenter**.

To return a server that you removed to the list of managed resources, add it again to XenCenter in the same way as you first connected to it. For more information, see Add a server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring Networking

Each managed server has one or more networks. XenServer® networks are virtual Ethernet switches that can be connected to an external interface or can be entirely virtual, internal to an individual server or pool. The external interface can be with or without a VLAN tag.

When the XenServer product is installed on a physical server, a network is created for each physical NIC on the server. The network works as a bridge between a virtual network interface on a VM (VIF) and a physical network interface (PIF) associated with a NIC on the server.

When you move a managed server into a pool, these default networks are merged and physical NICs with the same device name are attached to the same network. Typically, you add a network in the following cases:

- to create an internal network
- to set up a new VLAN using an existing NIC
- to create a NIC bond

You can configure up to 16 networks per managed server, or up to 8 bonded network interfaces.

Jumbo frames can be used to optimize performance of traffic on storage networks, VM networks, and the management network. You can set the Maximum Transmission Unit (MTU) for a new server network in the **New Network** wizard or for an existing network in its **Properties** window. The possible MTU value range is 1500–9216.

Network types

There are three different physical network types to choose from when creating a network within XenCenter.

Single-Server private network

This type of network is an internal network that has no association with a physical network interface. It provides connectivity only between the virtual machines on a given server, with no connection to the outside world.

External network

This type of network has an association with a physical network interface and provides a bridge between virtual machines and your external network. The bridge enables VMs to connect to external resources through the server's physical NIC.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bonded network

This type of network bonds two or more NICs to create a single, high-performing channel that provides connectivity between VMs and your external network. Three bond modes are supported:

- **Active-active**

  In this mode, traffic is balanced between the bonded NICs. If one NIC within the bond fails, all network traffic for the host automatically routes over the second NIC. This mode provides load balancing of virtual machine traffic across the physical NICs in the bond.

- **Active-passive**

  Only one NIC in the bond is active. The inactive NIC becomes active if and only if the active NIC fails, providing a hot-standby capability.

- **Link Aggregation Control Protocol (LACP) Bonding**

  This mode provides active-active bonding, where traffic is balanced between the bonded NICs. Unlike the active-active bond in a Linux bridge (deprecated) environment, LACP can load balance all traffic types. Two available options in this mode are:

  - **LACP with load balancing based on source MAC address**

    In this mode, the outgoing NIC is selected based on the MAC address of the VM from which the traffic originated. Use this option to balance traffic in an environment where you have several VMs on the same host. This option is not suitable if there are fewer VIFs than NICs: as load balancing is not optimal because the traffic cannot be split across NICs.

  - **LACP with load balancing based on IP and port of source and destination**

    In this mode, the source IP address, the source port number, the destination IP address, and the destination port number are used to route the traffic across NICs. This option is ideal to balance traffic from VMs and the number of NICs exceeds the number of VIFs. For example, when only one virtual machine is configured to use a bond of three NICs.

Notes

- Configure vSwitch as the network stack to be able to view the LACP bonding options in XenCenter and to create a LACP bond. Also, your switches must support the IEEE 802.3ad standard.
- Active-active and active-passive bond types are available for both the vSwitch and Linux bridge.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can bond either two, three, or four NICs when vSwitch is the network stack. However, you can only bond two NICs when a Linux bridge is the network stack.

NOTE:

The Linux bridge network stack is deprecated and will be removed in a future release.

For more information about the support for NIC bonds in XenServer, see Networking.

Related documentation

XenServer Current Release

- Manage networking

Add a network

To create a new network in a pool or on a standalone server, use the **New Network** wizard: select the server or pool in the **Resources** pane, select the **Networking** tab and then click **Add Network**.

To add an external network

An external network has an association with a physical NIC and provides a bridge between virtual machines and your external network. This bridge enables VMs to connect to external resources through the NIC.

1. Open the **New Network** wizard.
2. On the first page of the wizard, select **External Network** and then click **Next**.
3. Enter the name and an optional description for the new network, and then click **Next**.
4. On the **Network settings** page, configure the NIC, VLAN, and MTU settings for the new network:
    a. From the **NIC** list, choose a physical NIC.
    b. In the **VLAN** box, assign a number to the new virtual network.
    c. To use jumbo frames, set the Maximum Transmission Unit (**MTU**) to a value between 1500–9216.
    d. To create a VLAN on an SR-IOV network, choose the NIC on which SR-IOV is enabled (Step 4a). Check the **Create the VLAN on the SR-IOV network** check box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Select the **Automatically add this network to new virtual machines** check box to have the new network added to any new VMs created using the **New VM** wizard.
6. Click **Finish** to create the new network and close the wizard.

To add a single-server private network

A single-server private network is an internal network that has no association with a physical network interface. It provides connectivity only between the VMs on a given server. This network has no connection to VMs on other servers in the pool or to the outside world.

1. Open the **New Network** wizard.
2. On the first page of the wizard, select **Single-Server Private Network** and then click **Next**.
3. Enter a name and an optional description for the new network, and then click **Next**.
4. On the **Network settings** page, select the **Automatically add this network to new virtual machines** check box. This selection ensures that the new network is added to any new VMs created using the **New VM** wizard.
5. Click **Finish** to create the new network and close the wizard.

To add a new bonded network

This type of network bonds two or more NICs together to create a single, high-performing channel that provides connectivity between VMs and your external network.

NOTE:

Whenever possible, create NIC bonds when you initially create your resource pool and before joining more servers to the pool or creating VMs. The bond configuration is automatically replicated to servers as they joined the pool. This action reduces the number of steps required.

1. Open the **New Network** wizard.
2. On the first page of the wizard, select **Bonded Network** and then click **Next**.
3. On the **Bond Members** page, select the NICs you want to bond together. To select a NIC, select its check box in the list. Up to four NICs can be selected in this list. Clear the check box to deselect a NIC.
4. Under **Bond mode**, choose the type of bond:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Select **Active-active** to configure an active-active bond. With this bond, traffic is balanced between the bonded NICs. If one NIC within the bond fails, the server's network traffic automatically routes over the second NIC.
- Select **Active-passive** to configure an active-passive bond, where traffic passes over only one of the bonded NICs. In this mode, the second NIC only becomes active if the active NIC fails, for example, if it loses network connectivity.
- Select **LACP with load balancing based on source MAC address** to configure a LACP bond. With this bond, the outgoing NIC is selected based on the MAC address of the VM from which the traffic originated. Use this option to balance traffic in an environment where you have several VMs on the same host. This option is not suitable if there are fewer virtual interfaces (VIFs) than NICs: as load balancing is not optimal because the traffic cannot be split across NICs.
- Select **LACP with load balancing based on IP and port of source and destination** to configure a LACP bond. This bond uses the source IP address, source port number, destination IP address, and destination port number to allocate the traffic across the NICs. Use this option to balance traffic from VMs in an environment where the number of NICs exceeds the number of VIFs.

NOTES:

- To be able to view the LACP bonding options in XenCenter and to create a LACP bond, configure vSwitch as the network stack. Also, your switches must support the IEEE 802.3ad standard.
- Active-active and active-passive bond types are available for both the vSwitch and Linux bridge.
- You can bond either two, three, or four NICs when vSwitch is the network stack. However, you can only bond two NICs when the Linux bridge is the network stack.

5. To use jumbo frames, set the Maximum Transmission Unit (**MTU**) to a value between 1500–9216.
6. Select the **Automatically add this network to new virtual machines** check box to have the new network added to any new VMs created using the **New VM** wizard.
7. Click **Finish** to create the new network and close the wizard.

For more information, see Configuring NICs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To add an SR-IOV Network

Single Root I/O Virtualization (SR-IOV) is a PCI device virtualization technology that allows a single PCI device to appear as multiple PCI devices on the physical PCI bus. The physical device is known as a Physical Function (PF). The others are known as Virtual Functions (VF). SR-IOV enables the hypervisor to directly assign one or more of these VFs to a Virtual Machine (VM) using SR-IOV technology. The guest can then use the VF as any other directly assigned PCI device.

1. Open the **New Network** wizard.
2. On the first page of the wizard, choose **SR-IOV Network** and then click **Next**.
3. Enter a name and an optional description for the new network, and then click **Next**.
4. Choose a NIC from the list. NIC0 is not available in the list.
5. On the **Network settings** page, select the **Automatically add this network to new virtual machines** check box to have the new network added to any new VMs created using the New VM wizard.
6. Click **Finish**.

   Creating an SR-IOV network affects network connection status. XenCenter® connections to the pool can be temporarily disturbed.
7. Click **Create SR-IOV anyway** to create the network and close the wizard. The network created appears in the **NICs** tab indicating the number of VFs remaining or if it is disabled.

Related documentation

XenServer Current Release

- Manage networking

Remove a Network

1. Select the server or pool in the **Resources** pane.
2. Select the **Networking** tab.
3. On the **Networking** tab, select the network in the list.
4. Click **Remove Network**.

Related documentation

XenServer Current Release

- Manage networking

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View and Change Network Properties

To view a server's current networking configuration

Select the **Networking** tab for a server to see all the networks currently configured on the server, with information about each one:

Name	The name of the network.
Description	(Optional) A description of the network.
NIC	The physical NIC, NIC bond, or internal virtual network used by the network.
VLAN	For external networks, this column shows the virtual LAN (VLAN) tag.
Auto	This column shows whether the network is automatically added to any new virtual machines created using the **New VM** wizard.
Link Status	The link status of the network: connected or disconnected.
MAC	The MAC address of the network adapter (NIC). This value is a unique identifier for a particular network adapter.
MTU	A Maximum Transmission Unit value between 1500–9216 allows the use of jumbo frames.

To change a server's networking configuration

On the XenCenter® **Networking** tab, select the network and select **Properties**. In addition to name, description, folder, tags, and custom fields, you can also change various network configuration settings on the **Network Settings** tab:

Bond mode

This configuration option appears on bonded networks only.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Select **Active-active** to configure an active-active bond. With this bond, traffic is balanced between the bonded NICs. If one NIC within the bond fails, the host server's network traffic automatically routes over the second NIC.
- Select **Active-passive** to configure an active-passive bond, where traffic passes over only one of the bonded NICs. In this mode, the second NIC only becomes active if the active NIC fails, for example, if it loses network connectivity.
- Select **LACP with load balancing based on source MAC address** to configure a LACP bond. With this bond, the outgoing NIC is selected based on MAC address of the VM from which the traffic originated. Use this option to balance traffic in an environment where you have several VMs on the same host. This option is not suitable if there are fewer virtual interfaces (VIFs) than NICs: as load balancing is not optimal because the traffic cannot be split across NICs.
- Select **LACP with load balancing based on IP and port of source and destination** to configure a LACP bond. This bond uses the source IP address, source port number, destination IP address, and destination port number to allocate the traffic across the NICs. Use this option to balance the traffic in an environment where the number of NICs exceeds the number of VIFs.

NOTES:

- To be able to view the LACP bonding options in XenCenter and to create a LACP bond, configure vSwitch as the network stack. Also, your switches must support the IEEE 802.3ad standard.
- Active-active and active-passive bond types are available for both the vSwitch and Linux bridge.
- You can bond either two, three, or four NICs when vSwitch is the network stack, whereas you can only bond two NICs when Linux bridge is the network stack.

The Linux bridge network stack is deprecated and will be removed in a future release.
For more information, see Configuring NICs.

MTU

To use jumbo frames, set the Maximum Transmission Unit (**MTU**) to any value between 1500–9216.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Automatically add this network to new virtual machines

Select this check box to have the network automatically added to new VMs when they are created using the **New VM** wizard.

Related documentation

XenServer Current Release

- Manage networking

Configuring NICs

XenServer® automatically manages NICs as needed based on the related network, virtual network interface, server network, and bond configuration. You can view the available NICs, configure NIC bonds, and dedicate NICs to a specific function from the **NICs** tab.

NIC bonding can improve server resiliency by using two or more physical NICs as if they were one. Two or more NICs can be bonded to create a single, high-performing channel that provides connectivity between VMs and your external network. Three bond modes are supported:

Active-active: This mode provides load balancing of virtual machine traffic across the physical NICs in the bond. If one NIC within the bond fails, the server's network traffic automatically routes over the second NIC.

Active-passive: This mode provides failover capability. Only one NIC in the bond is active. The inactive NIC becomes active if and only if the active NIC fails.

Link Aggregation Control Protocol (LACP) Bonding: This mode provides active-active bonding, where traffic is balanced between the bonded NICs. Unlike the active-active bond in a Linux bridge (deprecated) environment, LACP can load balance all traffic types.

NOTE:

Configure vSwitch as the network stack to be able to view the LACP bonding options in XenCenter and to create a LACP bond. Also, your switches must support the IEEE 802.3ad standard. The switch must contain a separate LAG group configured for each LACP bond on the host. For more details about creating LAG groups, see Networking.

When you bond separate NICs using XenCenter®, a new NIC is created. This NIC is the bond interface, and the other NICs are referred to as the bonded NICs. The NIC bond can then be connected to XenServer network to allow virtual machine traffic and server management functions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

to take place. You can create NIC bonds in XenCenter from the **NICs** tab or from the server's **Networking** tab. Use the network type **Bonded Network**.

Viewing available NICs

For each available NIC on a server, the following device properties are shown on the **NICs** tab:

NIC	Identifies the physical NIC or internal virtual network.
MAC	The MAC (Media Access Control) address of the NIC.
Link Status	The connection status of the NIC: Connected or Disconnected.
Speed	The data transfer rate of the NIC.
Duplex	The duplexing mode of the NIC: full or half.
Vendor, Device	The NIC vendor and device names.
PCI Bus Path	The PCI bus path for pass-through devices.

When you add a physical interface on your server (for example, a new Ethernet controller) it might not appear in the list on the **NICs** tab. If this situation happens, complete the following steps:

1. Ensure that you restart your host after installing the new physical interface or related drivers.
2. Click **Rescan** on the **NICs** tab to force the server to scan for new cards. The interface now appears in the **NICs** tab of your server.
3. If the NIC is listed as **Disconnected**, you can reboot the host or run the command `xe pif.plug` in the host console. For more information, see Manage networking.

To create a NIC bond

1. Ensure that the NICs you want to bind together are not in use. Shut down any VMs with virtual network interfaces using the bonded NICs before creating the bond. After you have created the bond, reconnect the virtual network interfaces to an appropriate network.
2. Select the server in the **Resources** pane on the left, then click the **NICs** tab and click **Create Bond**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select the NICs you want to bond together. To select a NIC, select its check box in the list. Up to four NICs can be selected in this list. Clear the check box to deselect a NIC. To maintain a flexible and secure network, you can bond either two, three, or four NICs when vSwitch is the network stack. However, you can only bond two NICs when Linux bridge is the network stack.
4. Under **Bond mode**, choose the type of bond:

   - Select **Active-active** to configure an active-active bond. With this bond, traffic is balanced between the bonded NICs. If one NIC within the bond fails, the host server's network traffic automatically routes over the second NIC.
   - Select **Active-passive** to configure an active-passive bond, where traffic passes over only one of the bonded NICs. In this mode, the second NIC only becomes active if the active NIC fails, for example, if it loses network connectivity.
   - Select **LACP with load balancing based on source MAC address** to configure a LACP bond. With this bond, the outgoing NIC is selected based on MAC address of the VM from which the traffic originated. Use this option to balance traffic in an environment where you have several VMs on the same host. This option is not suitable if there are fewer virtual interfaces (VIFs) than NICs: as load balancing is not optimal because the traffic cannot be split across NICs.
   - Select **LACP with load balancing based on IP and port of source and destination** to configure a LACP bond. This bond uses the source IP address, source port, destination IP address, and destination port to allocate the traffic across the NICs. Use this option to balance traffic from VMs in an environment where the number of NICs exceeds the number of VIFs.

     NOTE:

     LACP bonding is only available for the vSwitch, whereas active-active and active-passive bonding modes are available for both the vSwitch and Linux bridge.

     For more information about the support for NIC bonds in XenServer, see the Networking.
5. To use jumbo frames, set the Maximum Transmission Unit (**MTU**) to a value between 1500–9216.
6. To have the new bonded network automatically added to any new VMs created using the **New VM** wizard, select the check box.
7. Click **Create** to create the NIC bond and close the dialog box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenCenter automatically moves management and secondary interfaces from bonded NICs to the bond interface when the new bond is created.

A server with its management interface on a bond is not permitted to join a pool. Reconfigure the server's management interface and move it back on to a physical NIC before it can join a pool.

Deleting a NIC bond

If reverting a server to a non-bonded configuration, be aware of the following requirements:

- As when creating a bond, all virtual machines with virtual network interfaces that use the bond must be shut down before destroying the bond. After reverting to a non-bonded configuration, reconnect the virtual network interfaces to an appropriate network.
- Move the management interface to another NIC using the **Management interfaces** dialog box before you delete the bond, otherwise connections to the server (including XenCenter) are dropped.

To delete a bond

1. Select the server in the **Resources** pane on the left, then click the **NICs** tab.
2. Click **Delete Bond**.

Dedicating a NIC to a specific function

You can assign IP addresses to NICs to dedicate a NIC to a specific function, such as storage or other types of network traffic. For more information, see Configuring IP Addresses.

Related documentation

XenServer Current Release

- Manage networking

Configuring IP Addresses

The NIC used as the management interface on a managed server is initially specified during XenServer installation. XenCenter®, xe CLI, and any other management software that runs on a separate machine use the IP address of the management interface to connect to the server.

If a server has two or more NICs, you can select a different NIC or NIC bond to use as its management interface. You can assign IP addresses to NICs and dedicate NICs to a specific function, such as storage or other types of network traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When a new server joins a pool, the new server inherits the pool coordinator's networking configuration, including network and bond information. However, the joining server's management interface is not changed to match the pool coordinator. Reconfigure it after joining to use the same bond as the pool coordinator server.

NOTE:

A server with its management interface on a bond is not permitted to join a pool. Reconfigure the server's management interface and move it back on to a physical NIC before it can join a pool.

In XenCenter, use the **Configure IP Addresses** dialog to assign an IP address to a NIC and change the management interface for a server or pool. The following sections provide instructions for completing these actions.

To assign an IP address to a NIC

You can use XenCenter to configure a NIC with an IP address to carry out a specific function, such as storage traffic. When you configure a NIC with an IP address, you are essentially creating a secondary interface.

To maintain a flexible and secure network, you can segment network traffic by creating secondary interfaces that use a dedicated NIC. For example, establish separate networks for server management, application production traffic, and storage traffic. In the default XenServer® networking configuration, all network traffic to IP-based storage devices occurs over the NIC used for the management interface. It is important to note that the secondary interfaces inherit the DNS server settings from the management interface.

To assign an IP address to a NIC, to carry out a specific function, ensure the appropriate network configuration is in place to ensure the NIC is used for the desired traffic. For example, to dedicate a NIC to storage traffic, assign the newly created interface an IP address that fulfills the following criteria:

- The IP address is on the same subnet as the storage controller, if applicable.
- The IP address is on a different subnet than the management interface.
- The IP address is not on the same subnet as any other secondary interfaces.

Ensure that you configure the NIC, storage target, switch, and VLAN so that the target is only accessible over the assigned NIC. This action allows the use of standard IP routing to control how traffic is routed between multiple NICs within a managed server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Perform the following tasks to assign an IP address to a NIC and create a secondary interface:

1. On the **Networking** tab for a server or pool, under **IP Address Configuration**, select **Configure**.
2. Click **Add IP address**.
3. Enter a name for the new secondary interface.
4. Choose your network from the **Network** list.
5. Configure the networking settings for the new interface:
   - To use the automated DHCP to automatically assign networking settings including the IP address, subnet mask and gateway, select **Automatically obtain settings using DHCP**.
   - To configure networking settings manually, select **Use these settings** and enter the required values. Enter an IP address and a subnet mask. You can optionally enter the gateway settings.
6. To configure extra interfaces, select **Add IP address** again and repeat the preceding configuration steps.
7. When you have finished, click **OK** to save your configuration choices.

> **NOTE:**
>
> If you choose to configure the network settings manually, you are prompted to confirm your settings. Click **Reconfigure anyway** to confirm.

To remove a secondary interface

1. On the **Networking** tab for a server or pool, under **IP Address Configuration**, select **Configure**.
2. From the list of configured interfaces, select the one you want to remove and then click **Remove IP Address**.
3. Click **OK** to save your configuration choices.

To change the management interface

1. On the **Networking** tab for a server or pool, under **IP Address Configuration**, select **Configure**.
2. On the **Management Interface** tab, choose your network from the **Network** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> The tagged VLAN networks are also displayed in this Network list.

3. Configure the networking settings for the management interface:
   - To use automated DHCP to assign network settings automatically, including the IP address, subnet mask, gateway and DNS server, select **Automatically obtain settings using DHCP**.
   - To configure network settings manually, select **Use these settings** and enter the required values. You must enter an IP address and a subnet mask, but the gateway and DNS server settings are optional.
4. When you have finished, click **OK** to save your configuration choices.

> **NOTE:**
>
> If you choose to configure the network settings manually, you are prompted to confirm your settings. Click **Reconfigure anyway** to confirm.

Related documentation

XenServer Current Release

- Manage networking

Managing SSH and Console Sessions

Overview

In XenServer, SSH access to dom0 is enabled by default and can be toggled in xsconsole. Administrators can now manage SSH access directly through XenCenter at both the host and pool level.

New capabilities include:

- Viewing SSH access status at host and pool level
- Enabling or disabling SSH with optional timeouts
- Enabling auto mode for SSH, letting XAPI dynamically control SSH status

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configuring idle timeout for SSH and VNC console sessions

These features simplify administration and align XenCenter with security best practices.

Benefits

- Improved security – Limit open SSH and console sessions with timeouts.
- Operational efficiency – Manage SSH access without logging in to xsconsole or using the CLI.
- Reduced misuse risk – Automatically terminate idle sessions.
- Flexibility – Temporarily enable SSH for troubleshooting, with automatic expiry.

Enabling SSH Access

1. Select a pool or host.
2. On the top Pool/Server menu or right click the pool/host, click **SSH Access** -> **Enable...**.
3. On the **Enable SSH access** dialog, there're 2 options:
    - Enable SSH access
    - Enable SSH access for a limited amount of time

    > **NOTE:**
    >
    > The option enables SSH access only for the amount of time you specify and once this amount of time elapses SSH is disabled automatically.

Enabling SSH access on the pool will apply the same settings to all hosts within the pool.

After enabling the SSH access, the server's Console tab displays a **Launch SSH Console** button. If SSH is disabled, this button is hidden.

Disabling SSH Access

1. Select a pool or host.
2. On the top Pool/Server menu or right click the pool/host, click **SSH Access** -> **Disable**.
3. On the **Disable SSH access** dialog, select whether to enable auto-mode while disabling SSH. Enabling SSH auto-mode will allow the server to automatically start the SSH service in case of an emergency where the XenServer API cannot be reached.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bulk Operations

SSH access can be enabled or disabled for multiple pools or multiple hosts at once. If selections have inconsistent statuses, both enable and disable options remain available on the menu.

View Server Properties

The **General** tab for a server has the following sections and information:

General

The **General** section of the **General** tab shows the following information:

- **Name**: The name you gave the host.
- **Description**: The description you gave the host.
- **Tags**: Any tags you assigned to the host.
- **Folder**: Any folders you assigned to the host.
- **Pool coordinator**: Whether the host is the pool coordinator.
- **Status**: Whether the host is enabled or in maintenance mode.
- **Secure Boot**: Whether or not Secure Boot is enabled on the host.
- **System manufacturer**: The manufacturer of the server hardware.
- **System model**: The model of the server hardware.
- **Certificate verification**: Whether certificate verification is enabled.
- **iSCSI IQN**: The unique name that identifies the host to the iSCSI network.
- **Log destination**: Whether logs are saved locally or in a remote location.
- **Server uptime**: How long since the server last started.
- **Toolstack uptime**: How long since the toolstack last started
- **Domain**: The Active Directory domain that this host is a member of.
- **UUID**: The unique identifier of this host.

Certificates

The **Certificates** section of the **General** tab shows the following information:

- **Server identity certificate**: The validity dates and thumbprint of the certificate used to verify the identity of a XenServer® host to any client applications that communicate with the pool on the management network.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Server internal identity certificate**: The validity dates and thumbprint of the certificate used to secure communications between hosts within the pool.

License Details

The **License Details** section of the **General** tab shows the following information:

- **Status**: Whether the server is licensed.
- **Expiry date**: When the license expires.
- **License**: The type of license is applied to this host.
- **Number of sockets**: The number of sockets that this host is using.
- **Licesne Server Address**: The host name or IP address of the Citrix® License Server hosting the license.
- **License Server Port**: The port on which XenServer communicates with the Citrix License Server.

Version Details

The **Version Details** section of the **General** tab shows the following information:

- **Version**: The version of XenServer running on this server.
- **DBV**: The date-based version of the host.

Updates

The **Updates** section of the **General** tab shows the following information for XenServer hosts:

- **Last updated**: When updates were last applied to this host.
- **Checksum of latest applied updates**: The checksum for the level of updates applied to this host.
- **Pending recommended tasks**: Any actions that must be taken to get full effectiveness from all applied updates.

Management Interfaces

The **Management Interfaces** section of the **General** tab shows the following information:

- **DNS hostname**: The host name of this server.
- **Management interface**: The IP address of the management interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A list of secondary interfaces and their IP addresses.
- **TCP port 80**: Whether port 80 is open.

Memory

The **Memory** section of the **General** tab shows the following information:

- **Server**: How much memory is available on the server and the server total memory.
- **VMs**: How much memory is allocated to each VM on the host.
- **XenServer Host**: How much memory is allocated to dom0.

CPUs

The **CPUs** section of the **General** tab shows a list of the CPUs with their vendor, model, and speed, and the vCPU:CPU ratio.

GFS2 Clustering Status

If GFS2 clustering is enabled in the pool, the **General** tab has a **GFS2 Clustering Status** section that shows the following information:

- **Status**: Whether the host is a live or not live member of the cluster.
- **Last updated status**: When the host status was last updated.

SSH Access

The **SSH Access** section of the **General** tab shows the following information:

Status: the SSH access status of the host.

Changing Server Properties

Select any connected server in the **Resources** pane and select the **General** tab to see its properties and status. Click **Properties** to change the properties of a server.



General properties - Name, Description, Folder, and Tags

You can change the name, description, folder, and tags for a server on the **General Properties** tab of the **Properties** dialog.

- To change the server's name, enter a new name in the **Name** box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To change its description, enter new text in the **Description** box.
- To place the server in a folder or to move it to a different folder, select **Change** in the **Folder** box and select a folder. For more information, see Using folders.
- To tag and untag the server and to create and delete tags, see Using tags.



iSCSI IQN (General tab)

The server's iSCSI IQN is used to uniquely identify it when connecting to iSCSI storage repositories (SRs). XenServer hosts support a single iSCSI initiator which is automatically created and configured with a random IQN during host installation. The single initiator can be used to connect to multiple iSCSI targets (SRs) concurrently. For more detailed information about XenServer support for iSCSI storage, see Storage.

IMPORTANT:

You must set different IQNS for the iSCSI target (SR) and all servers in the pool. If a non-unique IQN identifier is used, data corruption can occur or access to the target might be denied.

To change the iSCSI IQN value for a managed server

NOTE:

Before you change a server's iSCSI IQN value, all existing SRs must be detached. Changing the server IQN might make it impossible for the server to connect to new or existing SRs unless the storage target is updated appropriately.

1. Select the server in the **Resources** pane, select the **General** tab, and then click **Properties**.
2. On the **General** tab in the **Properties** dialog box, enter the new value in the **iSCSI IQN** box.
3. Click **OK** to save your changes and close the dialog box.



Custom Fields

Custom fields allow you to add information to managed resources to make it easier to search and organize them. For more information, see Using custom fields.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Alerts

Use this tab to configure performance alerts for the server's CPU, memory usage, and network activity. For more information, see Configuring performance alerts.



Email Notifications (standalone servers)

Use this tab to configure the email notification for system alerts generated on a standalone server. This feature is configured at pool level for servers in a pool. For more information, see XenCenter Alerts.



Multipathing

Dynamic storage multipathing support is available for Fibre Channel and iSCSI storage repositories. This feature can be enabled through the **Multipathing** tab on the server's **Properties** dialog.

For more information, see Storage Multipathing.



Power on (standalone servers)

Use this tab to configure your XenServer Host Power On feature, allowing managed servers to be powered on remotely. For more information about configuring this feature, see Configuring Host Power On. For servers in a pool, this feature is configured at pool level.



Drivers

This tab allows you to view and change driver variants installed on your server. It shows which variants are currently active and which variants will be active after the next reboot.

The list displays any drivers on the server that have multiple variants and apply to the current hardware. In the **Active after next reboot** column, choose a different variant if needed. The new variant becomes active after you reboot the server.

Select **Show single variant drivers** to include drivers that have only one variant.

Select **Show drivers not applicable to current hardware** to include drivers that are not applicable to the server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Log Destination

XenServer® system log messages are stored locally on the server itself. You can also choose to forward these logs to a remote server.

The remote server must be running a syslogd daemon to receive the logs and aggregate them correctly. The syslogd daemon is a standard part of all Linux and Unix installations. Third-party versions are available for Windows and other operating systems. Configure the remote server to allow remote connections from the hosts in the pool, and have its firewall configured appropriately.

To specify a remote XenServer log destination

1. Select the server in the **Resources** pane, select the **General** tab, and click **Properties**.
2. Select the **Log Destination** tab in the **Properties** dialog box.
3. Select **Also store the system logs on a remote server**.
4. In the **Server** field, enter an IP address or the host name of a server running the syslogd daemon. A port can be specified by appending `:<port>`, otherwise it will default to port 514.
5. Click **OK** to save your changes and close the dialog box.



GPU

The **GPU** tab allows you to:

1. Set a GPU placement policy
2. Enable Intel GPU pass-through for Windows VMs

Placement Policy

The **GPU** tab allows you to set a host-wide policy to assign VMs to available GPUs to achieve either maximum density or maximum performance. Select an option based on your requirements.

The **GPU** tab displays **Mixed** setting only when different settings are used for different GPU groups. For a **Mixed** setting, certain GPU groups are configured to achieve maximum density, and the rest are configured to achieve maximum performance.

It is **not** possible to set or edit the **Mixed** setting using XenCenter. Use the xe CLI if you want to use different settings for different GPU groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

GPU Virtualization is available for XenServer Premium Edition customers. The **GPU** tab is visible when the server meets the license requirements and has GPUs that support various virtual GPU types. For more information, see About XenServer Licensing.

Integrated GPU pass-through

When your XenServer server is connected to an Intel GPU on an Intel server, the control domain of the server is connected to the integrated GPU device. In such cases, the GPU is not available for pass-through. Select **This server will not use the Integrated GPU** to disable the connection between dom0 and the GPU and reboot the host for the changes to take effect.

For more information, see GPU.

NOTE:

The XenServer server's external console output (for example, VGA, HDMI, DP) is not available after disabling the connection between dom0 and the GPU.



NRPE

NOTE:

The NRPE feature is available for XenServer Premium or Trial Edition customers. For more information about XenServer licensing, see Licensing. To upgrade, or to get a XenServer license, visit the XenServer website.

This tab allows you to configure the NRPE service for a standalone host that is not part of a pool.

Users with the Pool Admin role can use any third-party monitoring tool that supports the Nagios Remote Plugin Executor (NRPE) to monitor resources consumed by your XenServer host and dom0 - the control domain of your host. For information about the host and dom0 metrics that you can capture by using NRPE, see Monitor host and dom0 resources with NRPE.

Select the **Enable NRPE** check box to enable NRPE for your standalone host. To add more monitoring servers that are allowed to talk to the NRPE daemon, specify the hosts as a comma-delimited list of IP addresses or host names. You can also adjust the warning and critical

© 1997–2026 Citrix Systems, Inc. All rights reserved.

thresholds of the plugin checks by modifying the values in the warning and critical thresholds table. For more information on how to configure the NRPE service, see Monitoring host and dom0 resources with NRPE.

NOTE:

The NRPE tab is only available to users with the Pool Admin role.



SNMP

NOTE:

The SNMP feature is available for XenServer Premium or Trial Edition customers. For more information about XenServer licensing, see Licensing. To upgrade, or to get a XenServer license, visit the XenServer website.

This tab allows you to configure the SNMP service for a standalone host that is not part of a pool.

With the Pool Admin role, you can use SNMP to remotely monitor resources consumed by your XenServer host and dom0 - the control domain of your host.

Select the **Enable SNMP** check box to enable SNMP for your standalone host. You can add one trap receiver by clicking **Add Trap Receiver**. For more information on how to configure the SNMP service, see Monitoring host and dom0 resources with SNMP.

NOTE:

The SNMP tab is only available to users with the Pool Admin role.

If you cannot see the **SNMP** tab in XenCenter, it might be because the host is not running a version of XenServer that supports SNMP. Update the host to the latest version of XenServer.

Console

Servers in pools

This tab allows you to configure SSH and VNC console idle timeout parameters.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Click the **Enable idle timeout for server SSH and VNC console sessions**, and enter a value (minutes).
  - 0 = sessions never expire
  - Non-zero value (for example, 60) = terminate idle sessions after specified minutes.

> **NOTE:**
>
> When the idle timeout is reached, the console session will automatically disconnect.

Standalone servers

This tab allows you to configure SSH and VNC console idle timeout parameters (including VM VNC sessions) and allows a single concurrent VNC console session for the server or per VM.

- Click the **Enable idle timeout for server SSH and VNC console sessions**, and enter a value (minutes).
  - 0 = sessions never expire
  - Non-zero value (for example, 60) = terminate idle sessions after specified minutes.
- Click the **Enable idle timeout for VM VNC console sessions**, and enter a value (minutes).
  - 0 = sessions never expire
  - Non-zero value (for example, 60) = terminate idle sessions after specified minutes

> **NOTE:**
>
> When the idle timeout is reached, the console session will automatically disconnect.

- Limit concurrent VNC console sessions to 1.

> **NOTE:**
>
> When XenCenter tries to connect to a VNC console session and the console session is limited and someone is occupying the console session, a dialog to inform the user is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Changing the Control Domain Memory

The control domain, also known as 'dom0', is a secure, privileged Linux Virtual Machine (VM) that runs the XenServer® management toolstack (XAPI). The control domain provides the XenServer management function. It also runs the driver stack that provides user-created VMs access to physical devices.

The amount of memory allocated to the control domain is set automatically during XenServer installation. The amount is based on the amount of physical memory on the server. For more information, see Memory usage.

You might want to increase the memory that is allocated to dom0 in the following cases: Storage Read Caching scenarios, PVS-Accelerator scenarios, or when running more than 50 VMs per XenServer server. On servers with a smaller amount of memory, you might want to reduce the memory that is allocated to dom0. The following section provides instructions to update the dom0 memory using XenCenter. For information about changing the dom0 memory using the xe CLI, see Command line interface.

NOTE:

- Citrix® recommends that you do not reduce the dom0 memory below 1 GiB.
- Increasing the amount of dom0 memory causes less memory being available to VMs.
- Customers cannot use XenCenter® to reduce dom0 memory below the value that was initially set during XenServer installation.

To update the dom0 memory

NOTE:

Place the server in Maintenance mode before updating the dom0 memory. For more information, see Run in maintenance mode.

1. Select the server in the **Resources** pane and click **Memory**. The **Memory** tab displays information about the memory currently used by the server. This information includes available memory, dom0 memory, total memory, and the percentage of the total memory used by the server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click the hyperlink displayed next to **Control domain memory**. Alternatively, from the **Server** menu, select **Control Domain Memory**.
3. Update the memory allocated to dom0 on the **Control Domain Memory Settings** dialog. Any change to the dom0 memory causes the server to reboot.
4. Click **OK** to confirm the changes and reboot the server.

Related documentation

XenServer Current Release

- Memory usage

Exporting and Importing a List of Managed Servers

You can export your list of managed servers from XenCenter® to a configuration file. You can import this configuration file into a XenCenter session on another computer. This feature can be useful, for example, to copy your list of managed servers from your desktop computer to a laptop. You can avoid having to manually adding a long list of servers on the new machine.

XenCenter saves the IP address or DNS name, port, and display name of each managed VM in XML format in a file with a `.config` file name extension. Your login credentials are not stored.

To export your list of managed servers

1. On the **File** menu, select **Export Server List**.
2. Specify the name and location of the export file and then click **Save**.

To import a list of servers

1. On the **File** menu, select **Import Server List**.
2. Locate the XenCenter configuration file and then click **Open**.

   The servers appear in the XenCenter **Resources** pane with a disconnected status 
   .
3. Double-click on each imported server in the **Resources** pane to connect to it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Managing Pools

XenServer pools allow you to view multiple servers and their connected shared storage as a single unified resource. Use this view to deploy VMs based on their resource needs and business priorities. A pool can contain up to 64 servers running the same version of XenServer software, at the same patch level, and with broadly compatible hardware. For more information, see Pool Requirements.

One server in the pool is designated as the pool coordinator. The pool coordinator provides a single point of contact for all servers in the pool, routing communication to other members of the pool as necessary.

If the pool coordinator shuts down, the pool is unavailable until the pool coordinator is back online or until you nominate another pool member as the new pool coordinator. Every member of a resource pool contains all the information necessary to take over the role of pool coordinator, if necessary. On an HA-enabled pool, a new pool coordinator is automatically nominated if the pool coordinator is shut down.

Related documentation

XenServer Current Release

- Hosts and resource pools

Pool Requirements

A resource pool is a homogeneous or heterogeneous aggregate of one or more servers, up to a maximum of 64. Before you create a pool or join a server to an existing pool, ensure the following requirements are satisfied for all servers in the pool.

Hardware requirements

All servers in XenServer® resource pools must have broadly compatible CPUs, that is:

- The CPU vendor (Intel, AMD) must be the same on all CPUs on all servers.
- All CPUs must have virtualization enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Other requirements

In addition to the hardware prerequisites, there are several other prerequisites for a server that joins a pool:

- It must have a consistent IP address (a static IP address on the server or a static DHCP lease). This requirement also applies to the servers providing shared NFS or iSCSI storage.
- Its system clock must be synchronized to the pool coordinator (for example, via NTP).
- It must be in either the same data center as the pool, or in a data center meeting the close-proximity definition, and connected by a low-latency (less than 5ms round-trip time), high-bandwidth (at least 10Gbps) network.
- It cannot be a member of an existing resource pool.
- It cannot have any running or suspended VMs or any active operations in progress on its VMs. All VMs must be shut down before a server can join a pool.
- It cannot have any shared storage already configured.
- It cannot have a bonded management interface. Reconfigure the joining server's management interface and move it back on to a physical NIC before joining the pool. After the server has successfully joined the pool, you can reconfigure it. For more information, see Configuring IP Addresses.
- It must be running the same version of XenServer software, at the same update level, as the servers already in the pool. If this is not the case, XenCenter® attempts to synchronize the joining server with the pool cooordinator and apply a matching set of updates.
- It must be configured with the same supplemental packs as the servers already in the pool. Supplemental packs are used to install add-on software into dom0 (XenServer control domain). To prevent inconsistencies in the user experience across a pool, ensure you install the same supplemental packs at the same revision on all the servers in the pool.
- It must have the same XenServer license as the servers already in the pool. You can change the license of any pool members after joining the pool. The server with the lowest license determines the features available to all members in the pool. For more information about licensing, see About XenServer Licensing.

Homogeneous pool

A homogeneous resource pool is an aggregate of servers with identical CPUs. In addition to the requirements in the preceding sections, a server that joins a homogeneous pool must have the same CPUs as those servers already in the pool. CPUs are considered the same if they have the same vendor, model, and features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Heterogeneous pool

XenServer enables expanding deployments over time by allowing disparate host hardware to be joined into a resource pool, known as heterogeneous resource pools. Heterogeneous resource pools are made possible by applying technologies in Intel (FlexMigration) and AMD (Extended Migration) CPUs that provide CPU "masking" or "leveling". These features allow a CPU to be configured to appear as providing a different make, model, or functionality than it actually does. This capability enables you to create pools of hosts with disparate CPUs but still safely support live migrations. Servers joining heterogeneous pools must meet the following requirements:

- The CPUs of the server that joins the pool must be of the same vendor (AMD, Intel) as the CPUs on servers already in the pool. However, the specific type of CPU (family, model, and stepping numbers) is note required to be the same.
- The CPUs of the server joining the pool must support either Intel FlexMigration or AMD Enhanced Migration.

XenServer simplifies the support for heterogeneous pools. You can add servers to existing resource pools, irrespective of the underlying CPU type, as long as the CPU is from the same vendor family. The pool feature set is dynamically calculated every time:

- a new server joins the pool
- a pool member leaves the pool
- a pool member reconnects following a reboot

Any change in the pool feature set does not affect VMs that are currently running in the pool. A running VM continues to use the feature set which was applied when it was started. This feature set is fixed at boot and persists across migrate, suspend, and resume operations. If the pool level drops when a less-capable server joins the pool, a running VM can migrate to any server in the pool, except the newly added server. When you move or migrate a VM to a different server within or across pools, XenServer compares the VM feature set to that of the destination server. If the feature sets are found to be compatible, the VM is allowed to migrate. This capability enables the VM to move freely within and across pools, regardless of the CPU features the VM is using. If you use Workload Balancing to choose an optimal destination server to migrate your VM, a server with an incompatible feature set is not recommended as the destination server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

To update a running VM to use the pool's new feature set, power off the VM and start it again. Rebooting the VM, for example, by clicking **Reboot** in XenCenter, does not cause the VM to update its feature set.

Shared pool storage

Although not a strict requirement for creating a resource pool, the advantages of pools are only available if the pool has one or more shared storage repositories (SRs). These advantages include running a VM on the most appropriate server and VM migration between servers.

We recommend that you do not attempt to create a pool until shared storage is available. After you add shared storage, you can quickly move any existing VMs whose disks are in local storage into shared storage by copying them.

When a server with a shared SR becomes a pool coordinator, this SR becomes a shared SR for the pool. If the new pool coordinator does not have any shared storage, you have to create a new shared SR for the pool: see Creating a New SR.

Related documentation

XenServer Current Release

- Hosts and resource pools

Create a New Pool

When you create a pool, XenCenter® attempts to resolve any pool configuration issues before creating the pool.

There might be other hardware or configuration issues that prevent a server from successfully joining a pool. For more information, see Pool requirements.

To create a pool

1. Open the **New Pool** wizard by clicking **New Pool** on the Toolbar.
2. Enter a name for the new pool and an optional description. The name is displayed in the **Resources** pane. Click **Next**.
3. Nominate the pool coordinator by selecting a server from the **Coordinator** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select more servers to place in the new pool from the **Additional members** list. All available managed servers are listed. If a server is not listed, you can add it to the list by clicking **Add New Server**. If a managed server does not satisfy one or more of the pool join requirements listed in Pool requirements, it appears disabled.

   Click **Next**.

5. On the **Pre-checks** panel, XenCenter identifies any pool configuration issues that might need to be resolved:

   - The supporting servers must be licensed at the same level as the pool coordinator.
     - If the supporting server does not have a license and the pool coordinator has licenses available on the connected License Server, XenCenter automatically applies the appropriate license.
     - If the supporting server has a different license to the pool coordinator, this server shows as disabled in the **Additional members** list. You cannot add the server to the pool.

     You can change the license of any pool members after joining the pool. The server with the lowest license determines the features available to all members in the pool. For more information about licensing, see About XenServer Licensing.
   - The supporting servers must be part of the same Active Directory domain as the pool coordinator.
     - If the pool coordinator is joined to a domain and the supporting server is not joined to a domain, XenCenter automatically joins the supporting server to the same domain.

       At the **Create Pool** step, you are prompted for credentials on the supporting server. Enter your AD credentials for the domain to which the pool is joined. These credentials must have sufficient privileges to add servers to the domain.
     - If the pool coordinator is joined to a domain and the supporting server is joined to a different domain, this server shows as disabled in the **Additional members** list. You cannot add the server to the pool.
   - The supporting server must be at the same level of updates as the pool coordinator. If the supporting server is at an earlier level of updates than the pool, XenCenter synchronizes it with the pool coordinator and applies updates from the pool coordinator to the supporting host.

   Click **Next** to attempt to resolve these pre-checks and create the pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. On the **Create Pool** panel, XenCenter resolves the pool configuration issues, creates the pool, and displays the results. Click **Finish** to close the wizard.

If the pool coordinator already has a shared storage repository (SR), this repository becomes a shared SR for the pool. If the new pool coordinator does not have any shared storage, you have to create a new shared SR for the pool. For more information, see Creating a New SR.

More pool configuration steps

To configure the new pool, use the property tabs:

1. To add shared storage to the pool, see Creating a New SR.
2. To add more servers to the pool, see Add a Server to a Pool.

Related documentation

XenServer Current Release

- Hosts and resource pools

Add a Server to a Pool

Before you add any new servers to a resource pool, ensure that the hardware and configuration requirements identified in Pool requirements are satisfied for the joining servers.

IMPORTANT:

Back up any virtual machines hosted on a server before attempting to add it to a pool.

To add a server to an existing pool

1. Select the server in the **Resources** pane, then do one of the following:

   - Drag the selected server onto the target pool in the **Resources** pane.
   - On the **Server** menu, select **Add to Pool** and then select the target pool.
   - Right-click and select **Add to Pool** on the shortcut menu. Select the target pool.

   The **Add to Pool** wizard opens.

2. On the **Pre-checks** panel, XenCenter® identifies any pool configuration issues that might need to be resolved:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The supporting servers must be licensed at the same level as the pool coordinator.
  - If the supporting server does not have a license and the pool coordinator has licenses available on the connected License Server, XenCenter automatically applies the appropriate license.
  - If the supporting server has a different license to the pool coordinator, an error is shown. You cannot add the server to the pool.

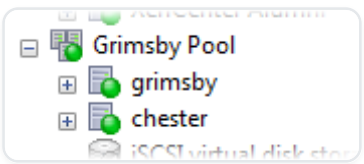
  You can change the license of any pool members after joining the pool. The server with the lowest license determines the features available to all members in the pool. For more information about licensing, see About XenServer Licensing.
- The supporting servers must be part of the same Active Directory domain as the pool coordinator.
  - If the pool coordinator is joined to a domain and the supporting server is not joined to a domain, XenCenter automatically joins the supporting server to the same domain.

    At the **Add to Pool** step, you are prompted for credentials on the supporting server. Enter your AD credentials for the domain to which the pool is joined. These credentials must have sufficient privileges to add servers to the domain.
  - If the pool coordinator is joined to a domain and the supporting server is joined to a different domain, an error is shown. You cannot add the server to the pool.
- The supporting server must be at the same level of updates as the pool coordinator. If the supporting server is at an earlier level of updates than the pool, XenCenter synchronizes it with the pool coordinator and applies updates from the pool coordinator to the supporting host.

Click **Next** to attempt to resolve these pre-checks and add the server to the pool.

3. On the **Add to Pool** panel, XenCenter resolves the configuration issues, adds the server to the pool, and displays the results. Click **Finish** to close the wizard.

Once you have placed a server in a pool, it is shown as a pool member in the **Resources** pane, for example:



When a new server joins a pool, that server automatically inherits the pool coordinator's networking configuration, including network and bond information. However, the joining server's management

© 1997–2026 Citrix Systems, Inc. All rights reserved.

interface does not change to match the pool coordinator. Reconfigure it after joining to use the same bond as the pool coordinator. For more information, see To change the management interface.

To place a server in a new pool

You place a managed server in a new pool using the **New Pool** wizard. The server becomes the pool coordinator in the new pool.

1. In the **Resources** pane, select the server.
2. Right-click and, on the shortcut menu, select **Add to Pool** and then **New Pool**.
3. Create the pool using the **New Pool** wizard. For more information, see Create a new pool.

Related documentation

XenServer Current Release

- Hosts and resource pools

Remove a Server From a Pool

1. Move any data stored on local disks to a shared storage repository in the same resource pool. For more information, see Move virtual disks.

   IMPORTANT:

   When you remove a server from a resource pool, all VM data stored on local disks is erased. Ensure you complete this step to retain any important data.

2. Shut down any VMs running on the server. For more information, see Shut Down a VM.
3. In the **Resources** pane, select the server and do one of the following:

   - Right-click and select **Remove Server from Pool** in the **Resources** pane shortcut menu.
   - In the **Pool** menu, select **Remove Server**.

Related documentation

XenServer Current Release

- Remove XenServer hosts from a resource pool

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Destroy a server from a pool

Destroying a server from a resource pool forgets the specified XenServer® server without contacting it explicitly. It permanently removes the server from the pool along with its local SRs, DVD drives, and removable storage. Use this option to destroy a server that cannot be contacted or has physically failed. Also, you cannot undo the destroy server operation. Reinstall the server before it can be used again.

1. In the **Resources** pane, select the server and do one of the following:
   - Right-click and select **Destroy** in the **Resources** pane shortcut menu.
   - In the **Server** menu, select **Destroy**.
2. Click **Yes, Destroy** to confirm.

Export Resource Data

Export Resource Data enables you to generate a resource data report for your pool and export the report into an `.xls` or `.csv` file. This report provides detailed information about various resources in the pool such as:

- servers
- networks
- storage
- virtual machines
- VDIs
- GPUs

Use this feature to track, plan, and assign resources based on various workloads such as CPU, storage, and Network.

NOTE:

Export Resource Data is available for XenServer Premium Edition customers. To learn more about XenServer licensing, see About XenServer Licensing.

To export resource data:

1. In the XenCenter® **Navigation** pane, select **Infrastructure** and then click the pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. From the XenCenter menu, select **Pool** and then select **Export Resource Data**.
3. Browse to a location where you would like to save report and then click **Save**.

Resource Data

The section lists the resources and various types of resource data included in the report.

Server

- Name
- Pool coordinator
- UUID
- Address
- CPU Usage
- Network (avg/max KBs)
- Used Memory
- Storage
- Uptime
- Description

Networks

- Name
- Link Status
- MAC
- MTU
- VLAN
- Type
- Location

VDI

- Name
- Type
- UUID
- Size

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Storage
- Description

Storage

- Name
- Type
- UUID
- Size
- Location
- Description

VMs

- Name
- Power State
- Running on
- Address
- MAC
- NIC
- Operating System
- Storage
- Used Memory
- CPU Usage
- UUID
- Uptime
- Template
- Description

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GPU

> **NOTE:**
>
> Information about GPUs is available only if there are GPUs attached to your XenServer® host.

- Name
- Servers
- PCI Bus Path
- UUID
- Power Usage
- Temperature
- Used Memory
- Computer Utilization

View Pool Properties

The **General** tab for a pool has the following sections and information:

General

The **General** section of the **General** tab shows the following information:

- **Name**: The name you gave the pool.
- **Description**: The description you gave the pool.
- **Tags**: Any tags you assigned to the pool.
- **Folder**: Any folders you assigned to the pool.
- **Pool License**: The type of license is applied to this pool.
- **Number of Sockets**: The number of license sockets used by this pool.
- **Certificate verification**: Whether certificate verification is enabled.
- **Version**: The version of XenServer® running on this pool.
- **UUID**: The unique identifier of this pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Certificates

The **Certificates** section of the **General** tab shows the following information:

- A list of CA certificateas installed in the pool and their type, validity dates, and thumbprint.

Updates

The **Updates** section of the **General** tab shows the following information:

- **Update channel**: The update channel that the pool is configured to receive updates from.
- **Last synchronized**: The last time the pool synchronized with the update channel and checked for new updates.
- **Synchronization checksum**: The checksum of the level of updates available from the update channel.
- **Checksum of latest applied updates**: The checksum of the level of updates applied to the pool.
- **Pending recommended tasks**: Any actions that must be taken on hosts in the pool to get full effectiveness from all applied updates.

Management Interfaces

For each host in the pool, the **Management Interfaces** section of the **General** tab shows the following information:

- **DNS hostname**: The host name of this server.
- **Management interface**: The IP address of the management interface.
- **TCP port 80**: Whether port 80 is open.
- A list of secondary interfaces and their IP addresses.

GFS2 Clustering Status

If GFS2 clustering is enabled in the pool, the **General** tab has a **GFS2 Clustering Status** section that shows the following information:

- **Number of live hosts**: How many of the hosts in the cluster are online and connected to the other hosts in the cluster.
- **Unreachable hosts**: A list of any hosts in the cluster that are not live. These hosts might be offline or fenced or online but unable to contact the cluster.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Corosync Version**: Displays the current Corosync version. If the XenServer is up to date, you will see an Upgrade GFS2 Cluster link. Click the link to launch the **Corosync Upgrade** wizard.
- **Quorum**: The number of live hosts required for the cluster to have quorum. For more information about how the quorum value is calculated, see GFS2 clustered pools.
- **GFS2 Cluster is quorate**: Whether the cluster has quorum.

SSH Access

The **SSH Access** section of the **General** tab shows the following information:

- The SSH access status of each host in this pool.

Change Pool Properties

Select any resource pool in the **Resources** pane and select the **General** tab to see its properties and status. Click **Properties** on the **General** tab to change the properties of a pool.



General properties - name, description, folder, tags

On the **General Properties** tab you can change the pool's name and description, place it in a folder, and manage its tags.

- To change the pool name, enter a new name in the **Name** box.
- To change its description, enter new text in the **Description** box.
- To add the pool to a folder or to move it to a different folder, select **Change** in the **Folder** box. Choose a folder. For more information, see Using folders.
- To tag and untag the pool and to create and delete tags, see Using tags.



Custom fields

Custom fields allow you to add information to managed resources to make it easier to search and organize them. See Using custom fields to find out how to assign custom fields to your managed resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Email options

Use this tab to configure the email notification for system alerts that are generated on any servers or VMs in the pool. For more information, see XenCenter Alerts. Users who want to receive performance alert emails can choose the preferred language from the list. The languages available are English, Chinese, and Japanese.

The default language for configuring performance alert email language for XenCenter is English.



Power on

The Power On feature allows you to configure power management preferences for servers that support power management. Servers can be powered off and on automatically depending on the pool's total workload (through Workload Balancing).

- In the list of servers at the top of the tab, select the servers for which you want to configure power management.
- Under **Power On mode**, specify the **Power On** settings (Disabled, Wake-on-LAN, IPMI or custom script) for the selected servers. The available power on settings depend on the version of your hosts.
- Under **Configuration options**, specify either the IP address and credentials or key-value pairs for a host power-on script. The options you must specify depend on the **Power On mode** option you chose.

For more information about prerequisites and configuration options for the Host Power On feature, see Configuring Host Power On.



Drivers

This tab allows you to view and change driver variants installed on all servers in the pool. It shows which variants are currently active and which variants will be active after the next reboot.

The top list shows all servers in the pool. When you select one or more servers, the bottom list shows any drivers on these servers that have multiple variants and apply to the current hardware. In the **Active after next reboot** column, choose a different variant if needed. The new variant becomes active after you reboot the servers.

Select **Show single variant drivers** to include drivers that have only one variant.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Select **Show drivers not applicable to current hardware** to include drivers that are not applicable to the servers.



GPU

This tab allows you to set a pool-wide policy to assign VMs to available GPUs to achieve either maximum density or maximum performance. Select an option based on your requirements.

The **GPU** tab displays **Mixed** setting only when different settings are used for different GPU groups. That is, when you configure certain GPU groups within a pool for maximum density, and configure the other GPU groups for maximum performance. It is **not** possible to set or edit the **Mixed** setting using XenCenter. To use different settings for different GPU groups, use the xe CLI.

NOTE:

GPU Virtualization is available for XenServer Premium Edition customers. XenCenter displays the **GPU** tab when the pool meets the license requirements and also has GPUs that support various virtual GPU types. For more information, see About XenServer Licensing.



Security

The **Security** tab enables you to specify whether TCP port 80 is open or closed for the management interface of the pool. We recommend that this port is closed.

For communication with the pool, only the TLS 1.2 protocol is supported.

For a list of cipher suites used for TLS 1.2 communication with your pool, see the information for your pool version:

- XenServer Current Release



Live patching

This tab allows you to enable or disable live patching. Live patching enables customers to install some Linux kernel and Xen® hypervisor updates without having to reboot the hosts. It is enabled by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

XenServer Live Patching is available for XenServer Premium Edition customers. For more information about licensing, see About XenServer Licensing.



Network

This tab allows you to enable or disable IGMP snooping. XenServer® sends multicast traffic to all guest VMs. This behavior leads to unnecessary load on host devices by requiring them to process packets they have not solicited. If you enable IGMP snooping, it prevents hosts on a local network from receiving traffic for a multicast group that they have not explicitly joined. This action improves the performance of multicast. IGMP snooping is especially useful for bandwidth-intensive IP multicast applications such as IPTV. This option is disabled by default.

NOTE:

- IGMP snooping is available only when the network back-end uses Open vSwitch.
- When enabling this feature on a pool, it might also be necessary to enable IGMP querier on one of the physical switches. Or else, multicast in the sub network falls back to broadcast and can decrease XenServer performance.
- When enabling this feature on a pool running IGMP v3, VM migration or network bond failover results in IGMP version switching to v2.
- XenServer IGMP snooping is available for XenServer Premium Edition customers. For more information about licensing, see About XenServer Licensing.



GFS2 Clustering

This tab allows you to enable or disable GFS2 clustering. Enable clustering on a pool to use thin-provisioned storage repositories with GFS2.

NOTE:

We recommend that you enable clustering only on pools that contain three or more servers and a GFS2 SR.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Do not enable clustering on pools that don't include a GFS2 SR.
When enabling this feature on a pool, specify a network. The clustering mechanism uses this network to communicate with all servers in the pool. If a server cannot communicate with most other servers in the clustered pool, after a timeout that server self-fences. To decrease the chance of a host self-fencing unnecessarily, ensure the network you use for clustering is reliable. We recommend that you use a physically separate bonded network. For more information, see Add a new network.

You can now upgrade your GFS2 cluster to Corosync version 3 if you are still using Corosync version 2.



Global VM Options

This tab allows you to configure options that apply to all VMs in a pool.

Performance enhancements

During the live migration of a VM, its memory is transferred as a data stream between two hosts using the network. You can compress this data stream and speed up the memory transfer on slow networks by enabling the migration stream compression feature. To enable the migration stream compression feature, select the **Compress VM memory and vGPU data during VM live migration** checkbox. This feature is disabled by default.

Automatic Secure Boot certificate updates

If the VMs created in your pool contain legacy Secure Boot certificates, you can select this option to automatically flag them to have their certificates updated on the next boot. This feature is disabled by default.



NRPE

NOTE:

The NRPE feature is available for XenServer Premium or Trial Edition customers. For more information about XenServer licensing, see Licensing. To upgrade, or to get a XenServer license, visit the XenServer website.

This tab allows you to configure the NRPE service for a pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **NRPE** tab displays the default NRPE configuration values for your pool. Users with the Pool Admin role can use any third-party monitoring tool that supports the Nagios Remote Plugin Executor (NRPE) to monitor resources consumed by your XenServer host and dom0 - the control domain of your host. For information about the host and dom0 metrics that you can capture by using NRPE, see Monitor host and dom0 resources with NRPE.

Select the **Enable NRPE** check box to enable NRPE for your pool. To add more monitoring servers that are allowed to talk to the NRPE daemon, specify the hosts as a comma-delimited list of IP addresses or host names. You can also adjust the warning and critical thresholds of the plugin checks by modifying the values in the warning and critical thresholds table. For more information on how to configure the NRPE service, see Monitoring host and dom0 resources with NRPE.

NOTE:

The NRPE tab is only available to users with the Pool Admin role.



SNMP

NOTE:

The SNMP feature is available for XenServer Premium or Trial Edition customers. For more information about XenServer licensing, see Licensing. To upgrade, or to get a XenServer license, visit the XenServer website.

This tab allows you to configure the SNMP service for a pool.

The **SNMP** tab displays the default SNMP configuration values for your pool. With the Pool Admin role, you can use SNMP to remotely monitor resources consumed by your XenServer host and dom0 - the control domain of your host.

Select the **Enable SNMP** check box to enable SNMP for your standalone host. You can add one trap receiver by clicking **Add Trap Receiver**. For more information on how to configure the SNMP service, see Monitoring host and dom0 resources with SNMP.

NOTE:

The SNMP tab is only available to users with the Pool Admin role.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you cannot see the **SNMP** tab in XenCenter, it might be because a member of the pool is not running a version of XenServer that supports SNMP. Update all members in the pool to the latest version of XenServer.

Console

This tab allows you to configure idle timeout for SSH and VNC console sessions, idle timeout for VM VNC console sessions, and whether to allow only 1 VNC console session per server or VM. Configuring these at the pool level will apply the settings to all hosts within the pool.

- Click the **Enable console idle timeout for server SSH and VNC console sessions**, and enter a value (minutes).
  - 0 = sessions never expire
  - Non-zero value (for example, 60) = terminate idle sessions after specified minutes
- Click the **Enable idle timeout for VM VNC console sessions**, and enter a value (minutes).
  - 0 = sessions never expire
  - Non-zero value (for example, 60) = terminate idle sessions after specified minutes

  NOTE:

  When the idle timeout is reached, the console session will automatically disconnect.
- Allow only 1 VNC console session per server or VM at a time.

  NOTE:

  When XenCenter tries to connect to a VNC console session and the console session is limited and someone is occupying the console session, a dialog to inform the user is displayed.

Pool security

Change the root password

You can change the root password for a pool – that is, for all servers in a pool – by completing the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In the **Resources** pane, select the pool or any server in the pool
2. On the **Pool** menu, select **Change Root Password**

If XenCenter is configured to save your server login credentials between sessions, the new password is remembered. For more information, see Store your server connection state.

When you change the root password you are also advised to rotate the pool secret.

Rotate the pool secret

The pool secret is a secret shared among the servers in a pool that enables the server to prove its membership to a pool. Users with the Pool Admin role can view this secret when connecting to the server over SSH. Rotate the pool secret if one of these users leaves your organization or loses their Pool Admin role.

You can rotate the pool secret for a pool, by completing the following steps:

1. In the **Resources** pane, select the pool or any server in the pool
2. On the **Pool** menu, select **Rotate Pool Secret**

When you rotate the pool secret you are also prompted to change the root password.

Related documentation

XenServer Current Release

- Hosts and resource pools

Delete a Pool

A resource pool containing only one managed server can be deleted, effectively turning that server into a standalone server.

To delete a pool, select the pool in the **Resources** pane and from the **Pool** menu, select **make into standalone server**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Managing Storage

XenServer storage repositories (SR) are storage containers on which virtual disks are stored. Both storage repositories and virtual disks are persistent, on-disk objects that exist independently of XenServer. SRs can be shared between servers in a resource pool and can exist on different types of physical storage device, both internal and external. These devices include local disk devices and shared network storage. Various different types of storage are available when you create a storage repository using the **New Storage Repository** wizard. Depending on the type of storage selected, several advanced storage features can be configured in XenCenter. These features include:

- **Dynamic multipathing**. On Fibre Channel and iSCSI SRs, you can configure storage multipathing using round robin mode load balancing. For more information, see Storage Multipathing.
- **Thin provisioning**. On NetApp and Dell EqualLogic SRs, you can choose the type of space management used.

  By default, allocated space is thickly provisioned and all virtual allocation guarantees are fully enforced on the filer. This behavior guarantees that virtual disks never run out of space and therefore experience failed writes to disk.

  Thin provisioning allows the disks to be better utilized, as physical capacity is allocated only as a VM needs it - when it writes. This behavior allows for over provisioning of the available storage and maximum utilization of your storage assets.
- **Reclaiming Freed Space**. On a thinly provisioned block-based SR, you can free up unused space (for example, deleted VDIs in a LUN). The storage repository can then reuse the reclaimed space. For more information, see Reclaiming Freed Space.
- **Live LUN Expansion**. Live LUN Expansion enables you to increase the size of the LUN without any VM downtime. For more information, see Live LUN Expansion.

When you configure a server or pool, you nominate a default SR which is used to store crash dump data and images of suspended VMs. This SR is the default SR used for new virtual disks. At pool level, the default SR must be a shared SR. Any new virtual disks, crash dump files or suspended VM images created within the resource pool are stored in the pool's default SR. This behavior provides a mechanism to recover from physical server failure. For standalone servers, the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

default SR can be local or shared. When you add shared storage to a standalone server, the shared storage automatically becomes the default SR for that server.

It is possible to use different SRs for VMs, crash dump data and suspended VM using XenServer xe CLI. For more information, see Command line interface.

Related documentation

XenServer Current Release

- Storage

Creating a New SR

To create a storage repository, select **New Storage** on the toolbar.

Alternatively, do one of the following:

- On the **Storage** tab for the selected pool or server, click **New SR**.
- On the Storage menu, click **New SR**.

Select the physical storage type on the first page of the **New Storage Repository** wizard. Follow the steps in the wizard as it takes you through the configuration process for that storage type. The set of available settings in the wizard depends on the storage system vendor/model you select on the first page.

To create a thin-provisioned shared GFS2 SR on block storage, you can choose either an iSCSI or hardware HBA repository type. However, using thin-provisioned shared GFS2 block storage has additional requirements and constraints. Before using this type of SR, review Thin-provisioned shared GFS2 block storage.

SR creation steps

The **New Storage Repository** wizard takes you through the process of creating an SR:

1. On the **Type** page, you select the type of underlying storage:

    - NFS: In NFS VHD SRs, VM images are stored as thin-provisioned VHD format files on a shared NFS target. Existing NFS servers that support NFS V4 and NFS V3 over TCP/IP can be used immediately as a storage repository for virtual disks. NFS SRs can be shared, allowing any VMs with their virtual disks in an NFS VHD storage repository to migrate between servers in the same resource pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- iSCSI: Software iSCSI is supported using the open-iSCSI software iSCSI initiator or by using a supported iSCSI Host Bus Adapter (HBA).
- Hardware HBA: Hardware HBA SRs connect to a Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) or shared Serial Attached SCSI (SAS) LUNs via an HBA. Complete the configuration required to expose the LUN before running the **New Storage Repository** wizard: the wizard automatically probes for available LUNs and displays a list of all the LUNs found.
- SMB Storage: SMB servers are a common form of Windows shared filesystem infrastructure. These servers can be used as a storage repository substrate for virtual disks. Virtual Machine images in SMB servers are stored as thinly provisioned VHD files on an SMB target.
- Software FCoE (deprecated): This option allows you to configure a Software FCoE SR. Software FCoE provides a standard framework to which hardware vendors can plug in their FCoE offload capable drivers and get the same benefits of a hardware-based FCoE. This feature eliminates the need for using expensive HBAs. Before you use the New Storage Repository wizard to create a Software FCoE storage, manually complete the required configuration to expose a LUN to the host.
- Window File Sharing (SMB/CIFS): This option allows you to handle CD images stored as files in ISO format available as a Windows (SMB/CIFS) share. This type of SR can be useful for creating shared ISO libraries, for example, VM installation images.
- NFS ISO: NFS ISO SRs handle CD images stored as files in ISO format available as an NFS share. This type of SR can be useful for creating shared ISO libraries, for example, VM installation images.

2. On the **Name** page, enter the name of the new SR. By default, the wizard automatically generates a description of the SR, including a summary of the configuration options you select as you progress through the wizard. To enter your own description, clear the **Auto-generate description** check box and type in the **Description** box.
3. If you select iSCSI or Hardware HBA as your storage type, the wizard displays the **Provisioning** page. Select the type of provisioning to use for this SR. The options available are

   - Thin provisioning (GFS2). This type of provisioning is only available on GFS2 clustered pools. For more information about GFS2 clustering, see Change pool properties
   - Full provisioning (LVM)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. On the **Location** page, you enter the location of the underlying storage array and set configuration settings. The options available on this and subsequent wizard pages depend on the type of storage you selected on the first page of the wizard.
5. Click **Finish** to create the SR and close the wizard.

Related documentation

XenServer Current Release

- Create a storage repository

NFS Storage

In an NFS storage repository (SR), VM images are stored as thin-provisioned VHD format files on a shared NFS target. Existing NFS servers (that support any version of NFSv3 or NFSv4 over TCP/IP) can be used immediately as an SR for virtual disks.

NFS SRs can be shared, allowing any VMs with their virtual disks in an NFS VHD storage repository to migrate between servers in the same resource pool.

Since virtual disks on NFS SRs are created as sparse, ensure that there is enough disk space on the SR for all required virtual disks.

To configure an NFS SR

1. Open the **New Storage Repository** wizard: click **New Storage** on the toolbar.
2. Select **NFS** as the physical storage type, then click **Next**.
3. On the **Name** page, enter the name of the new SR. By default, the wizard generates a description of the SR. This description includes a summary of the configuration options that you select as you progress through the wizard. To enter your own description, clear the **Auto-generate description based on SR settings** check box and type in the **Description** box. Click **Next** to continue.
4. On the **Location** page, specify the NFS storage target details:

    - **Share Name** The IP address or DNS name of the server and the path. For example, server:/path where server is the DNS name or IP address of the server computer, and path is the directory used to contain the SR. The NFS server must be configured to export the specified path to all servers in the pool.
    - **Advanced Options** You can enter any additional configuration options here.
    - **NFS Version** Select the NFS version used by the SR.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> If the underlying storage array does not support NFSv4, NFSv3 is used to mount the share.

5. Click **Scan** to have the wizard scan for existing NFS SRs in the location you specified.
6. The New Storage Repository wizard lists any existing SRs which are not already attached. You can select an SR from the list and attach it as the new storage repository. click **Reattach an existing SR** and select the SR from the list, then click **Finish**.
7. If no existing SRs are found, simply click **Finish** to complete the new SR configuration and close the wizard.

Related documentation

XenServer Current Release

- NFS storage

Software iSCSI Storage

Software iSCSI is supported using the open-iSCSI software iSCSI initiator or by using a supported iSCSI Host Bus Adapter (HBA).

Dynamic multipathing support is available for iSCSI storage repositories. By default, multipathing uses round robin mode load balancing, so both routes have active traffic on them during normal operation. You enable and disable storage multipathing in XenCenter by using the **Multipathing** tab on the server **Properties** dialog. For more information, see Storage Multipathing.

To create a software iSCSI SR

> **NOTE:**
>
> Before performing the following steps, ensure the iSCSI Initiator IQN is set appropriately for all hosts in the pool. For more information, see Changing Server Properties.

1. Open the **New Storage Repository** wizard: click **New Storage** on the toolbar. Alternatively:
   - On the **Storage** tab for the selected pool or server, click **New SR**.
   - On the **Storage** menu, click **New SR**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In the **Resources** pane, select a server or pool then right-click and click **New SR** on the shortcut menu.

2. Select **Software iSCSI** as the physical storage type, then click **Next**.
3. On the **Name** page, enter the name of the new SR. By default, the wizard generates a description of the SR. This description includes a summary of the configuration options you select as you progress through the wizard. To enter your own description, clear the **Auto-generate description** check box and type in the **Description** box. Click **Next** to continue.
4. On the **Provisioning** page, select the type of provisioning to use. The options available are

   - Thin provisioning (GFS2). This type of provisioning is only available on GFS2 clustered pools. For more information about GFS2 clustering, see Change pool properties
   - Full provisioning (LVM)

   Click **Next** to continue.
5. On the **Location** page, specify the iSCSI target details:

   - **Target Host**: The IP address or DNS name of the iSCSI target. This can also be a comma-separated list of values.
   - **Use CHAP**: If the iSCSI target is configured to used CHAP authentication, select the **Use CHAP** check box and fill in the details:
     - CHAP User: the CHAP authentication user name credential to apply when connecting to the target.
     - CHAP Secret: the CHAP authentication password credential to apply when connecting to the target.
   - **Target IQN**: To specify the iSCSI target IQN, click the **Discover IQNs** button and then choose an IQN from the **Target IQN** list.

     IMPORTANT:

     The iSCSI target and all servers in the pool must not have the same IQN set. Every iSCSI target and initiator must have a unique IQN. If a non-unique IQN identifier is used, data corruption can occur or access to the target can be denied or both.

   - **Target LUN**: To specify the LUN on which to create the storage repository, click the **Discover LUNs** button. Choose a LUN from the **Target LUN** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Each individual iSCSI storage repository must be contained entirely on a single LUN. The SR cannot span more than one LUN. If the LUN already contains an SR, choose either to use the existing SR or to replace the existing SR with a new one. Replacing the existing SR destroys any data present on the disk.

6. Click **Finish** to complete the new SR configuration and close the wizard.

Related documentation

XenServer Current Release

- Software iSCSI storage

Hardware HBA Storage

Hardware HBA SRs connect to Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) or shared Serial Attached SCSI (SAS) LUNs through an HBA. Do the configuration required to expose the LUN before you run the **New Storage Repository** wizard. The wizard automatically probes for available LUNs and displays a list of all the LUNs found.

Dynamic multipathing support is available for Fibre Channel and iSCSI storage repositories. To enable storage multipathing, open the **Multipathing** tab on the server's **Properties** dialog; see Storage Multipathing.

To create a hardware HBA SR

1. To open the **New Storage Repository** wizard, you can do any of the following actions:
   - On the toolbar, select **New Storage**.
   - On the **Storage** tab for the selected pool or server, select **New SR**.
   - On the **Storage** menu, select **New SR**.
   - In the **Resources** pane, select a server or pool then right-click and select **New SR** on the shortcut menu.
2. Select **Hardware HBA** as the physical storage type and then select **Next**.
3. On the **Name** page, enter the name of the new SR. By default, the wizard generates a description of the SR. This description includes a summary of the configuration options you select as you progress through the wizard. To enter your own description, clear the **Auto-generate description** check box and type in the **Description** box. Click **Next** to continue to the **Provisioning** page.
4. On the **Provisioning** page, select the provisioning type. The options available are

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Thin provisioning (GFS2). This type of provisioning is only available on GFS2 clustered pools. For more information about GFS2 clustering, see Change pool properties
- Full provisioning (LVM)

Click **Next** to continue to the **Location** page.

The wizard scans for available LUNs and then displays a page listing all the LUNs found. Select a LUN from the list and click **Create**.

NOTE:

A warning message is displayed if there are existing SRs on the LUN you have selected. Review the details and choose one of the following options.

- To use the existing, click **Reattach**.
- To delete the existing SR and to create an SR, click **Format**.
- If you prefer to select a different LUN, click **Cancel** and select a LUN from the list.

The **Summary** page displays information about the new SR. Read the information and then click **Finish** to complete the SR creation process.

Related documentation

XenServer Current Release

- Hardware HBA storage

SMB Storage

SMB servers are a common form of Windows shared filesystem infrastructure that you can use as a storage repository substrate for virtual disks. VM images in SMB servers are stored as thinly provisioned VHD files on an SMB target. As SMB servers are shared SRs, you can start VMs that have virtual disks in SMB servers on any server in a pool. These VMs readily migrate between the servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- SMB storage is available for XenServer Premium Edition customers. To learn more about XenServer licensing, see About XenServer Licensing.
- When using SMB storage, do not remove the share from the storage before detaching the SMB SR.

To configure an SMB SR

1. Open the **New Storage Repository** wizard: click **New Storage** on the toolbar.
2. Select **SMB** as the physical storage type, then click **Next**.
3. On the **Name** page, enter the name of the new SR. By default, the wizard generates a description of the SR. This description includes a summary of the configuration options you select as you progress through the wizard. To enter your own description, clear the **Auto-generate description based on SR settings** check box and type in the **Description** box. Click **Next** to continue.
4. On the **Location** page, specify the details of the storage target:
   - **Share Name** The IP address or DNS name of the server and the path. For example, `\\server\path` where `server` is the DNS name or IP address of the server computer, and `path` is a folder or file name. Configure the SMB server to export the specified path to all servers in the pool.
   - **User name and Password** (Optional) To connect to an SMB server using a different user name, enter your login user name and password.
5. Click **Scan** to have the wizard scan for existing SMB SRs in the location you specified.
6. The **New Storage Repository** wizard lists any existing SRs which are not already attached. You can select an SR from the list and attach it as the new storage repository. Click **Reattach an existing SR** and select the SR from the list, then click **Finish**.
7. If no existing SRs are found, simply click **Finish** to complete the new SR configuration and close the wizard.

Related documentation

XenServer Current Release

- SMB storage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Software FCoE Storage (deprecated)

Software FCoE provides a standard framework that hardware vendors can plug in their FCoE offload-capable NIC into. By using this framework, they get the same benefits of a hardware-based FCoE. This feature eliminates the need for using expensive HBAs. Software FCoE can be used with Open vSwitch and Linux bridge as the network back end.

Before creating a software FCoE storage, complete the configuration required to expose a LUN to the host. This process includes configuring the FCoE fabric and allocating LUNs to your SAN's public world wide name (PWWN). After you complete this configuration, the available LUN is mounted to the host's CNA as a SCSI device. You can then use the SCSI device to access the LUN as if it were a locally attached SCSI device. For information about configuring the physical switch and the array to support FCoE, see the documentation provided by the vendor. For detailed information about Software FCoE, see the Storage

NOTE:

- Software FCoE is deprecated and will be removed in a future release.
- When you configure the FCoE fabric, do not use VLAN 0. The XenServer® host cannot find traffic that is on VLAN 0.
- Software FCoE can be used when using Open vSwitch and Linux bridge as the network back end.

To create a Software FCoE SR

1. To open the **New Storage Repository** wizard, do one of the following actions:
   - On the toolbar, click **New Storage**.
   - On the **Storage** tab for the selected pool or server, click **New SR**.
   - On the **Storage** menu, click **New SR**.
   - In the **Resources** pane, select a server or pool then right-click and click **New SR** on the shortcut menu.
2. Select **Software FCoE** as the Storage type and click **Next**.
3. Enter a name for the new SR. By default, the wizard generates a description of the SR. This description includes a summary of the configuration options you select as you progress through the wizard. To enter your own description, clear the **Auto-generate description** check box and type in the **Description** box. Click **Next** to continue to the **Location page**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. XenCenter® probes for available LUNs and displays a list of LUNs currently exposed to the host. This page also displays detailed information about the LUN such as, the size, serial, ID, NIC. Choose the LUN (s) that you want to allocate to the SR and click **Next**.

   NOTE:

   If the host cannot find any LUNs, an error message is displayed. Verify your hardware configuration and retry to continue with the SR creation process.

5. Review the summary and click **Finish** to complete the SR creation process.

Related documentation

XenServer 8.4

- Software FCoE storage (deprecated)

ISO Storage

This type of SR can be useful for creating shared ISO libraries. For example, use it to create a library of VM installation images. The following ISO SR types are provided for handling CD images stored as files in ISO format:

- The **NFS ISO** SR type handles CD images stored as files in ISO format available as an NFS share.
- The **Windows File Sharing (SMB/CIFS)** SR type handles CD images stored as files in ISO format available as a Windows (SMB/CIFS) share.

To configure a new ISO SR on NFS storage

1. Open the **New Storage Repository** wizard: click **New Storage** on the toolbar.
2. Under **ISO library**, select **NFS ISO** as the storage type, then click **Next**.
3. On the **Name** page, enter the name of the new SR. By default, the wizard generates a description of the SR. This description includes a summary of the configuration options you select as you progress through the wizard. To enter your own description, clear the **Auto-generate description** check box and type in the **Description** box.

   Click **Next** to continue.

4. On the **Location** page, specify the ISO storage target details:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Share Name**: For example, `server:/path` where `server` is the DNS name or IP address of the server computer, and `path` is a folder or file name.
- **NFS Version**: Select the NFS version that the SR uses.

> **NOTE:**
>
> If the underlying storage array does not support NFSv4, NFSv3 is used to mount the share.

5. Click **Finish** to complete the new SR configuration and close the wizard.

To configure a new ISO SR on CIFS/SMB storage

1. Open the **New Storage Repository** wizard: click **New Storage** on the toolbar.
2. Under **ISO library**, select **Windows File Sharing (SMB/CIFS)** as the storage type, then click **Next**.
3. On the **Name** page, enter the name of the new SR. By default, the wizard generates a description of the SR. This description includes a summary of the configuration options you select as you progress through the wizard. To enter your own description, clear the **Auto-generate description** check box and type in the **Description** box.

   Click **Next** to continue.
4. On the **Location** page, specify the ISO storage target details:

   - **Share Name**: For example, `\\server\sharename` where `server` is the DNS name or IP address of the server computer, and `sharename` is a folder or file name.
   - **Use different user name**: If you want to connect to an SMB server using a different user name, select this check box and then enter your login user name and password.
5. Click **Finish** to complete the new SR configuration and close the wizard.

Related documentation

XenServer Current Release

- ISO library on NFS storage
- ISO library on CIFS/SMB storage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Thin-provisioned shared GFS2 block storage

Thin provisioning better utilizes the available storage by allocating disk storage space to VDIs as data is written to the virtual disk, rather than allocating the full virtual size of the VDI in advance. Thin provisioning enables you to significantly reduce the amount of space required on a shared storage array, and with that your Total Cost of Ownership (TCO).

Thin provisioning for shared block storage is of particular interest in the following cases:

- You want increased space efficiency. Images are sparsely and not thickly allocated.
- You want to reduce the number of I/O operations per second on your storage array. The GFS2 SR is the first SR type to support storage read caching on shared block storage.
- You use a common base image for multiple virtual machines. The images of individual VMs will then typically utilize even less space.
- You use snapshots. Each snapshot is an image and each image is now sparse.
- You want to create VDIs that are greater than 2 TiB in size. The GFS2 SR supports VDIs up to 16 TiB in size.
- Your storage does not support NFS or SMB3 and only supports block storage. If your storage supports NFS or SMB3, we recommend you use these SR types instead of GFS2.
- Your storage doesn’t support thin provisioning of LUNs. If your storage does thin provision LUNs, you can encounter problems and run out of space when combining it with GFS2. Combining GFS2 with a thin-provisioned LUN does not provide many additional benefits and is not recommended. XenCenter® shows a warning if you attempt to use GFS2 with a thin-provisioned LUN.

The shared GFS2 type represents disks as a filesystem created on an iSCSI or HBA LUN. VDIs stored on a GFS2 SR are stored in the QCOW2 image format.

1. Plan your GFS2 environment

To provide the benefits of thin provisioning on shared block storage without risk of data loss, your pool must deliver a good level of reliability and connectivity. It is crucial that the hosts in the resource pool that uses GFS2 can reliably communicate with one another. To ensure this, XenServer® requires that you use a clustered pool with your GFS2 SR. We also recommend that you design your environment and configure XenServer features to provide as much resiliency and redundancy as possible.

Before setting up your XenServer pool to work with GFS2 SRs, review the following requirements and recommendations for an ideal GFS2 environment:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Recommended:** Configure redundant networking infrastructure.
- **Recommended:** Create a dedicated bonded network
- **Required:** Set up a GFS2 clustered pool
- **Optional** Increase your control domain memory
- **Recommended:** Configure storage multipathing
- **Required:** Create a GFS2 SR

A clustered pool with GFS2 SRs has some differences in behavior to other types of pool and SR. For more information, see Constraints.

2. Configure redundant networking infrastructure

A bonded network links two or more NICs together to create a single channel for network traffic. We recommend that you use a bonded network for your GFS2 clustered pool traffic. However, before you set up your bonded network, ensure that your network hardware configuration promotes redundancy in the bonded network. Consider implementing as many of these recommendations as is feasible for your organization and environment.

The following best practices add resiliency against software, hardware, or power failures that can affect your network switches.

- Ensure that you have separate physical network switches available for use in the bonded network, not just ports on the same switch.
- Ensure that the separate switches draw power from different, independent power distribution units (PDUs).
- If possible, in your data center, place the PDUs on different phases of the power feed or even feeds provided by different utility companies.
- Consider using uninterruptible power supply units to ensure that the network switches and servers can continue to function or perform an orderly shutdown in the event of a power failure.

3. Create a dedicated bonded network

It is important to ensure that hosts in a GFS2 clustered pool can communicate reliably with one another. Creating a bonded network for this pool traffic increases the resiliency of your clustered pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The GFS2 cluster network cannot be on a non-management VLAN.

A bonded network creates a bond between two or more NICs to create a single, high-performing channel that your GFS2 clustered pool can use for cluster heartbeat traffic. We strongly recommend that this bonded network is not used for any other traffic. Create a separate network for the pool to use for management traffic.

NOTE:

If you have a firewall between the hosts in your pool, ensure that hosts can communicate on the GFS2 cluster network using the following ports:

- TCP: 8892, 8896, 21064
- UDP: 5404, 5405

For more information, see Communication ports used by XenServer.

To create a bonded network to use as the GFS2 cluster network:

1. Open the **New Network** wizard.
2. On the first page of the wizard, select **Bonded Network** and then click **Next**.
3. On the **Bond Members** page, select the NICs you want to bond together. To select a NIC, select its check box in the list. Up to four NICs can be selected in this list. Clear the check box to deselect a NIC.
4. Under **Bond mode**, choose the type of bond:
    - Select **Active-active** to configure an active-active bond. With this bond, traffic is balanced between the bonded NICs. If one NIC within the bond fails, the server's network traffic automatically routes over the second NIC.
    - Select **Active-passive** to configure an active-passive bond, where traffic passes over only one of the bonded NICs. In this mode, the second NIC only becomes active if the active NIC fails, for example, if it loses network connectivity.
    - Select **LACP with load balancing based on source MAC address** to configure an LACP bond. With this bond, the outgoing NIC is selected based on the MAC address of the VM from which the traffic originated. Use this option to balance traffic in an environment where you have several VMs on the same host. This option is not suitable if there are fewer virtual

© 1997–2026 Citrix Systems, Inc. All rights reserved.

interfaces (VIFs) than NICs: as load balancing is not optimal because the traffic cannot be split across NICs.

- Select **LACP with load balancing based on IP and port of source and destination** to configure an LACP bond. This bond uses the source IP address, source port number, destination IP address, and destination port number to allocate the traffic across the NICs. Use this option to balance traffic from VMs in an environment where the number of NICs exceeds the number of VIFs.

NOTES:

- To be able to view the LACP bonding options in XenCenter and create an LACP bond, configure vSwitch as the network stack. Also, your switches must support the IEEE 802.3ad standard.
- Active-active and active-passive bond types are available for both the vSwitch and Linux bridge.
- You can bond either two, three, or four NICs when vSwitch is the network stack. However, you can only bond two NICs when the Linux bridge is the network stack. The Linux bridge network stack is deprecated and will be removed in a future release.

5. To use jumbo frames, set the Maximum Transmission Unit (**MTU**) to a value between 1500–9216.
6. Select the **Automatically add this network to new virtual machines** check box to have the new network added to any new VMs created using the **New VM** wizard.
7. Click **Finish** to create the new network and close the wizard.

After you create your bonded network on the pool coordinator, when you join other XenServer hosts to the pool, the network and bond information is automatically replicated to the joining server.

For more information, see Configuring NICs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTES:

- Changing the IP address of the GFS2 cluster network by using XenCenter requires clustering and GFS2 to be temporarily disabled.
- Do not change the bonding of your GFS2 cluster network while the cluster is live and has running VMs. This action can cause hosts in the cluster to hard restart (fence).
- If you have an IP address conflict (multiple hosts having the same IP address) on your GFS2 cluster network involving at least one host with clustering enabled, the cluster does not form correctly and the hosts are unable to fence when required. To fix this issue, resolve the IP address conflict.

4. Set up a GFS2 clustered pool

To use shared GFS2 storage, the XenServer resource pool must be a clustered pool. Enable GFS2 clustering on your pool before creating a GFS2 SR.

To create a GFS2 clustered pool:

1. Open the **New Pool** dialog box by clicking **New Pool** on the toolbar.
2. Enter a name for the new pool and an optional description. The name is displayed in the **Resources** pane.
3. Nominate the pool coordinator by selecting a server from the **Coordinator** list.
4. Select more servers to place in the new pool from the **Additional members** list. All available managed servers are listed. If a server is not listed, you can add it to the list by clicking **Add New Server**. If a managed server is not listed, it might be because it does not satisfy one or more of the pool join requirements listed in Pool requirements.
5. Select **Create Pool** to create the pool and close the dialog box.
6. Select the pool in the **Resources** panel and in its **General** tab, select **Properties**. The **Pool Properties** window opens.
7. In the **GFS2 Clustering** tab, select **Enable GFS2 clustering** and choose the dedicated bonded network you created to be the cluster network.
8. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Increase your control domain memory

If you have insufficient control domain memory on your hosts, your pool can experience network instabililty. Network instability can cause problems for a clustered pool with GFS2 SRs.

It is important to ensure that your GFS2 clustered pool has an appropriate amount of control domain memory. For information about changing the amount of control domain memory, see Changing the control domain memory.

6. Configure storage multipathing

Ensure that storage multipathing is set up between your clustered pool and your GFS2 SR.

Multipathing routes storage traffic to a storage device over multiple paths for redundancy. All routes can have active traffic on them during normal operation, which results in increased throughput.

Before enabling multipathing, verify that the following statements are true:

- Your ethernet or fibre switch is configured to make multiple targets available on your storage server.

  For example, an iSCSI storage back-end queried for `sendtargets` on a given portal returns multiple targets, as in the following example:

  ```
  iscsiadm -m discovery --type sendtargets --portal 192.168.0.161

  192.168.0.161:3260,1 iqn.strawberry:litchie

  192.168.0.204:3260,2 iqn.strawberry:litchie
  ```

  However, you can perform additional configuration to enable iSCSI multipath for arrays that only expose a single target. For more information, see iSCSI multipath for arrays that only expose a single target.
- For iSCSI only, the control domain (dom0) has an IP address on each subnet used by the multipathed storage.

  Ensure that for each path to the storage, you have a NIC and that there is an IP address configured on each NIC. For example, if you want four paths to your storage, you must have four NICs that each have an IP address configured.
- For iSCSI only, every iSCSI target and initiator has a unique IQN.
- For iSCSI only, the iSCSI target ports are operating in portal mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For HBA only, multiple HBAs are connected to the switch fabric.
- If possible, use multiple redundant switches.

To enable multipathing:

Complete the following steps for every server in your pool:

1. In the **Resources** pane, select the server and then put it into **maintenance mode**. There is a short delay while XenCenter migrates any active virtual machines and unplugs the existing storage. If the server is a pool coordinator, it is disconnected and might disappear from the **Resources** pane temporarily while a new pool coordinator is assigned. When the server reappears in the **Resources** pane with the server maintenance mode icon(), continue to the next step.
2. On the **General** tab, select **Properties** and then select the **Multipathing** tab.
3. To enable multipathing, check the **Enable multipathing on this server** check box. To disable multipathing, clear the check box.
4. Click **OK** to apply the new setting and close the dialog box. There is a short delay while XenCenter saves the new storage configuration.
5. Take the server back out of maintenance mode. Select the server in the **Resources** pane, right-click, and select **Exit Maintenance Mode**.

Ensure that you enable multipathing on all hosts in the pool. All cabling and, in the case of iSCSI, subnet configurations must match the corresponding NICs on each host.

7. Create a GFS2 SR

Create your shared GFS2 SR on an iSCSI or an HBA LUN that is visible to all XenServer hosts in your resource pool.

NOTE:

We do not recommend using a thin-provisioned LUN with GFS2. XenCenter shows a warning if you attempt to use GFS2 with a thin-provisioned LUN.

However, if you do choose this configuration, you must ensure that the LUN always has enough space to allow XenServer to write to it.
You can add up to 62 GFS2 SRs to a clustered pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To create a software iSCSI SR

NOTE:

Before performing the following steps, ensure that the iSCSI Initiator IQN is set appropriately for all hosts in the pool. For more information, see Changing Server Properties.

1. Open the **New Storage Repository** wizard: click **New Storage** on the toolbar. Alternatively:
   - On the **Storage** tab for the selected pool or server, click **New SR**.
   - On the **Storage** menu, click **New SR**.
   - In the **Resources** pane, select a server or pool then right-click and click **New SR** on the shortcut menu.
2. Select **Software iSCSI** as the physical storage type, then click **Next**.
3. On the **Name** page, enter the name of the new SR. By default, the wizard generates a description of the SR. This description includes a summary of the configuration options you select as you progress through the wizard. To enter your own description, clear the **Auto-generate description** check box and type in the **Description** box. Click **Next** to continue.
4. On the **Provisioning** page, select **Thin provisioning (GFS2)**.
5. On the **Location** page, specify the iSCSI target details:
   - **Target Host**: The IP address or DNS name of the iSCSI target. This can also be a comma-separated list of values.
   - **Use CHAP**: This is not supported with GFS2 SRs. Leave this option unselected.
   - **Target IQN**: To specify the iSCSI target IQN, click the **Discover IQNs** button and then choose an IQN from the **Target IQN** list.

     IMPORTANT:

     The iSCSI target and all servers in the pool must not have the same IQN set. Every iSCSI target and initiator must have a unique IQN. If a non-unique IQN identifier is used, data corruption can occur, access to the target can be denied, or both.

   - **Target LUN**: To specify the LUN on which to create the storage repository, click the **Discover LUNs** button. Choose a LUN from the **Target LUN** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Each individual iSCSI storage repository must be contained entirely on a single LUN. The SR cannot span more than one LUN. If the LUN already contains an SR, choose either to use the existing SR or to replace the existing SR with a new one. Replacing the existing SR destroys any data present on the disk.

6. Click **Finish** to complete the new SR configuration and close the wizard.

To create a hardware HBA SR

1. To open the **New Storage Repository** wizard, you can do any of the following actions:
   - On the toolbar, select **New Storage**.
   - On the **Storage** tab for the selected pool or server, select **New SR**.
   - On the **Storage** menu, select **New SR**.
   - In the **Resources** pane, select a server or pool then right-click and select **New SR** on the shortcut menu.
2. Select **Hardware HBA** as the physical storage type and then select **Next**.
3. On the **Name** page, enter the name of the new SR. By default, the wizard generates a description of the SR. This description includes a summary of the configuration options you select as you progress through the wizard. To enter your own description, clear the **Auto-generate description** check box and type in the **Description** box. Click **Next** to continue to the **Provisioning** page.
4. On the **Provisioning** page, select the **Thin provisioning (GFS2)**.
5. Click **Next** to continue to the **Location** page.
6. The wizard scans for available LUNs and then displays a page listing all the LUNs found. Select a LUN from the list and click **Create**.

   NOTE:

   A warning message is displayed if there are existing SRs on the LUN you have selected. Review the details and choose one of the following options.

   - To use the existing, click **Reattach**.
   - To delete the existing SR and to create an SR, click **Format**.
   - If you prefer to select a different LUN, click **Cancel** and select a LUN from the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. The **Summary** page displays information about the new SR. Read the information and then click **Finish** to complete the SR creation process.

Constraints

Shared GFS2 storage currently has the following constraints:

- As with any thin-provisioned SR, if the GFS2 SR usage grows to 100%, further writes from VMs fail. These failed writes can then lead to failures within the VM, possible data corruption, or both.
- XenCenter shows an alert when your SR usage grows to 80%. Ensure that you monitor your GFS2 SR for this alert and take the appropriate action if seen. On a GFS2 SR, high usage causes a performance degradation. We recommend that you keep your SR usage below 80%.
- VM migration with storage migration (live or offline) is not supported for VMs whose VDIs are on a GFS2 SR. You also cannot migrate VDIs from another type of SR to a GFS2 SR.
- The FCoE transport is not supported with GFS2 SRs.
- Trim/unmap is not supported on GFS2 SRs.
- CHAP is not supported on GFS2 SRs.
- You cannot export VDIs that are greater than 2 TiB as VHD or OVA/OVF. However, you can export VMs with VDIs larger than 2 TiB in XVA format.
- We do not recommend using a thin-provisioned LUN with GFS2. However, if you do choose this configuration, you must ensure that the LUN always has enough space to allow XenServer to write to it.
- We do not recommend using SAN deduplication with GFS2 SRs. However, if you do choose this configuration, you must use suitable external monitoring of your SAN utilization to ensure that there is always space for XenServer to write to.
- Your GFS2 file system cannot be larger than 100 TiB.
- You cannot have more than 62 GFS2 SRs in your pool.
- GFS2 clustered pools only support up to 16 hosts per pool.
- For GFS2 cluster traffic, we strongly recommend that you use a bonded network that uses at least two different network switches. Do not use this network for any other purposes.
- Changing the IP address of the GFS2 cluster network by using XenCenter requires clustering and GFS2 to be temporarily disabled.
- Do not change the bonding of your GFS2 cluster network while the cluster is live and has running VMs. This action can cause hosts in the cluster to hard restart (fence).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you have an IP address conflict (multiple hosts having the same IP address) on your GFS2 cluster network involving at least one host with GFS2 clustering enabled, the cluster does not form correctly and the hosts are unable to fence when required. To fix this issue, resolve the IP address conflict.

Related documentation

XenServer Current Release

- GFS2 clustered pools
- Thin-provisioned shared GFS2 block storage

Storage properties

Viewing storage properties

You can view the details for all storage repositories (SRs) in your XenServer® pool from the **Storage** tab of the pool. Select a server or pool in the **Resources** pane and then click the **Storage** tab. This tab displays information about the local and shared storage repositories. This information includes the name, description, storage type, usage, the size of the SR, and the virtual allocation.

To view detailed information about an individual storage repository, select the SR repository in the **Resources** pane. In the main pane, the following tabs are available: **General**, **Storage**, and **Search**.

General

The **General** section of the **General** tab displays the information about the storage repository. This information can include the name, description, any tags applied to the SR, the folder the SR is in, storage type, the size of the SR, the SCSI ID, and the UUID of the SR.

NOTE

For GFS2 SRs, the size is displayed in the form "*a* GB used of *b* GB total (*c* GB allocated)". The values in this statement have the following meanings:

- *c* is the space that is allocated and used in the SR. (If you run the `du` command, this is the value shown.)
- *b* is the actual total size of the LUN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- *a* is the 'used' space. This value is the sum of the file sizes for the files on the SR and does not take into account blocks that have been freed from sparse files. These freed blocks can now be used by other VMs. (If you run the `df` command, this is the value shown.)

  On GFS2 SRs, the VM disks are stored in the QCOW2 format, which is both thinly provisioned and sparse. When data blocks are deleted from the VM the associated data blocks in the VM disk file are freed back to the SR filesystem and marked as unallocated, but the file size is unchanged. This behavior can cause discrepencies between the value of *a* and the value of *c*.

The **Status** section lists the state of the SR and shows whether it is connected to servers in the pool.

The **Multipathing** section shows whether multipathing is active between the SR and servers in the pool.

Storage

The **Storage** tab lists the virtual disks located on the storage repository. For each disk, the table shows the disk name, description, size, virtual machine name, and whether changed block tracking is enabled.

Search

Using the **Search** tab, you can construct queries based on object types, folders, and attributes. For more information, see Searching Resources.

Changing SR properties

The **Properties** dialog box allows you to modify the details of your SRs and manage them effectively by organizing the resources using folders, tags, and custom fields. It also allows you to configure alerts when the storage throughput exceeds specific limits.

You can access the **Properties** dialog box for an SR in one of the following ways:

- Select a server or pool in the **Resources** pane and then click the **Storage** tab. This lists the local and shared storage in your pool. Select an SR from the list and click **Properties**.
- Select the storage repository in the **Resources** pane. In the **General** tab for the SR, click **Properties**.

General

The **General** tab allows you to change the name and description of the SR, and manage its folder and tags:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To change the name of the SR, enter a new name in the **Name** box.
- To change its description, enter new text in the **Description** box.
- To place the SR in a folder or to move it to a different folder, click **Change** in the **Folder** box and select a folder. For more information, see Using folders.
- To tag and untag the SR and to create and delete tags, see Using tags.

Custom fields

Custom fields allow you to define or modify any additional information about the SR. This tab helps you to search and effectively organize your storage repositories. For more information, see Using custom fields.

Alerts

The **Alerts** tab allows you to configure alerts when the total read and write storage throughput activity on a Physical Block Device (PBD) exceeds the specified limit. Check **Generate storage throughput alerts** and set the storage throughput and time threshold that triggers the alert.

NOTE:

Physical Block Devices (PBD) represent the interface between a specific XenServer host and an attached SR. When the total read/write SR throughput activity on a PBD exceeds the threshold you have specified, alerts are generated on the host connected to the PBD. Unlike other host alerts, this alert must be configured on the relevant SR.

Read Caching

Read caching improves performance on NFS, EXT3/EXT4, SMB, or GFS2 SRs that host multiple VMs cloned from the same source. You might want to disable read caching in the following cases:

- You have no file-based SRs
- You do not have any cloned VMs
- It is not providing any performance benefits

On the **Read Caching** tab, you can choose to enable or disable read caching on NFS, EXT3/EXT4, or SMB SRs.

For GFS2 SRs, the **Read caching** tab is not shown and read caching cannot be disabled.

For more information, see Storage read caching.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- Storage

Removing an SR

Using XenCenter®, a storage repository can be removed temporarily or permanently:

- **Detach**. Detaching a storage repository breaks the association between the storage device and the pool or server, and its virtual disks become inaccessible. The contents of the virtual disks and the meta-information used by virtual machines to access the virtual disks are preserved. **Detach** can be used when you must temporarily take a storage repository offline, for example, for maintenance. A detached SR can then be reattached. For more information, see Reattaching an SR.
- **Forget**. When you forget an SR, the contents of the virtual disks on the SR are preserved. However, the information used to connect virtual machines to the virtual disks it contains is permanently deleted. The SR is removed from the **Resources** pane.

  A Forget operation cannot be undone.
- **Destroy**. Destroying an SR deletes the contents of the SR permanently and the SR is removed from the **Resources** pane.

  A Destroy operation cannot be undone. For information about how to destroy an SR, refer to the Storage.

NOTE:

- You cannot remove a storage repository if it contains virtual disks of a currently running virtual machine.
- When using SMB storage, do not remove the share from the storage before detaching the SMB SR.

To detach a storage repository

1. Select the SR in the **Resources** pane and click the **Storage** tab.
2. Note the virtual machines that currently have attached virtual disks on this storage repository.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Ensure that the virtual machines that have disks on this storage repository are not running.
4. Select the SR in the **Resources** pane and then do one of the following:
   - Right-click and click **Detach** on the **Resources** pane shortcut menu.
   - On the **Storage** menu, click **Detach**.
5. Click **Yes** to confirm.

NOTE:

While a storage repository is detached, you cannot start any virtual machines that have attached virtual disks on that storage repository.

To forget a storage repository

Certain types of storage repositories, such as iSCSI, must be detached before attempting to forget the SR.

IMPORTANT:

An SR Forget operation cannot be undone. The information used to connect VMs to the virtual disks on the SR is permanently deleted.

Perform the following steps to forget an SR:

1. Select the SR in the Resources pane and then do one of the following:
   - Right-click and click **Forget** on the **Resources** pane shortcut menu.
   - On the **Storage** menu, click **Forget**.
2. Click **Yes, Forget** to confirm.

Related documentation

XenServer Current Release

- Manage storage repositories

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Reattaching an SR

A detached storage device has no association with any pool or server, but the data stored on it is preserved. When you reattach an SR to a managed server, provide the storage configuration information in the same way as when you add an SR.

To reattach a detached SR

1. Select the detached SR in the **Resources** pane and then do one of the following:
   - Right-click and select **Reattach Storage Repository** on the **Resources** pane shortcut menu.
   - On the **Storage** menu, select **Reattach Storage Repository**.
2. Enter the required configuration information in the same way as when you add an SR. See:
   - NFS VHD Storage
   - Software iSCSI Storage
   - Hardware HBA Storage
   - ISO Storage
3. Click **Finish** to complete the SR configuration and close the wizard.

Related documentation

XenServer Current Release

- Manage storage repositories

Storage Multipathing

Dynamic multipathing support is available for Fibre Channel and iSCSI storage repositories. By default, multipathing uses round robin mode load balancing, so both routes have active traffic on them during normal operation. You enable and disable storage multipathing in XenCenter® via the **Multipathing** tab on the server's **Properties** dialog.

Before you enable multipathing:

- Verify that multiple targets are available on your storage server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The server must be placed in maintenance mode. This action ensures that any running virtual machines with virtual disks in the affected storage repository are migrated before the changes are made.
- Multipathing must be configured on each host in the pool. All cabling and, in the case of iSCSI, subnet configurations must match for the corresponding NICs on each host. (For example, all NICs must be configured to use the same subnet. For more information, see Configuring IP Addresses.)

For more in-depth multipathing information, see Multipathing.

You can use up to 16 paths to a single LUN.

To enable multipathing

1. In the **Resources** pane, select the server and then put it into **maintenance mode**. There is a short delay while XenCenter migrates any active virtual machines and unplugs the existing storage. If the server is a pool coordinator, it is disconnected and might disappear from the **Resources** pane temporarily while a new pool coordinator is assigned. When the server reappears in the **Resources** pane with the server maintenance mode icon, continue to the next step.

2. On the **General** tab, select **Properties** and then select the **Multipathing** tab.
3. To enable multipathing, check the **Enable multipathing on this server** check box. To disable multipathing, clear the check box.
4. Click **OK** to apply the new setting and close the dialog box. There is a short delay while XenCenter saves the new storage configuration.
5. Take the server back out of maintenance mode. Select the server in the **Resources** pane, right-click, and select **Exit Maintenance Mode**.

Related documentation

XenServer Current Release

- Storage multipathing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Storage Read Caching

Read Caching improves a VM's disk performance as, after the initial read from an external disk, data is cached within the host's free memory. It greatly improves performance in situations where many VMs are cloned off a single base VM as it drastically reduces the number of blocks read from disk. For example, Read Caching improves performance in Citrix Virtual Desktops Machine Creation Services™ (MCS) environments.

This performance improvement can be seen whenever data must be read from disk more than once, as it gets cached in memory. This performance difference is most noticeable in the degradation of service that occurs during heavy I/O situations. For example:

- When a significant number of end users boot up within a narrow time frame (boot storm)
- When a significant number of VMs are scheduled to run malware scans at the same time (antivirus storm)

NOTE:

The amount of memory assigned to the XenServer control domain (dom0) might need to be increased for the most efficient use of read caching. For instructions on increasing dom0 memory, see Changing the Control Domain Memory.

XenCenter® displays the status of Read Caching on the VM's **General** tab.

NOTE:

Storage Read Caching is available for XenServer® Premium Edition customers.

Read Caching is enabled by default, provided:

- The XenServer host is licensed with XenServer Premium Edition.
- The VM is attached to a VDI on a file-based SR such as NFS, EXT3/EXT4, or GFS2. Read Caching cannot be used with other SR types.
- The VM is created from a fast clone or a snapshot, or the VM is attached to a read-only VDI.

For detailed information about Read Caching, see Storage read caching.

To disable read caching

You can disable read caching for an NFS, EXT3/EXT4, or SMB SR in its **Properties** dialog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In the **Resources** pane, select the SR that you want to disable read caching on.
2. In the **General** tab, click **Properties**.
3. In the **Properties** dialog, deselect **Enable Read Caching**.
4. Click **OK**.

For GFS2 SRs, the **Read caching** tab is not shown and read caching cannot be disabled.

To enable read caching

You can enable read caching for an SR in its **Properties** dialog.

1. In the **Resources** pane, select the SR that you want to enable read caching on.
2. In the **General** tab, click **Properties**.
3. In the **Properties** dialog, select **Enable Read Caching**.
4. Click **OK**.
5. Restart any VMs that you want to benefit from the changed setting.

Related documentation

XenServer Current Release

- Storage read caching

PVS-Accelerator

The XenServer PVS-Accelerator feature enhances performance by caching PVS read requests on each XenServer host. This feature is available for customers using XenServer and Citrix Provisioning (PVS), a popular solution for image management and hosting in Citrix Virtual Apps and Desktops. To take advantage of PVS-Accelerator, use XenServer with Citrix Provisioning 7.12 or higher.

Enable PVS-Accelerator

Enabling the PVS-Accelerator involves two key steps:

1. Configure PVS-Accelerator in XenServer.
2. Complete the cache configuration in PVS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure PVS-Accelerator in XenServer

You can configure PVS-Accelerator in XenServer by using XenCenter or the xe CLI. The following section contains XenCenter instructions. For information about configuring the PVS-Accelerator using the xe CLI, see the XenServer product documentation.

Configure PVS-Accelerator by using XenCenter®:

1. In XenCenter, select the pool or the standalone host and then select the **PVS** tab.

   The **PVS** tab appears at the pool-level (or host-level if there is no pool) in XenCenter after installing the *PVS-Accelerator Supplemental Pack* and assigning a Premium Edition license. The **PVS** tab displays a summary of the Read caching status for all the VMs running inside the pool.
2. Select **Configure PVS-Accelerator**.
3. On the **PVS-Accelerator configuration** dialog, select **Add cache configuration** to add a PVS site.

   a. Enter a name for the PVS site in the **Site name** field.

   b. For each host in the pool, specify what cache to use:

      - **Memory only**: Uses up to the specified cache size in the Control Domain memory. This option requires additional memory to be assigned to the Control Domain. For information on how to assign memory to the Control Domain, see Changing the Control Domain Memory.
      - **Storage Repository (SR)**: Uses up to the specified cache size on the SR. It also implicitly uses available control domain memory as a best effort cache tier.

   Important:

   - If neither Memory only nor an SR is specified, the read cache is not activated.
   - PVS-Accelerator has been designed to utilize either memory only, or a combination of disk and memory. Irrespective of the configuration choice, increase the amount of memory allocated to the Control Domain to ensure there is no system performance degradation.
   - We recommend that you allocate at least 4 GB of Control Domain memory per host to avoid frequent disk accesses that cause higher read-latency and therefore degrade performance. For more information, see Changing the Control Domain Memory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- We recommend that you allocate at least 5 GB of cache space per vDisk version that you actively use.

4. Click **OK**. The new PVS site and the chosen cache storage configuration are added in the XenServer server.

Complete the cache configuration in PVS

After configuring the PVS-Accelerator in the XenServer server, complete the cache configuration for the newly created site using the Citrix Provisioning Console or the PowerShell Snap-In CLI. For more information, see Citrix Provisioning Documentation. When this step is complete, you can view a list of PVS Servers configured for the new site by clicking **View PVS Servers** on the **PVS-Accelerator configuration** dialog.

Cache operation

After you start a VM with PVS-Accelerator, the caching status for the VM is displayed on the **PVS** tab and on the **General** tab of the VM. The following table lists the status messages displayed on these tabs.

PVS-ACCELERATOR STATUS	DESCRIPTION
Initialized	PVS-Accelerator has been started and is ready to cache. If the cache remains in this state when the VM has been booted, it means that the PVS Server IP addresses have not been configured correctly, or the VM is not communicating with the PVS server using its primary network interface.
Caching	PVS-Accelerator is working.
Stopped	PVS-Accelerator is not running for the VM. The cache remains in this state when the VM is not running, or when the cache is not configured sufficiently.
Incompatible Write Cache Mode	There is no caching as the VM is configured to persist changes on the PVS server. Ensure the VM type is "Production" or "Test" and the vDisk is in "Standard Image" Access mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PVS-ACCELERATOR STATUS	DESCRIPTION
Incompatible Protocol Version	The PVS Server version is incorrect. Ensure that you are using Provisioning Services 7.12 or higher.

The PVS-Accelerator functionality caches:

- **Reads** from a vDisk but not writes or reads from a write cache
- **Based on image versions**. Multiple VMs share cached blocks if they use the same image version
- Devices with **any write cache type**
- A vDisk with the Access mode set to **Standard Image**. Caching is not compatible with any vDisk set to Private Image mode
- Devices that are marked as type **Production** or Test. Devices marked as type **Maintenance** are not cached

Notes:

- PVS-Accelerator is available for XenServer Premium Edition customers.
- XenCenter displays various PVS-Accelerator performance graphs on the host-level Performance tab. The performance graphs provide detailed insight into the cache operation.
- The PVS-Accelerator feature uses the capabilities of OVS and is therefore not available on hosts that use Linux Bridge (deprecated) as the network back end.
- PVS-Accelerator works on the first virtual network interface (VIF) of a cached VM. Therefore, use the first VIF to connect the PVS storage network for the caching to work.

Related documentation

XenServer Current Release

- PVS-Accelerator

Reclaiming Freed Space

Use the **Reclaim freed space** option in XenCenter you to free up unused blocks on a LUN that is thinly provisioned by the storage array. Once released, the array can then reuse the reclaimed space. The **Reclaim freed space** operation is only available for LVM-based SRs that are thinly

© 1997–2026 Citrix Systems, Inc. All rights reserved.

provisioned on the array. These SR types are iSCSI, Fibre Channel, or Local LVM. This feature is not enabled on file-based SRs such as NFS and EXT3/EXT4 as these SR types do not require a manual space reclamation operation.

To reclaim freed space:

1. Select the **Infrastructure** view and then select the host or the pool that contains the SR.
2. Select the **Storage** tab.
3. Select the SR from the list and then select **Reclaim freed space**.

   NOTE:

   Reclaiming freed space is an intensive operation and can affect the performance of the storage array. Perform this operation only when space reclamation is required on the array. Citrix® recommends that you schedule this work outside the peak array demand hours.

4. Click **Yes** to confirm the operation. To view the status of this operation, select **Notifications** and then **Events**.

Related documentation

XenServer Current Release

- Manage storage repositories

Live LUN Expansion

To fulfill capacity requirements, you might need to add capacity to the storage array to increase the size of the LUN provisioned to your XenServer® host. Use live LUN Expansion to increase the size of the LUN and use the newly gained space without detaching the SR or taking the hosts or VMs offline.

WARNING:

It is not possible to shrink or truncate LUNs. Reducing the LUN size on the storage array can lead to data loss.

To expand the size of the LUN:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Add the extra storage to the storage array.
2. Select the **Infrastructure** view and then click the SR.
3. Click the **Storage** tab in the Properties pane.
4. Click **Rescan**. This operation rescans the SR and any extra capacity is added and made available.

Related documentation

XenServer Current Release

- Manage storage repositories

Corosync Upgrade Wizard

Overview

The upgrade wizard can be accessed from either the GFS2 Clustering tab or the Settings page.

Before you Start

The wizard first displays a summary of automated steps required to upgrade from Corosync 2 to Corosync 3.

1. Click **Show affected VMs** to view all impacted virtual machines.
2. Click **Show affected SRs** to view all impacted storage repositories.

Pre-Checks

The wizard automatically disables High Availability (HA) if it is currently enabled.

XenCenter performs each step automatically and displays progress in real time.

Before you continue, verify that the pre-checks have passed and that all affected virtual machines remain shut down.

When ready, click **Next** to start the upgrade process.

Upgrade process

During the upgrade, do not close XenCenter or restart any host. The Progress bar shows the status of each automated action.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After the upgrade completes, XenCenter displays a summary of the results and any actions performed during the process.

If the wizard disabled High Availability (HA) earlier, XenCenter re-enables it automatically once the upgrade finishes successfully.

Virtual machines then restart on the same hosts where they were running before shutdown. When you review the summary and confirm completion, click Finish to close the wizard.

If there are errors hit the **retry** button or Click **Finish** once the GFS2 storage is successfully upgraded to Corosync 3.

NOTE:

If HA was disabled by the wizard, it will only be re-enabled upon successful completion of the upgrade.

After the upgrade, VMs will restart on the same host they were running on prior to shutdown.

XenCenter RPU behavior during upgrade

When upgrading from XenServer 8.4 to a greater version, the Rolling Pool Upgrade (RPU) wizard performs additional checks based on Corosync status.

CASE	CONDITION	ACTION
1	Corosync 3 is active	Proceed with upgrade.
2	Corosync 2 is active, GFS2 clustering enabled but no SRs attached	Wizard allows disabling clustering via Disable GFS2 Clustering
3	Corosync 2 is active, GFS2 clustering enabled with SRs attached	Upgrade is blocked until Corosync 3 is installed

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Creating VMs

A virtual machine (VM) is a software container that runs on a host physical computer. The VM behaves as if it were a physical computer itself. VMs consist of an operating system plus CPU, memory (RAM) and networking resources, and software applications.

A template is a virtual machine encapsulated into a file, making it possible to rapidly deploy new VMs. Each template contains installation metadata. This metadata is the setup information needed to create a VM with a specific guest operating system, and with the optimum storage, CPU, memory, and virtual network configuration.

You can create VMs in XenCenter® in several different ways:

- The New VM wizard takes you step by step through the process of creating a VM from a template or a snapshot. This wizard enables you to configure the operating system, CPU, storage, networking, and other parameters.
- You can bypass the **New VM** wizard and create an *instant VM* based on a custom VM template that specifies all the required VM configuration parameters. You simply select your preconfigured template in XenCenter then right-click and select Instant VM from template. This mode of unattended VM installation can be useful for deploying large numbers of identical VMs.
- You can copy (or "clone") an existing VM.
- You can import a VM that has been previously exported.

XenServer® VM Tools

XenServer fully virtualizes VMs, enabling them to run at near-native processor speeds on virtualization-enabled hardware without requiring any modification to the guest operating system.

For Linux VMs, performance is further enhanced by utilizing x86 virtual container technologies in modern processors. These VMs use paravirtualized (PV) drivers built into the kernel for network and storage operations, providing efficient access in PV mode.

I/O drivers (also known as PV drivers) are essential for optimizing disk and network performance for both Windows and Linux VMs. It's recommended to install these drivers on all new VMs. For Windows VMs, you can manage driver updates through Windows Update, a setting configurable

© 1997–2026 Citrix Systems, Inc. All rights reserved.

when selecting a VM template in the **New VM** wizard in XenCenter. For details on enabling I/O driver updates through Windows Update, see Overview of VM creation steps.

The combination of I/O drivers and the Management Agent is collectively referred to as XenServer VM Tools. Key features such as VM migration and historical performance data tracking are available only when these tools are installed. For detailed installation steps, see Installing XenServer VM Tools.

Using templates

Several different templates are supplied with the XenServer server. These templates contain all the various configuration settings needed to install a specific guest operating system on a new VM. You can also create your own customized templates configured with the appropriate guest operating system, memory, CPU, storage and network settings, and use them to create VMs. See Guest OS support for a list of the templates/operating systems supported at this release, and for detailed information about the different install mechanisms on Windows and Linux.

You can view the XenServer templates supplied with the product and any custom templates that you create in the **Resources** pane.



- XenServer template



- Custom template

You can control whether to display the XenServer and Custom templates in the **Resources** pane:

- In the XenCenter Navigation pane, select **Infrastructure**.

  This panel displays a tree view of your managed resources in the **Resources** pane.
- To display standard XenServer VM templates: on the **View** menu, select **XenServer Templates**. To hide XenServer templates, select again to remove the check mark.
- To show custom VM templates: on the **View** menu, select **Custom Templates**. To hide custom templates, select again to remove the check mark.

Related documentation

XenServer Current Release

- VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Creating a New VM

The **New VM** wizard takes you through the process of creating a new virtual machine (VM), step-by-step. To start the **New VM** wizard, on the toolbar, click **New VM**.

Alternatively, do one of the following:

- Press **Ctrl+N**.
- On the **VM** menu, click **New VM**.
- Select a server in the **Resources** pane, right-click and then click **New VM** on the shortcut menu.

Using the wizard, you can configure the new VM exactly the way you want it, adjusting various configuration parameters for CPU, storage, and networking resources. Depending on the VM template you choose on the first page of the wizard, you see slightly different VM configuration options presented on subsequent pages. The installation options presented are tailored for each guest operating system. Click **Help**, or press **F1** on any wizard page for more information on what to do.

In XenServer environments where Role-Based Access Control (RBAC) is implemented, the **New VM** wizard checks that you have a role with sufficient permissions to create VMs. If your RBAC role does not have sufficient permissions, for example, a VM Operator or Read-only role, you cannot continue with VM creation. For more information, see RBAC overview.

Overview of VM creation steps

The **New VM** wizard takes you through the following steps to create a VM:

1. Select a VM template.

   To begin, choose a suitable VM template. Templates contain the setup information to create a VM with a specific guest operating system, and with the optimum storage, CPU, memory, and virtual network configuration. Various different templates are supplied, and you can add custom templates of your own. For more information, see Template and BIOS options.

   When selecting a built-in Windows template, you have the option to manage I/O driver updates for XenServer VM Tools via Windows Update by enabling or disabling the **Allow Windows Update to deliver I/O drivers** checkbox.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For custom templates or snapshots, the **New VM** wizard displays the current value of the `has-vendor-device` field. This field must be set to true to allow delivery of PV drivers through Windows Update.

> **NOTE:**
>
> If you intend to use your Windows VM as a Citrix Provisioning target or with the reset-on-boot flag enabled, you cannot use any of the automated update mechanisms. In such cases, ensure that the **Allow Windows Update to deliver I/O drivers** checkbox is disabled. For more information, see Settings for Citrix Provisioning targets or reset-on-boot machines.

2. Give the new VM a name.

   Next, you give the new VM a name and, optionally, a description. VM names are not checked for uniqueness within XenCenter, so it makes it easier for you to manage different VMs if you give them meaningful, memorable names. For more information, see VM name and description.

3. Specify the operating system installation media, boot mode, and whether to attach a vTPM.

   Windows operating systems can be installed from an ISO library, from install media in a physical DVD/CD drive or from network boot. Linux operating systems can be installed from a network install repository, an ISO library, or from install media in a physical DVD/CD drive.

   You can now allow some guest operating systems to boot in UEFI mode. For more information, see OS installation media.

   For Windows 11 VMs, you must attach a vTPM. The option **Create and attach a new vTPM** is selected and cannot be unselected. For other VM operating systems that support vTPM, you can choose whether to select **Create and attach a new vTPM**. The vTPM provides a TPM 2.0 compliant API to applications in the VM. TPM 1.2 is not supported.

4. Choose a home server.

   This step is optional, but you can choose a home server for the new VM. XenServer always attempts to start the VM on the nominated home server if it can. For more information, see Home server. If you have assigned a home server to the VM and later assign the VM to a group, the home server takes priority.

5. Configure the VM group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can choose to put the VM in a group. Groups affect where the VM is placed when it is started, resumed, or evacuated from a host. The home server setting has higher priority than the placement rules of the group. You can choose an existing group or create a new group by clicking **New VM group...**. For more information, see VM group.

6. Configure CPU and memory.

   - **For Windows VMs**: You can assign virtual CPUs (vCPUs) to the new VM, specify the number of cores per socket to present to the vCPUs, and allocate memory. These settings can be adjusted later, after the new VM has been created. For more information, see CPU and memory configuration.
   - **For Linux VMs**: You can assign a maximum number of vCPUs to the VM, specify the number of cores per socket to present to the vCPUs, set the initial number of vCPUs, and allocate memory. These settings can be adjusted later, after the new VM has been created. For more information, see CPU and memory configuration.
   - For all VMs, ensure cores per socket is a power of 2. If it is not, you might experience unexpected behaviors. For more information, see Known issues.
   - The number of vCPUs must be divisible by the number of cores per socket.

7. Assign a graphics processing unit (GPU).

   The **New VM** wizard prompts you to assign a dedicated GPU or one or more virtual GPUs to the VM. This feature enables the VM to use the processing power of the GPU, empowering high-end 3D professional graphics applications such as CAD/CAM, GIS, and Medical Imaging applications. For more information, see GPU.

   NOTE:

   GPU Virtualization is available for XenServer Premium Edition customers. For more information, see About XenServer Licensing.

8. Configure storage.

   The next step is to configure virtual disks for the new VM. The wizard automatically configures a minimum of one virtual disk and the template you select might include more. For more information, see Virtual disk configuration.

9. Configure networking.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The last step in the process of provisioning a new VM is to configure networking. You can configure up to four virtual network interfaces on each VM. For more information, see Configure virtual network interfaces.

10. Complete new VM creation.

    On the final page of the wizard, you can review all the configuration options you have chosen. Select the Start VM automatically check box to have the new VM start automatically when it is created.

Related documentation

XenServer Current Release

- VMs

VM Template and BIOS Options

Various different VM templates are supplied with the XenServer® server. These templates can be used in different ways to create VMs. Each template contains installation metadata: the information used to create a VM with a specific guest OS with the optimum storage, CPU, memory, and virtual network configuration.

For a full list of guest operating systems that XenServer supports, see Guest operating system requirements.

You can also create your own customized templates configured with the appropriate guest operating system, memory, CPU, storage, and network settings. For more information, see Creating new templates.

Select a BIOS option

XenServer VMs can be BIOS-generic or BIOS-customized:

BIOS-generic: the VM has generic XenServer BIOS strings;

BIOS-customized: VMs support customization of the BIOS in two ways, namely: Copy-Host BIOS strings and User-Defined BIOS strings.

- Copy-Host BIOS Strings: The VM has a copy of the BIOS strings of a particular server in the pool.
- User-Defined BIOS Strings: The user can set custom values in selected BIOS strings using CLI/API.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If a VM does not have BIOS strings set when it starts, the standard XenServer BIOS strings are inserted into it, and the VM becomes BIOS-generic.

For more information, refer to Advanced VM information.

When you create a VM using the **New VM** wizard, you can copy the BIOS strings from an OEM server in the same pool into the new VM. This action enables you to install Reseller Option Kit (BIOS-locked) OEM versions of Windows on the VM later, if needed. The OEM server from which you copy the BIOS strings is nominated as the home server for the new VM.

BIOS-customized VMs can be migrated, imported, and exported to servers with the same BIOS strings and to servers with different BIOS strings.

IMPORTANT:

It is your responsibility to comply with any EULAs governing the use of any BIOS-locked operating systems that you install.

Related documentation

XenServer Current Release

- VMs

VM Name and Description

Enter the name of the new VM in the **Name** box. You can choose any name you like, but a descriptive name is best. Although it is advisable to avoid having multiple VMs with the same name, it is not a requirement. XenCenter® does not enforce any uniqueness constraints on VM names.

You can more easily manage different VMs if you give them meaningful names. For example, include one of the following pieces of information in the VM name:

- The operating system of the VM (Windows 10 64-bit)
- The application software on the VM (XenServer Web Self-Service v1.0 (Build 9057))
- The role of the VM (`db-server`, Outlook Server, Test).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

It is not necessary to use quotation marks for names that include spaces.

You can also include a longer description of the VM on this page of the wizard (optional).

Related documentation

XenServer Current Release

- VMs

OS Installation Media

The options for OS installation media and boot mode available on the **Installation Media** page of the **New VM** wizard depend on the OS or template that you selected on the first page of the wizard.

OS installation media options

Install from ISO library or DVD drive

Templates: Windows and Linux guests

Select **Install from ISO library or DVD drive** and then choose an ISO image or a DVD drive from the list.

If the ISO image you want to use is not listed here, click **New ISO library** and create an ISO SR using the **New Storage Repository** wizard. After creating the ISO SR, you can select it from the list of available ISO libraries here.

If there are no ISO images listed here, you need to make the ISOs available to the server by creating an external NFS or SMB/CIFS share directory.

Boot from network

Templates: Windows and Linux guests

Select this option to use PXE/network booting for guests.

Selecting this option places the network at the top of the boot order for the new VM.

Boot mode

Choose a boot mode for the VM. Specify the boot mode when you create a VM. It is not possible to change the boot mode after booting the VM for the first time.

- Select **BIOS Boot** to boot the VM in legacy BIOS mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Select **UEFI Boot** to boot the VM in UEFI mode.
- Select **UEFI Secure Boot** to boot the VM in UEFI Secure Boot mode.

The most secure boot mode is selected by default. You can only select those boot options that are available to your new VM.

UEFI boot and UEFI Secure Boot are supported only on certain operating systems. For more information, see Guest UEFI boot and Secure Boot.

vTPM

You can attach a vTPM to UEFI boot mode guests by using the option **Create and attach a new vTPM**.

- A vTPM is required for a Windows 11 VM. The option is selected and cannot be unselected. If you are upgrading from Windows 10 to Windows 11, attach a vTPM to your Windows 10 VM before upgrading the operating system to Windows 11.
- The vTPM provides a TPM 2.0 compliant API to applications in the VM. TPM 1.2 is not supported.

For more information, see vTPM.

Related documentation

XenServer Current Release

- VMs

Home Server

A home server is the server which provides the resources for a VM in a pool. When you nominate a home server for a VM, XenServer® always attempts to start up the VM on that server if it can. If XenServer cannot start the VM on that server, an alternate server within the same pool is selected automatically.

- To nominate a home server for the VM in the **New VM** wizard, select **Place the VM on this server** and choose a server from the list.
- If you do not want to nominate a home server, click **Don't assign this VM a home server**. The VM uses the resources on the most suitable available server.

If you are creating a BIOS-customized VM, the OEM server from which you copy the BIOS strings is automatically selected as the home server for the new VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can change the home server configuration for a VM from the VM's Properties dialog box; see Change VM properties.

Workload Balancing (WLB) and Virtual GPU considerations

The following section lists scenarios when the home server nomination does not take effect:

- In pools with Workload Balancing (WLB) enabled, the nominated home server is not used for starting, restarting, resuming, or migrating the VM. Instead, WLB nominates the best server for the VM by analyzing XenServer resource pool metrics and by recommending optimizations.
- If a VM has one or more virtual GPUs assigned to it, the home server nomination does not take effect. Instead, the server nomination is based on the virtual GPU placement policy set by the user. For more information, see GPU Placement Policy.

Related documentation

XenServer Current Release

- VM placement

VM Group

You can assign your VMs to VM groups that are started on hosts in your pool according to the placement rules of the group. The available placement types are "anti-affinity" and "normal".

VM groups with normal placement do not have any special behavior.

VM groups with anti-affinity placement have the following rules:

1. No single host is the only place all VMs in a particular group are running.
2. The count of VMs within the group for each host is as even as possible.

When a VM in a VM group with anti-affinity placement rules is started or evacuated from a host, XenServer® chooses to place the VM on a host that enables the VM group to follow these anti-affinity placement rules as closely as possible. If the VM start or host evacuate cannot be done without breaching the placement rules, XenServer prioritizes completing the action over following the placement rules.

If the anti-affinity rules are breached, you receive an alert. Alerts are generated if all the running VMs in an anti-affinity group reside on a single host. If this changes, the alert is cleared. This alert is not generated if only one of the VMs in the group is running or no VMs in the group are running. For more information, see XenCenter Alerts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In the following scenarios the VM group placement rules do not take effect:

- In pools with Workload Balancing (WLB) enabled, the VM group is not used for starting, restarting, resuming, or migrating the VM. Instead, Workload Balancing nominates the best server for the VM by analyzing XenServer resource pool metrics and by recommending optimizations. These recommendations can cause the VM anti-affinity rules to be breached.
- If the VM has a home server defined, this setting takes priority over the VM group setting.

Considerations when using VM groups:

- Only 5 anti-affinity groups per pool are supported.
- When you clone a VM that is in a VM group, the new VM is not added to the same VM group. You must explicitly set the VM group for the new VM.
- If you revert a VM to a previous snapshot, the VM retains its current VM group setting. This setting does not change to the value it had when you took the snapshot.
- Exporting a VM does not retain the VM group setting. If you import this VM again, it is not added to a VM group. You must explicitly set the VM group for the imported VM.

In the **New VM** wizard on the **VM group** tab, you can select the VM group to add the VM to. This tab also gives the option to create a new group. You can add a VM to only one VM group.

After VM creation, you can change a VM's group in one of the following places:

- In the **Resources** pane of XenCenter®, you can right-click on a VM and choose **Assign to VM group**. The submenu shows the available VM groups and also gives you the option to create a new VM group. The current VM group for the VM is marked with a check.
- In the **Resources** pane of XenCenter, you can right-click on the pool and choose **Manage VM groups**. For more information, see Manage VM groups.
- In the XenCenter main menu, you can select **VM > Assign to VM group**. The submenu shows the available VM groups and also gives you the option to create a new VM group. The current VM group for the VM is marked with a check.
- In the XenCenter main menu, you can select **Pool > Manage VM groups**. For more information, see Manage VM groups.

You can manage your VM groups in XenCenter by using the **Manage VM group** dialog box. For more information, see Manage VM groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- VM placement

VM CPU and Memory Allocation

When you create a VM, you can allocate virtual CPUs, specify how many cores-per-socket to present to the vCPUs, and set initial memory resources for the VM. You can change the settings at any time after the new VM is created.

Ensure cores-per-socket is a power of 2. If it is not, you might experience unexpected behaviors. For more information, see Known issues. The number of vCPUs must be divisible by the number of cores per socket.

The **vCPU hotplug** feature in XenCenter® enables customers to dynamically increase the number of vCPUs assigned to a running Linux VM, without having to restart the VM.

Options

Number of vCPUs

(for Windows VMs)

Enter the number of virtual CPUs (vCPUs) you would like to allocate to the new VM.

To get the best performance out of the VM, the number of vCPUs assigned to the VM mustn't exceed the number of physical CPUs on the server.

NOTE:

This value can be changed later, if needed. For more information, see Change VM properties: CPU and memory. For information about the maximum number of vCPUs supported on a VM, see the XenServer Configuration Limits.

Maximum number of vCPUs

(for Linux VMs)

Select the maximum number of virtual CPUs (vCPUs) you would like to allocate to the new VM from the menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To get the best performance out of the VM, the number of vCPUs assigned to the VM mustn't exceed the number of physical CPUs on the server.

NOTE:

This value can be changed later, if needed. For more information, see Change VM properties: CPU and memory.

Topology

Specify the topology for the vCPU.

By default, XenServer® allocates one core per socket for each vCPU. For example, allocating 4 vCPUs appear as 4 sockets with 1 core per socket. Click the **Topology** menu to change this setting and choose an option from the list.

Ensure cores-per-socket is a power of 2. If it is not, you might experience unexpected behaviors. For more information, see Known issues. The number of vCPUs must be divisible by the number of cores per socket.

NOTE:

The cores-per-socket setting depends on the number of sockets present on the server and the operating system installed. Some operating systems have restrictions on the number of CPUs. Comply with the operating system requirements when setting this option.

Initial number of vCPUs

(for Linux VMs)

This option displays the initial number of vCPUs allocated to the VM. By default, this number is equal to the Maximum number of vCPUs set in the previous step. You can choose from the list and modify the initial number of vCPUs allocated to the VM.

Memory

Enter the amount of memory you want to allocate to the VM.

The XenServer templates provide typical VM configurations and set reasonable defaults for the memory, based on the type of guest operating system. The following considerations can affect how much memory you decide to initially allocate to a new VM:

- The kinds of applications that run on the VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Other virtual machines that use the same memory resource.
- Applications that run on the server alongside the virtual machine.

You can adjust the memory allocation after the new VM is created on the VM's **CPU and Memory** tab. On this tab, you can also enable Dynamic Memory Control (DMC) to allow dynamic reallocation of memory between VMs in the same pool. For more information, see Configuring VM memory.

VM power state scenarios

The following table lists the three VM power states and describes their various vCPU scenarios.

VM POWER STATE	MAXIMUM NUMBER OF VCPUS	INITIAL NUMBER OF VCPUS	CURRENT NUMBER OF VCPUS
Running	Cannot be increased/decreased	N/A	Can only be increased.
Shutdown	Can be increased/ decreased	Can be increased/ decreased	N/A
Suspended	Cannot be modified	N/A	Cannot be modified

Related documentation

XenServer Current Release

- VMs

GPU

XenCenter allows you to assign a dedicated graphics processing unit (GPU) or one or more virtual GPUs to a new VM during VM creation. This feature enables a VM to use the processing power of the GPU, providing better support for high-end 3D professional graphics applications. For example, CAD/CAM, GIS, and Medical Imaging applications.

For detailed information, see Configuring graphics.

XenServer supports Intel's virtual GPU: a graphics acceleration solution that requires no additional hardware. It uses the Intel Iris Pro functionality embedded in some processors, and utilizes a standard Intel GPU driver installed within the VM. The motherboard must have a chipset which

© 1997–2026 Citrix Systems, Inc. All rights reserved.

enables GPU functionality, for example, C226 for Xeon E3 v4 CPUs or C236 for Xeon v5 CPUs. For information about supported processors, refer to the XenServer Hardware Compatibility List.

The following table lists whether GPU pass-through, shared GPU (vGPU), and multiple shared GPU (vGPU) are supported for guests:

NOTE:

You can add multiple vGPUs to a VM if your NVIDIA GPU supports this feature and the vGPUs are of the same type.

	GPU PASS-THROUGH FOR WINDOWS VMS	GPU PASS-THROUGH FOR LINUX VMS	SHARED GPU (VGPU) FOR WINDOWS VMS	SHARED GPU (VGPU) FOR LINUX VMS	MULTIPLE SHARED GPU (VGPU) FOR WINDOWS VMS	MULTIPLE SHARED GPU (VGPU) FOR LINUX VMS
AMD	YES					
Intel	YES		YES (deprecated)			
NVIDIA	YES	YES	YES	YES	YES	YES

You might need a vendor subscription or a license depending on the graphics card used.

When you click **Add**, the **GPU type** list displays available GPUs, supported virtual GPU types, resolution, and the maximum number of displays per virtual GPU. Select a GPU or a virtual GPU type from the list to add a GPU or a virtual GPU to the VM.

If you are using the virtual GPU feature, select **Pass-through whole GPU** to allow a VM to use the full processing power of the GPU. The GPU or virtual GPU selection can be modified later, if necessary. For more information, see Change VM Properties.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- GPU Pass-through and Graphics Virtualization are only available for XenServer Premium Edition customers. For more information, see About XenServer Licensing.
- There is no licensing restriction to use NVIDIA GPU pass-through for Linux VMs.
- When you allocate a GPU to Linux VMs, the **GPU type** list displays all GPU types available on the host or the pool. However, only NVIDIA GPU pass-through is supported for Linux VMs.

Enabling Intel GPU pass-through

XenServer supports the GPU pass-through feature for Windows VMs using an Intel integrated GPU device. This feature is supported on Haswell (Xeon E3-12xx v3) or newer CPUs that contain an Intel integrated GPU device and have a graphics-capable chipset. For more information on the supported hardware, refer to the XenServer Hardware Compatibility List.

When using an Intel GPU on Intel servers, the XenServer® server control domain (dom0) have access to the integrated GPU device. In such cases, the GPU is not available for pass through. To use the Intel GPU pass-through feature on Intel servers, disable the connection between dom0 and the GPU before passing through the GPU to the VM.

To disable the connection:

1. Select the XenServer host on the **Resources** pane.
2. On the **General** tab, click **Properties** and then click **GPU** on the left pane.
3. In the **Integrated GPU pass-through** section, click **This server will not use the integrated GPU**.

   This setting disables the connection between dom0 and the Intel integrated GPU device.
4. Click **OK**.
5. Reboot the XenServer server for the changes to take effect.

   The Intel GPU is now visible on the GPU type list during new VM creation and on the VM's **Properties** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The XenServer host's external console output (for example, VGA, HDMI, DP) will not be available after disabling the connection between dom0 and the GPU.

Related documentation

XenServer Current Release

- VMs
- Graphics

Virtual Storage Configuration

Virtual machines created using the **New VM** wizard have at least one virtual disk and the selected VM template might also include extra virtual disks. A VM can have up to seven virtual disks including a virtual CD-ROM.

From the **Storage** page in **New VM** wizard, you can:

- Add more virtual disks
- Remove virtual disks
- Change the size and location of virtual disks

Options

Use these virtual disks

Select this option to use the virtual disks listed.

- To add more virtual disks, click **Add** and specify the name, size and location (SR); see Add virtual disks.
- To delete a virtual disk, click **Delete**.
- To move a virtual disk to a different SR, select it in the list and click **Properties**, then choose an SR from the **Location** list.
- To make a virtual disk bigger or smaller, select it in the list and click **Properties**, then enter a new value in the **Size** box.
- To change the name or description of a virtual disk, select it in the list and click **Properties**, then enter the new text.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use storage-level fast disk clone

This check box appears if any of the virtual disks in the template or snapshot you are using to create the VM are on the same SR. Select the check box to use hardware-level cloning features for copying the disks from the template/snapshot to the new VM. Using storage-level fast disk clone enables you to quickly create VMs.

This option is only supported for VMs using remote NFS shared storage or local VHD-based storage.

Create a diskless VM that boots from the network

If you selected the **Boot from network** option on the OS Installation media page earlier in the wizard, you can select this option to make the new VM a diskless VM.

Related documentation

XenServer Current Release

- VMs

Virtual Networking Configuration

You can configure up to 4 virtual network interfaces from the **Networking** page of the **New VM** wizard. To configure more than 4, go to the VM's **Networking** tab after it has been created and add them from there.

By default, an automatically created random MAC address is used for all virtual network interfaces. To enter a different MAC address, click **Properties**. Enter a new address in the **Virtual Interface Properties** dialog box, using hexadecimal characters in the form `aa:bb:cc:dd:ee:ff`.

- To add a new virtual network interface, click **Add**.
- To remove a virtual network interface, select it in the list and then click **Delete**.
- To change the virtual disk's physical network, MAC address or quality-of-service (QoS) priority, select it and then click **Properties**. For more information, see Change virtual network interface properties.

You can use the **Networking** tab to change the VM's virtual networking configuration later, if necessary. For more information, see Configuring VM networking.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- VMs

Complete New VM Creation

On the last page of the **New VM** wizard, choose **Start VM automatically** to ensure the new VM starts up automatically when it is installed.

The process of creating the VM might take some time. The time it takes depends on the size of the template and the speed and bandwidth of the network connection between the destination server and XenCenter. You can view the progress on the status bar and on the **Events** view under **Notifications**.

After creating a VM, install XenServer VM Tools to ensure optimized I/O performance. For more information, see Installing XenServer VM Tools.

Related documentation

XenServer Current Release

- VMs

Express (unattended) VM Creation

You can create multiple identical VMs based on a custom VM template by bypassing the **New VM** wizard and using the **Quick Create** feature in XenCenter®:

1. Create a custom VM template that specifies all the configuration parameters you want for your new VMs. For more information, see Creating new templates.
2. Choose your custom template in the **Resources** pane. On the **Templates** menu, point to **Create VM From Selection** and then choose **Quick Create**. Alternatively, right-click in the **Resources** pane and choose **Quick Create** on the shortcut menu.

The new VM is then created and provisioned using all the configuration settings specified in your template.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- VMs

Creating New Templates

You can create custom templates in several different ways in XenCenter®:

- By copying an existing template; see Copying VMs and templates.
- By converting an existing VM into a new template.
- By saving a copy of a VM snapshot as a new template.
- By importing a template that has previously been exported from an existing template or VM snapshot as an XVA file.

To convert an existing VM into a template

When you create a template using this method, the VM's disks are copied to the new template and the original VM no longer exists. A VM that is currently in a vApp cannot be converted into a template.

1. Shut down the VM as described in Shutdown a VM.
2. In the **Resources** pane, select the VM, right-click and then select **Convert to Template**.
3. Click **Convert** to confirm. You can view the conversion progress in the status bar at the bottom of the XenCenter window and on the **Events** view under **Notifications**.

When conversion is complete, the VM disappears from the **Resources** pane and reappears as a new custom template. The new custom template can then be used to create VMs in the same way as any other template.

To save a copy of a snapshot as a new template

1. On the **Snapshots** tab, select the snapshot, right-click and then select **Create Template from Snapshot** on the shortcut menu.
2. Enter the name of the new template and then click **OK**.

After the template is successfully created, it appears as a custom template in the **Resources** pane and on the **Templates** page in the **New VM** wizard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To import a template from an XVA file

VM templates and snapshots that have been exported as XVA files can be imported into XenCenter using **Import** wizard:

1. On the **File** menu, select **Import**
2. Select the XVA file containing the template on the first page of the wizard
3. Follow the same steps as when importing a VM from XVA

For more information, see Import VMs from XVA.

The import progress is displayed on the status bar at the bottom of the XenCenter window and also on the **Events** view under **Notifications**. The import process can take some time, depending on the size of the template and the speed and bandwidth of the network connection between XenCenter and the server. When the newly imported template is available, it appears in the **Resources** pane as a custom template. The new template has the same configuration properties as the original exported template. To change its configuration properties, use the template's **Properties** window.

Export a Template to a File

When you export a custom template, it is saved in an XVA file in the location of your choice. This file contains a complete copy of the template (including disk images). You can then import the template and use it to create a VM in the same or in a different resource pool.

To export a template to a file

1. In the **Resources** pane, select the template.
2. On the **Templates** menu, select **Export to File...**. Alternatively, right-click on the template and choose **Export to File...** from the context menu.
3. On the page **Export File Details** of the wizard, enter the XVA file name and browse to locate the folder where you want to create the file. Click **Next** to continue.
4. On the **Finish** page, review the settings you have selected. To have XenCenter verify the exported package, select the **Verify export on completion** check box. Then select **Finish** to begin the export.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- VMs

Copying VMs and Templates

You can create VMs and templates by copying (cloning) an existing VM or a template. XenCenter® enables you to copy VMs and templates within and across pools.

XenServer® has two mechanisms for copying VMs and templates, full copy or fast clone:

- **Full copy** makes a complete copy of the VM's disks.
- **Fast clone** (Copy-on-Write) writes only modified blocks to disk. This feature uses hardware-level cloning features for copying the disks from the existing VM to the new VM. This mode is only supported for file-backed VMs. Copy-on-Write is designed to save disk space and allow fast clones, but can slightly slow down normal disk performance.

Copying a VM

IMPORTANT:

- Before copying a Windows VM, use the Windows utility Sysprep to ensure the uniqueness of the Security IDs (SIDs). Copying a VM without first taking the recommended system preparation steps can lead to duplicate SIDs and other problems. For information about cloning VMs and running Sysprep, see Prepare to clone a Windows VM by using Sysprep.
- If the VM you want to copy is a Windows VM, run the Sysprep utility.
- If the VM is running, you must shut it down before you can copy it.
- A VM created by copying an existing VM is not added to the same VM group as the original VM.

To copy a VM within the pool

1. Select the VM in the **Resources** pane, and on the **VM** menu, select **Copy VM**.
2. On the **Destination** page, select **Within Pool**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Name and Storage** page, enter the name of the new VM and (optionally) a meaningful description.
4. Select the Copy Mode: **Fast clone** or **Full copy**.
5. If you choose **Full copy** as the copy mode, select the storage repository (SR) where you want to copy the VM's virtual disks. If you are moving a VM from local to shared storage, make sure that you select a shared SR here.
6. Select **Finish**.

To copy a VM to a different pool

1. Select the VM in the **Resources** pane, and on the **VM** menu, select **Copy VM**.
2. On the **Destination** page, select **Cross-pool**. and select **Next**
3. Select a standalone server or a pool from the **Destination** menu.
4. Select a server from the **Home Server** list to assign a home server for the VM and select **Next**
5. On the **Storage** page, specify the storage repository on which to place the virtual disks of the copied VM and select **Next**.
   - The **Place all migrated virtual disks on the same SR** option is selected by default and displays the default shared SR on the destination pool.
   - Select **Place migrated virtual disks onto specified SRs** to specify an SR from the **Storage Repository** menu. This option allows you to select different SR for each virtual disk on the migrated VM.
6. On the **Networking** page, map the virtual network interfaces in the VM to networks in the destination pool or server. Specify your options using the **Target Network** menu and select **Next**.
7. Select a storage network on the destination pool to use for the live migration of the VM's virtual disks. Select **Next**.

   NOTE:

   Due to performance reasons, it is recommended that you do not use the management network for copying VMs.

8. Review the configuration settings and select **Finish** to start copying the VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Copying a template

To copy a template within the pool

1. Select the template in the **Resources** pane, and on the **Templates** menu, select **Copy Template**.
2. On the **Destination** page, select **Within Pool**.
3. **Name and Storage** page, enter the name of the new template and a meaningful description.
4. Select the Copy Mode: **Fast clone** or **Full copy**.
5. If you choose **Full copy** as the copy mode, select the SR where the copied virtual disks are placed.
6. Select **Finish.**

To copy a template to a different pool

1. Select the template in the **Resources** pane, and on the **Templates** menu, select **Copy**.
2. On the **Destination** page, select **Cross-pool** and select **Next**.
3. Select a standalone server or a pool from the **Destination** menu.
4. Select a server from the **Home Server** list to assign a home server for the VM and select **Next**
5. On the **Storage** page, specify a storage repository on which to place the virtual disks of the copied template and select **Next**.
    - The **Place all migrated virtual disks on the same SR** option is selected by default and displays the default shared SR on the destination pool.
    - Select **Place migrated virtual disks onto specified SRs** to specify an SR from the **Storage Repository** menu. This option allows you to select different SR for each virtual disk on the migrated VM.
6. On the **Networking** page, map the virtual network interfaces in the selected template to networks in the destination pool or server. Specify your options using the **Target Network** menu and select **Next**.
7. Select a storage network on the destination pool or server to use to copy the template's virtual disks. Select **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> Due to performance reasons, it is recommended that you do not use the management network for copying VMs.

8. Review the configuration settings and select **Finish** to start copying the template.

Related documentation

XenServer Current Release

- VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring VMs

- Installing XenServer VM Tools
- VM memory configuration
- VM storage configuration
  - Add virtual disks
  - Attach virtual disks
  - Detach virtual disks
  - Move virtual disks
  - Delete virtual disks
  - Change virtual disk properties
- VM networking configuration
  - Add a virtual network interface
  - Activate/deactivate a virtual network interface
  - Remove a virtual network interface
  - Change virtual network interface properties
- Configuring Virtual GPU
- Change VM properties

Installing XenServer® VM Tools

XenServer VM Tools (formerly Citrix VM Tools or XenServer PV Tools) provide high performance I/O services without the overhead of traditional device emulation.

XenServer VM Tools for Windows

XenServer VM Tools for Windows consist of I/O drivers (also known as paravirtualized drivers or PV drivers) and the Management Agent.

The I/O drivers contain storage and network drivers, and low-level management interfaces. These drivers replace the emulated devices and provide high-speed transport between Windows and the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenServer product family software. While installing a Windows operating system, XenServer uses traditional device emulation to present a standard IDE controller and a standard network card to the VM. This emulation allows the Windows installation to use built-in drivers, but with reduced performance due to the overhead inherent in emulating the controller drivers.

The Management Agent, also known as the Guest Agent, is responsible for high-level virtual machine management features and provides a full set of functions to XenCenter.

Get the XenServer VM Tools for Windows installer from the XenServer downloads page.

The version of the XenServer VM Tools for Windows is updated independently of the version of XenServer. For more information about the latest version of the tools, see What's New.

Install the latest version of XenServer VM Tools for Windows on each Windows VM for that VM to have a fully supported configuration, and to be able to use the xe CLI or XenCenter. A VM functions without the XenServer VM Tools for Windows, but performance is hampered when the I/O drivers are not installed. Install XenServer VM Tools for Windows on Windows VMs to be able to perform the following operations:

- Cleanly shut down, reboot, or suspend a VM
- View VM performance data in XenCenter
- Migrate a running VM (using live migration or storage live migration)
- Create snapshots with memory (checkpoints) or revert to snapshots

For more information, see Install XenServer VM Tools for Windows.

XenServer VM Tools for Linux

XenServer VM Tools for Linux contain a guest agent that provides extra information about the VM to the host.

Get the XenServer VM Tools for Linux installer from the XenServer downloads page.

Install the XenServer VM Tools for Linux on Linux VMs to be able to perform the following operations:

- View VM performance data in XenCenter.

  For example, the following memory performance values are visible in XenCenter only when the XenServer VM Tools are installed: "Used Memory", "Disks", Network" and "Address".
- In XenCenter, view the Linux guest operating system information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In the XenCenter **Networking** tab, view the IP address of the VM.
- Launch an SSH Console to the VM from XenCenter.
- Adjust the number of vCPUs on a running Linux VM.
- Enable Dynamic Memory Control (DMC).

> **NOTE:**
>
> Some Linux guest operating systems do not support memory ballooning with the Xen® hypervisor, and as such cannot use the Dynamic Memory Control (DMC) feature. For information on what guest operating systems this applies to, see Guest OS Feature Support.

For more information, see Install XenServer VM Tools for Linux.

> **IMPORTANT:**
>
> To have a supported configuration when running a VM, ensure that you install XenServer VM Tools. While a Windows VM can function without them, performance is hampered when the I/O drivers are not installed. Run Windows VMs with these drivers to be supported. Some features, such as live relocation across physical hosts, are available only with the I/O drivers installed and active.

Finding out the virtualization state of a VM

XenCenter reports the virtualization state of a VM on the VM's **General** tab. You can see whether XenServer VM Tools (I/O drivers and the Management Agent) are installed, and whether the VM can install and receive updates from Windows Update. The following section lists the messages displayed in XenCenter:

I/O optimized (not optimized) - displays whether the I/O drivers are installed on the VM.

Management Agent installed (not installed) - displays whether the latest version of the Management Agent is installed on the VM.

Able to (Not able to) receive updates from Windows Update - specifies whether the VM is able to receive I/O drivers from Windows Update.

Install I/O drivers and Management Agent - indicates that the VM does not have the I/O drivers or the Management Agent installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you have many VMs on your server or a pool, select the server or pool on the Resources pane and select the **Search** tab. From the **Saved Searches** list, select **VMs without XenServer VM Tools Installed**. This search displays a list of VMs that do not have XenServer VM Tools installed.

Updating XenServer VM Tools

XenServer has a simpler mechanism to automatically update I/O drivers (PV drivers) and the Management Agent for Windows VMs. This mechanism enables customers to install updates as they become available.

The **Virtualization state** section on a VM's **General** tab specifies whether the VM is able to receive updates from Windows Update. You can enable I/O driver updates through Windows Update when selecting a VM template in the **New VM** wizard in XenCenter. For details on enabling I/O driver updates through Windows Update, see Overview of VM creation steps. If you do not want to receive I/O driver updates from Windows Update, disable Windows Update on your VM, or specify a group policy.

IMPORTANT:

- If you are currently using the 8.2.x.x drivers or earlier and want to use the Management Agent MSI file to update to the latest version of the drivers, you must use Device Manager to uninstall the 8.2.x.x drivers from your VM before installing these drivers. If you do not complete this step, the MSI install process fails.
- We recommend that you snapshot your VM before installing or updating the XenServer VM Tools.
- Ensure that all requested VM restarts are completed as part of the update. Multiple restarts might be required. If all requested restarts are not completed, this update might result in unexpected behavior.

Updating the I/O drivers

You can get I/O driver updates automatically from Microsoft Windows Update, provided:

- You have created a Windows VM using XenCenter issued with XenServer 7.0 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Windows Update is enabled within the VM
- You have access to the internet, or are able to connect to a WSUS proxy server

NOTE:

Customers can also receive I/O driver updates automatically through the automatic Management Agent update mechanism. See *Updating the Management Agent* for details.

Updating the Management Agent

XenServer enables you to automatically update the Management Agent on both new and existing Windows VMs. By default, XenServer allows the automatic updating of the Management Agent. However, it does not allow the Management Agent to update the I/O drivers automatically. You can customize the Management Agent update settings during XenServer VM Tools installation. For more information, see Install XenServer VM Tools for Windows. The automatic updating of the Management Agent occurs seamlessly, and does not reboot your VM. In scenarios where a VM reboot is required, XenCenter issues notification to users about the required action.

To update the Management Agent automatically:

- You must have installed XenServer VM Tools issued with XenServer 7.0 or later
- The Windows VM must be connected to the internet

Related documentation

XenServer Current Release

- XenServer VM Tools for Windows
- Linux VMs

Configuring Virtual Storage

Storage on XenServer® VMs is provided by virtual disks. A virtual disk is a persistent, on-disk object that exists independently of the VM to which it is attached. Virtual disks are stored on XenServer Storage Repositories (SRs), and can be attached, detached, and reattached to the same or different VMs when needed. New virtual disks can be created at VM creation time (from within the **New VM** wizard). They can also be added after the VM has been created from the VM's **Storage** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual disks on VMs with XenServer VM Tools installed can be *hot plugged*. That is, you can add, delete, attach, and detach virtual disks without having to shut down the VM first. VMs without XenServer VM Tools installed must be shut down before you carry out any of these operations. To avoid this situation, install XenServer VM Tools on all virtual machines. For more information, see XenServer VM Tools.

On the VM's **Storage** tab in XenCenter®, you can:

- Add new virtual disks.
- Configure virtual disks - change a virtual disk's size, location, read/write mode, and other configuration parameters.
- Attach existing virtual disks to the VM.
- Detach virtual disks - preserving the virtual disk and all the data on it.
- Move a virtual disk to a specified storage repository.
- Delete virtual disks - permanently destroying the disk and any data stored on it.

Related documentation

XenServer Current Release

- VMs

Add Virtual Disks

To add a new virtual disk, use the **Add Virtual Disk** dialog box.

IMPORTANT:

If the VM is running without XenServer VM Tools installed, shut it down before you can add any virtual disks. To avoid this situation, install XenServer VM Tools on all virtual machines. For more information, see XenServer VM Tools.

Procedure:

1. Open the **Add Virtual Disk** dialog box by doing any of the following:
   - Select the VM or storage repository in the **Resources** pane, select the **Storage** tab and then select **Add**.
   - On the **Storage** menu, select **Virtual Disks** and then **New Virtual Disk**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On the **Storage** page of the **New VM** wizard, select **Add**.

2. Enter the name of the new virtual disk and, optionally, a description.
3. Enter the size of the new virtual disk. Ensure that the storage repository (SR) on which the virtual disk is to be stored has sufficient space for the new virtual disk.
4. Select the SR where the new virtual disk is stored.
5. Click **Create** to add the new virtual disk and close the dialog box.

Related documentation

XenServer Current Release

- VMs

Attach Virtual Disks

You can add storage to a VM by attaching an existing virtual disk.

1. Select the VM in the **Resources** pane, select the **Storage** tab, and then select **Attach**. Alternatively, on the **Storage** menu, select **Virtual Disks** then **Attach Virtual Disk**.
2. Select a virtual disk from the list.
3. To set access to the virtual disk to read-only, select the **Attach as read-only** check box. This setting can help prevent data from being overwritten or changed when multiple VMs access the disk. It also allows you to attach the virtual disk to many VMs. To allow write access to the virtual disk, clear the check box.
4. Click **Attach**.

> **TIP:**
>
> Problems on an underlying SR can sometimes cause an attached virtual disk to become deactivated ("unplugged"). If this situation happens, activate it again from the VM's **Storage** tab by selecting it and clicking **Activate**.

Related documentation

XenServer Current Release

- VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Detach Virtual Disks

When you detach a virtual disk from a VM, the virtual disk and the data on it are preserved. The virtual disk is no longer available to the VM. The detached storage device can later be reattached to the same VM, attached to a different VM, or moved to a different storage repository (SR).

You can detach a virtual disk without shutting down the VM (*hot unplug*) if the following conditions are met:

- The VM is not suspended.
- The VM must have XenServer® VM Tools installed.
- The virtual disk is not a system disk.
- The virtual disk must be deactivated to be able to detach it cleanly. The term *deactivate* is equivalent to *unplug*, which is the term used for this operation in the product documentation and in the CLI.

If any of these conditions are not satisfied, shut the VM down before you can detach the virtual disk.

To detach the virtual disk:

1. Select the VM in the **Resources** pane and click the **Storage** tab.
2. Select the virtual disk in the list, click **Deactivate**, and click **Detach**.
3. Click **OK** to confirm the operation.

Related documentation

XenServer Current Release

- VMs

Move Virtual Disks

Virtual disks can be moved or migrated from one storage repository (SR) to a different SR within the same pool. The following types of virtual disks can be moved or migrated:

- Virtual disks that are not currently attached to any VM.
- Virtual disks attached to VMs that are not running.
- Virtual disks attached to running VMs (using storage live migration)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You can move a virtual disk on local storage to shared storage on a different server, but you cannot move it to a local storage on a different server.

About storage live migration

Storage live migration allows you to move virtual disks without having to shut down the VM first, enabling administrative operations such as:

- Moving a VM from cheap local storage to fast, resilient, array-backed storage.
- Moving a VM from a development environment to a production environment.
- Moving between tiers of storage when a VM is limited by storage capacity.
- Performing storage array upgrades.

Virtual disks with more than one snapshot cannot be migrated.

To move a virtual disk

1. In the XenCenter® **Resources** pane, select the SR where the virtual disk is stored, and then select the **Storage** tab. To locate a virtual disk:
   - In the XenCenter **Resources** pane, select the VM to which the virtual disk that you want to move is attached.
   - Click the **Storage** tab and identify the SR on which the virtual disk is stored.
2. From the **Virtual Disks** list, select one or more virtual disks that you would like to move, and then select **Move**. Alternatively, right-click on the selected virtual disk and select **Move Virtual Disk** from the shortcut menu.
3. In the **Move Virtual Disk** dialog box, select the target SR that you would like to move the virtual disk to. Make sure that the target SR has sufficient space for another virtual disk: the available space is shown in the list of available SRs.
4. Click **Move** to move the virtual disk.

Related documentation

XenServer Current Release

- VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Delete Virtual Disks

You can delete a virtual disk without shutting down the VM first if the following conditions are met:

- The VM is not suspended.
- The VM must have XenServer® VM Tools installed.
- The virtual disk is not a system disk.
- The virtual disk must be deactivated first. The term *deactivate* is equivalent to *unplug*, which is the term that is used for this operation in the product documentation and in the CLI.

If any of these conditions are not satisfied, shut the VM down before you can delete the virtual disk.

IMPORTANT:

Deleting a virtual disk permanently deletes the disk, destroying any data stored on it.

To delete the virtual disk:

1. On the VM's **Storage** tab, select the virtual disk in the list and select **Deactivate** and then **Delete**.
2. Click **OK** to confirm the deletion.

Related documentation

XenServer Current Release

- VMs

Change Virtual Disk Properties

To change the properties of a virtual disk, select the VM's **Storage** tab, then select the virtual disk and select **Properties**.

General properties - name, description, folder, tags



PROPERTY	DESCRIPTION
Name	The virtual disk name
Description	A description of the virtual disk (optional)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PROPERTY	DESCRIPTION
Folder	The name of the resource folder where the virtual disk is located, if applicable.
Tags	A list of tags that have been applied to this virtual disk.

Custom fields



On the **Custom Fields** tab you can assign new custom fields to a virtual disk, change the value of existing custom fields, and remove custom fields.

For information on adding, setting, modifying, and deleting custom fields, see Using custom fields.

Disk size and location



Set the size of the virtual disk on this tab and select the storage repository where the virtual disk is located.

Device options



The final tab on the virtual disk **Properties** dialog box allows you to set some device options for the virtual disk.

OPTION	DESCRIPTION
Mode	The disk read/write permissions of a virtual disk can be changed. For example, change this setting to prevent data from being overwritten on a virtual disk that you use for backup purposes.
Device position	The position to use for this virtual disk in the drive sequence.
Disk access priority	For some virtual disks, you can adjust the disk I/O priority. This setting is only available for virtual disks on storage repositories that are LVM-based: local, shared iSCSI, or hardware HBA. This option is visible only after the disk

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPTION	DESCRIPTION
	scheduler is changed to `cfq`. It is not available by default. For more information, see Manage storage repositories.

Related documentation

XenServer Current Release

- VMs

Configuring VM Networking

Each virtual machine (VM) can have one or more virtual network interfaces that act as virtual NICs.

A virtual network interface has the following properties:

PROPERTY	DESCRIPTION
Network	The (physical) network location of the virtual network interface.
MAC address	The MAC address of the virtual network interface.
QoS limit	An optional I/O priority Quality of Service (QoS) setting for maximum network transfer rate. When memory resources are low, using I/O throttling in this way slows the memory processing and helps make the system more stable by preventing crashes.

All the virtual network interfaces for a VM are listed on the VM's **Networking** tab. Here, you can add new virtual network interfaces. You can also edit, activate, deactivate, and remove existing virtual network interfaces.

- Networking
- Add a Virtual Network Interface
- Activate/deactivate a Virtual Network Interface
- Remove a Virtual Network Interface

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Change Virtual Network Interface Properties

Add a Virtual Network Interface

You can add up to seven Virtual Network Interfaces (VNIs) for a VM. For more information about the maximum number of VNIs supported for a VM, see the XenServer Configuration Limits.

1. Open the **Add Virtual Interface** dialog box by doing one of the following:
   - Select the VM in the **Resources** pane. Go to the **Networking** tab. Click **Add Interface**.
   - On the **Network** page of the **New VM** wizard, click **Add**.
2. Select a network location from the **Network** list.
3. Specify the MAC address.
   - To use a generated MAC address, select **Auto-generate a MAC address**.
   - To explicitly enter a MAC address, select **Use this MAC address**. Enter an address in the form XY:XX:XX:XX:XX:XX where X is any hexadecimal digit, and Y is one of 2, 6, A or E.
4. To set an optional I/O priority Quality of Service (QoS) setting for maximum network transfer rate, select the check box and enter a value in kilobytes per second (kB/s).
5. Click **Add**.

Related documentation

XenServer Current Release

- VMs

Activate/deactivate a Virtual Network Interface

You can activate or deactivate a virtual network interface on a running VM when the VM meets the following conditions:

- The VM is not suspended.
- The VM must have XenServer® VM Tools installed.

To activate ("plug") or deactivate ("unplug") a virtual network interface:

1. On the VM's **Networking** tab, select the interface.
2. Click the button labeled **Activate** or **Deactivate**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- VMs

Remove a Virtual Network Interface

You can remove a virtual network interface from a VM without shutting down the VM ("hot unplug") if the VM meets the following conditions:

- The VM is not suspended.
- The VM must have XenServer® VM Tools installed.

If one or both of these conditions are not satisfied, shut the VM down before you can remove the virtual network interface.

To remove a virtual network interface:

1. Select the VM in the **Resources** pane.
2. Select the **Networking** tab.
3. On the **Networking** tab, choose the virtual network interface in the list. Click **Remove**.

Related documentation

XenServer Current Release

- VMs

Change Virtual Network Interface Properties

To change properties of a virtual network interface, open the **Virtual Interface Properties** dialog box by doing one of the following:

- Click the VM's **Networking** tab, then select the virtual network interface and click **Properties**.
- On the **Network** page of the **New VM** wizard, click **Edit**.

You can change the network location and MAC address of a virtual network interface, and you might also be able to set its I/O priority.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PROPERTY	DESCRIPTION
Network	The network location of the virtual network interface.
MAC address	The MAC address of the virtual network interface. You can autogenerate this value or enter it manually in the form XY:XX:XX:XX:XX:XX where X is any hexadecimal digit, and Y is 2, 6, A or E.
Enable QoS limit	Select this option and enter a value in kilobytes per second (kB/s) to set an optional I/O priority Quality of Service (QoS) setting for maximum network transfer rate. When memory resources are low, using I/O throttling in this way slows the memory processing and helps make the system more stable by preventing crashes.

Related documentation

XenServer Current Release

- VMs

Configuring Virtual GPU

GPUs are grouped based on the types of virtual GPUs supported on a particular GPU. XenCenter enables you to modify the virtual GPU types allowed per GPU, and group the GPUs based on your requirements. For more information, see GPU.

To modify the virtual GPU types allowed on a particular GPU:

1. Select the Pool in the **Resources** pane and select the **GPU** tab.
2. If you have selected a pool, select GPUs that you would like to modify using the check boxes located beside the GPU. Remember, each horizontal bar on the GPU tab represents a physical GPU.
3. Click **Edit Selected GPUs**. The GPU window displays a list of virtual GPU types. It contains information specific to each virtual GPU type. This information includes: the number of virtual GPUs allowed per GPU, maximum resolution, maximum number of displays per virtual GPU, and the Video RAM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Modify the selection based on your requirements and select **OK**. If you would like to pass-through the whole GPU, select **Pass-through whole GPU**.

Related documentation

XenServer Current Release

- VMs
- Graphics

Configuring VM Memory

When a VM is first created, it is allocated a fixed amount of memory. To improve the utilization of physical memory in your XenServer® environment, you can use Dynamic Memory Control (DMC). DMC is a memory management feature that enables dynamic reallocation of memory between VMs.

The **Memory** tab in XenCenter® shows memory usage and configuration information for your VMs and servers.

- For servers, the total available memory and the current memory usage are shown, and you can see how memory is divided between hosted VMs.
- For VMs, in addition to current memory usage you can also see the VM's memory configuration information. That configuration includes whether DMC is enabled and the current dynamic minimum and maximum values. You can edit DMC configuration settings in this tab.

VMs with the same memory configuration are grouped in the **Memory** tab, enabling you to view and configure memory settings for individual VMs and for groups of VMs.

NOTE:

Some Linux guest operating systems do not support memory ballooning with the Xen® hypervisor, and as such cannot use the Dynamic Memory Control (DMC) feature. For information on what guest operating systems this applies to, see Guest OS Feature Support.

Dynamic Memory Control (DMC)

Dynamic memory control (sometimes known as *dynamic memory optimization*, *memory overcommit*, or *memory ballooning*) works by automatically adjusting the memory of running VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DMC keeps the amount of memory allocated to each VM between specified minimum and maximum memory values
- DMC guarantees performance
- DMC permits greater density of VMs per server

Without DMC, if you start further VMs when a server is full, the action fails with "out of memory" errors. To reduce the existing VM memory allocation and make room for more VMs, you must edit each VM's memory allocation and then reboot the VM. With DMC enabled, XenServer attempts to reclaim memory by automatically reducing the current memory allocation of running VMs within their defined memory ranges.

Dynamic and static memory range

For each VM, you can set a dynamic memory range. This dynamic memory range is the range within which memory can be added or removed from the VM without requiring a reboot. You can adjust the dynamic range while the VM is running, without having to reboot it. XenServer always guarantees to keep the amount of memory allocated to the VM within the dynamic range. For example, if the Dynamic Minimum Memory is 512 MB and the Dynamic Maximum Memory is 1,024 MB, the VM has a Dynamic Memory Range of 512–1,024 MB. The VM operates within this range. With DMC, XenServer guarantees to always assign each VM memory within its specified DMR.

When host memory is plentiful, all running VMs receive their Dynamic Maximum Memory level. When host memory is scarce, all running VMs receive their Dynamic Minimum Memory level. If new VMs are required to start on *full* servers, running VMs have their memory *squeezed* to start new ones. The required extra memory is obtained by squeezing the existing running VMs proportionally within their pre-defined dynamic ranges.

Many operating systems that XenServer supports do not fully support dynamically adding or removing memory. As a result, the XenServer server must declare the maximum amount of memory that a VM can be asked to consume when the VM starts. The guest operating system can use this information to size its page tables and other memory management structures accordingly. This feature introduces the concept of a static memory range within the XenServer product. The static memory range cannot be adjusted while the VM is running. The dynamic range is constrained such as to be always contained within this static range until the VM is next rebooted. The static minimum is there to protect the administrator. Set the static minimum to the lowest amount of memory that the OS can run with on a XenServer server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

We advise you not to change the static minimum level as this value is set at the supported level per operating system. By setting a static maximum level higher than a dynamic max, you can allocate more memory to a VM in the future without requiring a reboot.

DMC memory constraints

XenCenter enforces the following constraints when setting DMC values:

- The minimum dynamic memory value cannot be lower than the static minimum memory value.
- The minimum dynamic memory value cannot be greater than the maximum dynamic memory value.
- The maximum dynamic memory value cannot be greater than the maximum static memory value.
- The minimum dynamic memory must be at least 75% of the static maximum. A lower amount can cause in-guest failures and is not supported.

You can change a VM's memory properties to any values that satisfy these constraints, subject to validation checks. In addition to these constraints, we support only certain VM memory configurations for specific operating systems.

To enable DMC

1. Choose a VM or server in the **Resources** pane and select the **Memory** tab.
2. Select the **Edit** button for the VM or group of VMs you want to configure.
3. For multiple VMs with the same current memory configuration, choose the VMs you want to configure and click **Next**.
4. Select the **Automatically allocate memory within this range** option.
5. Set the required maximum and minimum dynamic memory range values by using the slider or by typing the values directly.
6. Click **OK** to apply the changes and close the dialog box.

To disable DMC

1. Choose the VM or server in the **Resources** pane and select the **Memory** tab.
2. Select the **Edit** button for the VM or group of VMs you want to configure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. For multiple VMs with the same current memory configuration, choose the VMs you want to configure and click **Next**.
4. Select the **Set a fixed memory** option.
5. Specify the amount of memory to allocate.
6. Click **OK** to apply the changes and close the dialog box.

Related documentation

XenServer Current Release

- VM memory

View VM Properties

The **General** tab for a VM has the following sections and information:

General

The **General** section of the **General** tab shows the following information:

- **Name**: The name you gave to this VM.
- **Description**: The description you gave to this VM.
- **Tags**: Any tags you assigned to the VM.
- **Folder**: Any folders you assigned to the VM.
- **Operating System**: The operating system that is running in this VM.
- **BIOS strings copied**: Whether BIOS strings have been copied to this VM.
- **NUMA optimization**: Whether or not NUMA has been enabled on this VM and the number of nodes it applies to.
- **vApp**: The vApp that the VM is part of, if any.
- **VM group**: The VM group that the VM is part of, if any.
- **Home Server**: The home server associated with this VM.
- **UUID**: The unique identifier of this VM.

The **Virtualization & VM Tools** section of the **General** tab shows the following information:

- **Virtualization mode**: The virtualization mode of the VM.
- **Virtualization state**: Whether the XenServer® VM Tools are installed in the VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Management Agent version**: The management agent version (Windows VMs).
- **VM Tools version**: The version of XenServer VM Tools installed (Linux VMs).
- **Installed drivers and versions**: Lists the drivers installed on the VM along with their version numbers.

Boot Options

The **Boot Options** section of the **General** tab shows the following information:

- **Boot order**: Which devices this VM boots from and in what order.
- **Boot mode**: Whether the VM is UEFI or BIOS boot mode.
- **Secure boot certificates**: The status of the Secure Boot certificates in the VM (for UEFI Secure Boot enabled VMs).

CPUs

The **CPUs** section of the **General** tab shows the following information:

- **Virtual CPUs**: The number of virtual CPUs currently assigned to this VM.
- **Max number of CPUs**: (Linux VMs only) The maximum number of vCPUs that can be assigned to this VM.
- **Topology**: The socket topology for this VM.

Read Caching

The **Read Caching** section of the **General** tab shows the following information:

- **Status:** Whether the VM is using read caching.
- **Reason:** Why the VM is or isn't using read caching.

Device Security

The **Device Security** section of the **General** tab shows the following information:

- **Trusted Platform Module**: Whether a vTPM is attached to this VM.

Updates

The **Updates** section of the **General** tab shows the following information:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Pending recommended tasks**: Any actions that must be taken to get full effectiveness from all applied updates.

Change VM Properties

Select a virtual machine in the **Resources** pane. On the **General** tab, select the **Properties** button to view or change the properties of the VM.

General



On the **General Properties** tab you can change the VM's name and description, place it in a folder, and manage its tags.

- To change the VM name, enter a new name in the **Name** box.
- To change the VM description, enter the new text in the **Description** box.
- To place the VM in a folder or to move it to a different folder, click **Change** in the **Folder** box and choose a folder. For more information, see Using folders.
- To tag and untag the VM and to create and delete tags, see Using tags.

Custom fields



Custom fields allow you to add information to managed resources to make it easier to search and organize them. For more information, see Using custom fields.

CPU and memory



On the **CPU and memory** tab, you can adjust the number of virtual CPUs allocated to the VM, set cores-per-socket for the vCPU, and specify the vCPU priority. Shut down the VM before you modify these settings.

Ensure cores-per-socket is a power of 2. If it is not, you might experience unexpected behaviors. For more information, see Known issues. The number of vCPUs must be divisible by the number of cores per socket.

Number of vCPUs (for Windows VMs)

To modify the number of virtual CPUs allocated to the VM, change the number in the **Number of vCPUs** list. To get the best performance out of your VM, ensure the number of vCPUs does not exceed the number of physical CPUs on its host server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Maximum number of vCPUs (for Linux VMs)

To modify the maximum number of virtual CPUs allocated to the VM, change the number in the **Maximum Number of vCPUs** list. To get the best performance out of your VM, ensure the maximum number of vCPUs does not exceed the number of physical CPUs on its host server.

Topology

By default, XenCenter® allocates one core per socket for each vCPU. The **Topology** list displays valid cores-per-socket combinations. Select an option from the list to modify this setting.

Depending on the number of vCPUs you select, XenCenter displays a list of options where the number of vCPUs is divisible by the number of cores per socket. For example, if you specify 8 vCPUs for your VM, the number of cores per socket can only be 1, 2, 4, or 8.

Current number of vCPUs (for Linux VMs)

This list displays the current number of vCPUs allocated to the VM. You can increase the number of vCPUs allocated to the VM even when the VM is running by choosing the required number of vCPUs from the list.

NOTE:

Shut down the VM to decrease the number of vCPUs allocated to the VM.

vCPU priority for this virtual machine

vCPU priority is the priority given to each of the VM's vCPUs during host CPU scheduling, relative to the other VMs running on the same host server. To adjust the vCPU priority for the VM, move the vCPU slider.

The XenServer® templates provide typical VM configurations and set reasonable defaults for the memory, based on the type of guest operating system. Consider the following factors when deciding how much memory you give to a VM:

- The kinds of applications that run on the VM.
- Other virtual machines that use the same memory resource.
- Applications that run on the server alongside the virtual machine.

Boot options



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The available boot options on this tab can vary, depending on the guest operating system. For example, on some VMs, you can change the boot order (or boot sequence), or specify extra boot parameters.

- To change the boot order, select an item in the **Boot Order** list and select **Move Up** or **Move Down**.
- To specify extra boot parameters, enter them in the **OS Boot parameters** box. For example, on a Debian VM, you can enter single to boot the VM in single-user mode.

Start options



On this tab you can adjust the **start order**, the start delay interval, and the **HA restart priority** for the selected VM.

Start order

Specifies the order in which individual VMs are started up within a vApp or during a high availability recovery operation, allowing certain VMs to be started before others. VMs with a start order value of 0 (zero) are started first, then VMs with a start order value of 1, and so on.

Attempt to start next VM after

This value is a delay interval that specifies how long to wait after the VM starts before starting the next group of VMs in the startup sequence. This setting applies to VMs within a vApp and to individual VMs during a high availability recovery operation.

HA restart priority

In a pool with high availability enabled, this setting specifies which VMs are restarted automatically if the underlying hardware fails or their host server is lost.

- VMs with an HA restart priority of **Restart** are guaranteed to be restarted if sufficient resources are available within the pool. They are restarted before VMs with a **Restart if possible** priority.
- VMs with an HA restart priority of **Restart if possible** are not considered when calculating a failure plan. However, one attempt to restart them is made if a server that is running them fails. This restart is attempted after all higher-priority VMs are restarted, and if the attempt to start them fails, then it will not be retried.
- VMs with an HA restart priority of **Do not restart** are not restarted automatically.

For more information, see VM startup settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alerts



On the **Alerts** tab, you can configure performance alerts for the VM's CPU usage, network, and disk activity.

For information about configuring alerts, see Configuring performance alerts.

Home server



On the **Home Server** tab of the VM **Properties** dialog box you can nominate a server which provides resources for the VM. The VM is started up on that server if possible. If it is not possible to start eh VM on that server, an alternate server within the same pool is selected automatically. For more information, see Creating a new VM.

In pools with Workload Balancing (WLB) enabled, you cannot set a home server. Instead, XenCenter nominates the best server for the VM by analyzing XenServer resource pool metrics and recommending optimizations. You can decide if you want these recommendations geared towards resource performance or hardware density. You can fine-tune the weighting of individual resource metrics (CPU, network, memory, and disk) so that the placement recommendations and critical thresholds align with your environment's needs.

GPU



On the VM's **GPU** properties tab, you can assign a dedicated graphics processing unit (GPU) or one or more virtual GPUs to a VM. This configuration gives the VM direct access to the graphics hardware. The VM can use the processing power of the GPU, providing better support for high-end 3D professional graphics applications such as CAD/CAM, GIS, and Medical Imaging applications.

NOTE:

You can add multiple vGPUs to a VM if your NVIDIA GPU supports this feature and the vGPUs are of the same type.

Click **Add** to add a GPU to the VM. The **GPU type** list displays available GPUs and virtual GPU types. Select a virtual GPU type from the list to assign a specific virtual GPU type to the VM. Alternatively, select **Pass-through whole GPU** to allow a VM to use the full processing power of the GPU.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

GPU Virtualization is available for XenServer Premium Edition customers. For more information about licensing, see About XenServer Licensing.

USB



On the VM's **USB** properties tab, the right side pane displays the list of USBs attached to the VM. You can attach extra (maximum of 6) USBs to the VM. You can also choose to detach USBs from the VM.

For more information, see Tabs.

NOTE:

- USB pass-through is available for XenServer Premium Edition customers.
- USB pass-through is supported for the following USB versions: 1.1, 2.0, and 3.0.

Related documentation

XenServer Current Release

- VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Managing VMs

- Start a VM
- Suspend and resume a VM
- Shut down a VM
- Reboot a VM
- Run a remote console session
- Migrate VMs
- Delete VMs
- Changed Block Tracking
- Secure Boot Certificates

Start a VM

For VMs in a pool, you can choose where to start your VMs. This choice is subject to available resources on the selected host server. Your choice of server depends on how the VM and the pool are configured:

- In a pool with Workload Balancing (WLB) enabled, recommendations are provided to help you choose the best possible physical server for the VM's workload.
- In a pool without Workload Balancing configured, you start the VM on any server in the pool (subject to available storage on that server). For more information, see Creating a new VM.

When the VM is up and running, its status indicator changes to the **VM running** icon in the **Resources** pane.



To start a VM on a specific server

1. Select the VM in the **Resources** pane.
2. Right-click and select **Start on Server** and then select the server you want on the shortcut menu. Alternatively, on the **VM** menu, select **Start on Server** and then select the server you want on the submenu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To start the VM on the optimal or home server

Select the VM in the **Resources** pane and then select **Start** on the Toolbar.



Alternatively, do one of the following:

- Right-click in the **Resources** pane and select **Start** on the shortcut menu.
- On the **VM** menu, select **Start**.

In a WLB-enabled pool, this action starts the VM on the optimal server.

In a pool without Workload Balancing configured, this action starts the VM on its home server. If no home server has been set, the VM starts on the first available server.

Related documentation

XenServer Current Release

- VMs

Suspend and Resume a VM

When you suspend a VM, its current state is stored in a file on the default storage repository (SR). This feature allows you to shut down the VM's host server. After rebooting the server, you can resume the VM and return it to its original running state.

NOTE:

It might not be possible to resume a suspended VM that was created on a different type of server. For example, a VM created on a server with an Intel VT-enabled CPU might not be resumed on a server with an AMD-V CPU.

To suspend a VM

1. If the current default SR is detached, select a new default SR.
2. Select the VM in the **Resources** pane and then select **Suspend** on the Toolbar.

   Alternatively:

   - Right-click and select **Suspend** on the shortcut menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On the **VM** menu, select **Suspend**.

When a VM has been suspended, its status indicator changes to the Suspended VM icon in the **Resources** pane.



To resume a suspended VM

For VMs in a pool, you can normally choose where to resume them. Your choice of server depends on how the VM and the pool are configured:

- In a pool with Workload Balancing (WLB) enabled, recommendations are provided to help you choose the best possible physical server for the VM's workload.
- In a pool without Workload Balancing configured, you can resume the VM on any server in the pool (subject to available storage on that server). For more information, see Home server.

When a suspended VM has been successfully resumed, its status indicator changes to the **VM Running** icon in the **Resources** pane.



To resume a suspended VM on a specific server

1. Select the VM in the **Resources** pane.
2. Right-click and select **Resume on Server** and then select the server you want on the shortcut menu. Alternatively, on the **VM** menu, select **Resume on Server** and then select the server you want on the submenu.

To resume the VM automatically on the optimal or home server

Select the VM in the **Resources** pane and then select **Resume** on the toolbar.



Alternatively, do one of the following:

- Right-click in the **Resources** pane and select **Resume** on the shortcut menu.
- On the **VM** menu, select **Resume**.

In a WLB-enabled pool, the VM starts on the optimal server.

In a pool without Workload Balancing configured, the VM starts on its home server. If no home server has been set or if the nominated server is unavailable, the VM starts on the first available server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- VMs

Shut Down a VM

You might need to shut down a running VM for several different reasons. For example:

- to free up its resources
- to reconfigure its virtual network hardware
- to reconfigure its virtual disk storage

You can shut down a VM via the VM's console or using XenCenter. XenCenter provides two ways to shut down a VM:

- A soft shutdown performs a graceful shutdown of the VM, and all running processes are halted individually.
- A forced shutdown performs a hard shutdown and is the equivalent of unplugging a physical server. It might not always shut down all running processes and you risk losing data if you shut down a VM in this way. Only use a forced shutdown when a soft shutdown is not possible.

A VM running without XenServer VM Tools installed, can only be shut down using a forced shutdown. To avoid this situation, install XenServer VM Tools on all virtual machines. For more information, see XenServer VM Tools.

To perform a soft shutdown

Select the VM in the **Resources** pane and then choose **Shut Down** on the toolbar.



Alternatively:

- Right-click and click **Shut Down** on the **Resources** pane shortcut menu.
- On the **VM** menu, click **Shut Down**.

To shut down a VM from within its floating console window, click the lifecycle icon and then click **Shut Down**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The VM's console displays shutdown messages as running processes are stopped. When the shutdown is complete, the VM status indicator in the **Resources** pane changes to the stopped VM icon.



To perform a forced shutdown

Select the VM in the **Resources** pane and then click **Force Shutdown** on the toolbar.



Alternatively:

- Right-click and click **Force Shutdown** on the **Resources** pane shortcut menu.
- On the **VM** menu, click **Force Shutdown**.

To forcibly shut down a VM from within its floating console window, click the lifecycle icon and then click **Force Shut Down**.



When the shutdown is complete, the VM status indicator changes to the stopped VM icon in the **Resources** pane.



Related documentation

XenServer Current Release

- VMs

Reboot a VM

There are two different ways of rebooting a VM in XenCenter®:

- A soft reboot performs an orderly shutdown and restart of the VM.
- A forced reboot is a hard reboot which restarts the VM without first performing any shut-down procedure. This action works like pulling the plug on a physical server and then plugging it back in and turning it back on.

Only do a forced reboot as a last resort to forcibly retrieve the system from instances such as a critical error.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A VM without XenServer VM Tools installed can only be rebooted using a forced reboot. To avoid this situation, install XenServer VM Tools on all virtual machines. For more information, see XenServer VM Tools.

To reboot a VM cleanly

In the **Resources** pane, select the VM and then select **Reboot** on the toolbar.



Alternatively:

- Right-click and select **Reboot** on the **Resources** pane shortcut menu.
- On the **VM** menu, select **Reboot**.

The VM is shut down and rebooted. When this process is complete, its status indicator in the **Resources** pane changes back to the **VM start** icon.



To do a forced reboot

In the **Resources** pane, select the VM and then select **Force Reboot** on the toolbar.



Alternatively:

- Right-click and select **Force Reboot** on the **Resources** pane shortcut menu.
- On the **VM** menu, select **Force Reboot**.

The VM is immediately shut down and rebooted. When this process is complete, its status indicator in the **Resources** pane changes back to the **VM start** icon.



Related documentation

XenServer Current Release

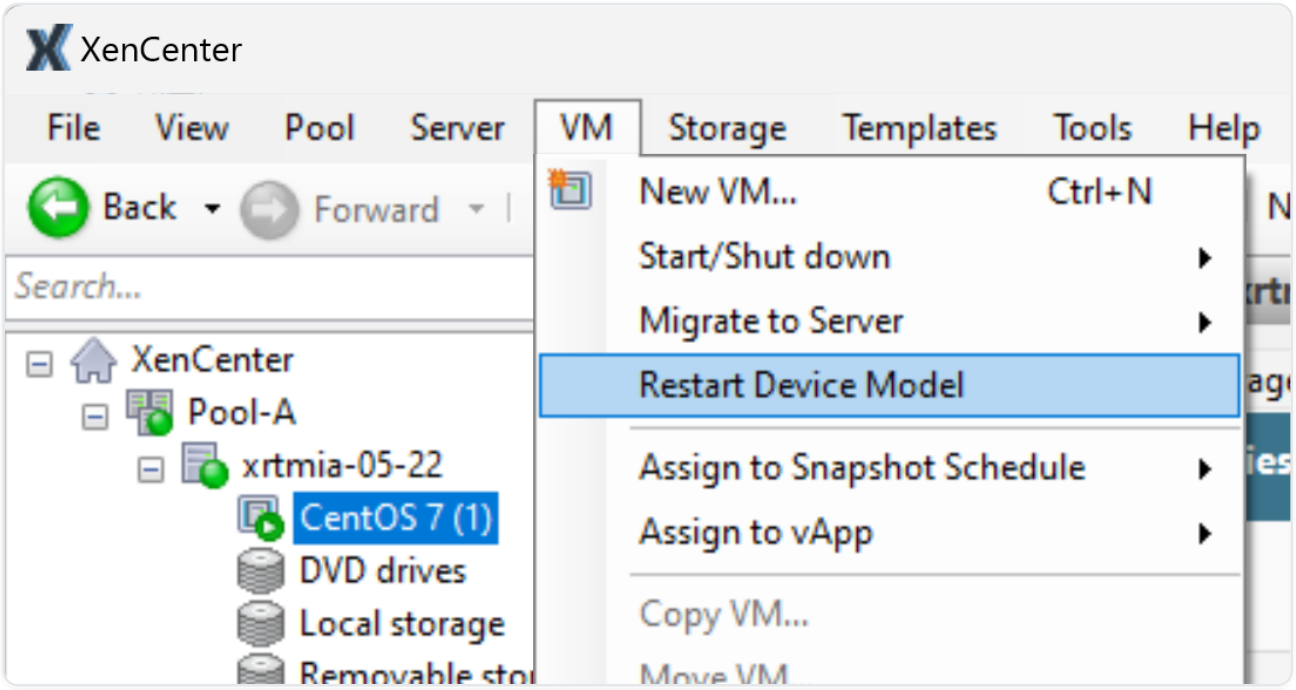
- VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Restart the VM device model

The **Restart device model** option enables you to restart the device model of a VM or VMs. Restarting the device model can enable the VM to benefit from fixes and improvements included in an update.

To restart the device model



1. Select the VM or VMs in the **Resources** pane.
2. On the **VM** menu, click **Restart device model**.
3. Click **Yes** to confirm.

While the device model restarts, the VM shows a yellow triangle icon in the **Resources** pane (). You cannot stop, start, or migrate the VM during this time.

Run a Remote Console Session

To open a remote console session on a VM, select the VM and then select the Console tab.

Linux VMs

You can run a graphical console session on Linux VMs or initiate an SSH connection to the VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

For Linux guests, screen blanking can take effect after a period of inactivity (typically 10 minutes). When screen blanking happens, the console is black and remains blank until a key is pressed at which point the text reappears.

You can disable this behavior within the guest by adding `consoleblank=0` to the kernel boot parameters.

SSH console

XenCenter allows you to initiate SSH connections to Linux VMs using the **Open SSH Console** button on the VM's Console tab. This action launches an SSH console for the VM in an external pop-up window. The SSH console also allows you to copy/paste content to and from the VM's console. To use the SSH console feature, you must:

- Ensure that the VM and XenCenter® are accessible on the same network
- Install the Linux guest agent on the VM. For more information about installing the Linux Guest agent, see Linux VMs.
- Verify that the SSH daemon is running on the VM and accepts remote connections

NOTE:

When you close the SSH console, any operations that are still running in the console are terminated.

Windows VMs

Console sessions on Windows VMs can use either the standard graphical console or a Remote Desktop console, both of which support full keyboard and mouse interactivity. The standard graphical console uses the in-built VNC technology that XenServer developed to provide remote access to your VM console. The Remote Desktop console uses RDP (Remote Desktop Protocol) technology. Switch between a standard graphic console and a Remote Desktop console by using the **Switch to Remote Desktop/Switch to Default Desktop** button on the XenCenter **Console** tab.

To use a Remote Desktop console connection, ensure that the following requirements are met:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Remote Desktop must be enabled on the virtual machine - see Windows VMs for information on how to enable Remote Desktop on a Windows virtual machine.
- XenServer® VM Tools must be installed.
- The virtual machine must have a network interface and be able to connect to XenCenter.
- The Credential Security Support Provider protocol (CredSSP) update must be applied to either both or neither of the client and server in the RDP connection. For more information, see `<https://support.microsoft.com/en-gb/help/4295591/credssp-encryption-oracle-remediation-error-when-to-rdp-to-azure-vm>`.

There are various different XenCenter settings that affect your Remote Desktop console environment:

- Windows Key combinations are sent to the Remote Desktop console.
- Sounds from applications running on the Remote Desktop console are played on your local computer.
- By default, when opening a Remote Desktop console session, a connection is made to the console session on the remote server instead of creating a virtual console session.
- XenCenter automatically scans for an RDP connection and can automatically switch to the Remote Desktop console when it becomes available.

You can change these and other Remote Desktop console settings via the **Console** tab in the XenCenter **Options** dialog box; see Changing XenCenter options.

NOTE:

You can enhance VNC performance by using XenCenter on the local machine rather than using RDP to connect to XenCenter.

Manage VM groups

You can assign your VMs to VM groups that are started on hosts in your pool according to the placement rules of the group. The available placement types are "anti-affinity" and "normal".

VM groups with normal placement do not have any special behavior.

VM groups with anti-affinity placement have the following rules:

1. No single host is the only place all VMs in a particular group are running.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. The count of VMs within the group for each host is as even as possible.

When a VM in a VM group with anti-affinity placement rules is started or evacuated from a host, XenServer® chooses to place the VM on a host that enables the VM group to follow these anti-affinity placement rules as closely as possible. If the VM start or host evacuate cannot be done without breaching the placement rules, XenServer prioritizes completing the action over following the placement rules.

If the anti-affinity rules are breached, you receive an alert. Alerts are generated if all the running VMs in an anti-affinity group reside on a single host. If this changes, the alert is cleared. This alert is not generated if only one of the VMs in the group is running or no VMs in the group are running. For more information, see XenCenter Alerts.

In the following scenarios the VM group placement rules do not take effect:

- In pools with Workload Balancing (WLB) enabled, the VM group is not used for starting, restarting, resuming, or migrating the VM. Instead, Workload Balancing nominates the best server for the VM by analyzing XenServer resource pool metrics and by recommending optimizations. These recommendations can cause the VM anti-affinity rules to be breached.
- If the VM has a home server defined, this setting takes priority over the VM group setting.

Considerations when using VM groups:

- Only 5 anti-affinity groups per pool are supported.
- When you clone a VM that is in a VM group, the new VM is not added to the same VM group. You must explicitly set the VM group for the new VM.
- If you revert a VM to a previous snapshot, the VM retains its current VM group setting. This setting does not change to the value it had when you took the snapshot.
- Exporting a VM does not retain the VM group setting. If you import this VM again, it is not added to a VM group. You must explicitly set the VM group for the imported VM.

Manage VM groups dialog

In this dialog, you can create, delete, and update VM groups.

You can open the **Manage VM group** dialog from one of the following places:

- In the **Resources** view, right-click on the pool and select **Manage VM Groups...**.
- In the XenCenter main menu, you can select **Pool > Manage VM groups**. For more information, see Manage VM groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The window lists the VM groups in your pool and for each of them shows:

- The user-defined group name
- The type of placement this group uses
- An optional description of the group
- The number of VMs in the group

Select a VM group to display the list of VMs in that group in the right panel.

Create a VM group

> **NOTE:**
>
> If you try to create more than 5 anti-affinity groups, XenCenter® displays a warning that this operation is not supported.

To create a new VM group:

1. In the **Manage VM group** dialog, click **New VM group**. The **New VM group** wizard opens.
2. In the **Name** panel, specify the following:

   - The **Name** for the VM group.
   - (Optional) A **Description** for the group.
   - The type of **Placement** to use. The option "anti-affinity" is selected by default.

   Click **Next**.
3. In the **Virtual Machines** panel, choose the VMs to add to the new group.

   If a VM is already a member of an existing group, XenCenter shows a warning that adding the VM to this group removes it from the existing group. A VM cannot be in more than one VM group. Click **Yes** to continue with this move and **No** to leave the VM in its current group.

   Click **Next** to continue.
4. In the **Finish** panel, review the settings you specified. If they are correct, click **Finish**.

Delete a VM group

To delete a VM group:

1. In the **Manage VM group** dialog, select the group you want to delete.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **Delete**.
3. XenCenter shows a warning that you are deleting a VM group. To confirm the deletion, click **Yes**.

If you delete a VM group that has VMs in it, the VMs are no longer associated with a group, but are not otherwise affected.

Update the properties of a VM group

1. In the **Manage VM group** dialog, select the group you want to edit.
2. Click **Properties**.
3. In the **Name** panel, you can update the **Name** and **Description** of the group. **Placement** cannot be updated.
4. In the **Virtual Machines** panel, you can add and remove VMs in the group.
5. Click **OK**.

Related documentation

XenServer Current Release

- VM placement

Migrate Virtual Machines

This topic contains information about migrating and moving virtual machines within and across pools and standalone servers.

Definitions:

- Migrate a VM: Move a running or a suspended VM to a different server or a pool.
- Move a VM: Move a shut-down VM to a different server or pool.

Live migration

Live migration is available in all versions of XenServer. This feature allows you to move a running or a suspended VM between XenServer servers, when the VM's disks are on storage shared by both servers. This capability allows for pool maintenance features such as Workload Balancing (WLB), high availability, and Rolling Pool Upgrade (RPU) to automatically move VMs. Storage can

© 1997–2026 Citrix Systems, Inc. All rights reserved.

only be shared between hosts in the same pool. As a result, you can move VMs only within the same pool.

During the live migration of a VM, its memory is transferred as a data stream between two hosts using the network. The migration stream compression feature compresses this data stream, speeding up the memory transfer on slow networks. This feature is disabled by default, but this can be changed by using XenCenter or the xe CLI. For more information, see Pool Properties - Advanced and Pool parameters.

Live migration enables the following to occur without any VM downtime:

- Workload leveling
- Infrastructure resilience
- Upgrade of the server software

Storage live migration

Storage live migration allows a VM to be moved from one host to another when the VMs's disks are not on storage shared between the two hosts. As a result, you can migrate VMs stored on local storage without downtime and you can move VMs from one pool to another with virtually no service interruption. The choice of destination server depends on how the VM and the pool are configured. In a pool with Workload Balancing (WLB) enabled, for example, recommendations are provided to help select the best possible physical server for the VM's workload. For more information, see Choosing an Optimal Server for VM Initial Placement, Migrate, and Resume.

Storage live migration enables system administrators to:

- Rebalance VMs between XenServer pools (for example from a development environment to a production environment)
- Upgrade and update standalone XenServer servers without any VM downtime
- Upgrade the XenServer server hardware

NOTE:

- Migrating a VM from one host to another preserves the VM *state*. The state information includes information that defines and identifies the VM and the historical performance metrics, such as CPU and network usage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Storage live migration also allows you to move virtual disks from one Storage Repository (SR) to a different SR within the same pool. For more information, see Move Virtual Disks.

Compatibility requirements

When migrating a VM with live migration or storage live migration, the VM and servers must meet the following compatibility requirements.

General requirements:

- The target host must have the same or a more recent version of XenServer installed as the source host. This also includes ensuring that your target host has the same or more recent level of updates as the source host.
- XenServer VM Tools for Windows must be installed on each Windows VM that you want to migrate.
- You cannot concurrently migrate more than three VMs that have their source location in the same pool.

CPU requirements:

- If the CPUs on the source and target host are different, the target host must be at least as capable as the source host. Generally, this means that the target has the same or a newer CPU.
  - If you are migrating within the same pool, the pool automatically attempts to make a VM compatible.
  - If you are migrating between pools, you must ensure that the VM is compatible with the feature set in the destination pool.
- You cannot live migrate a VM between AMD and Intel processors.

Memory requirements:

- The target host must have sufficient spare memory capacity or be able to free sufficient capacity using Dynamic Memory Control. If there is not enough memory, the migration fails to complete.
- Storage migration only: A host in the source pool must have sufficient spare memory capacity to run a halted VM that is being migrated. This requirement enables the halted VM to be started at any point during the migration process.

Disk space requirements:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Storage migration only: The target storage must have enough free disk space available for the incoming VMs. The free space required can be three times the VDI size (without snapshots). If there is not enough space, the migration fails to complete.
- The source storage must have enough free disk space to create temporary snapshots of the VM's VDIs during the migration. If there is not enough space, the migration fails to complete. The free space required can be up to two times the size of the VM's disk.

Live migration and storage live migration limitations

Live migration and storage live migration are subject to the following limitations:

- VMs using SR-IOV cannot be migrated. For more information, see Use SR-IOV enabled NICs
- VM performance is reduced during migration.
- If using the high availability feature, ensure the VM being migrated is not marked as protected.
- VMs that have the `on-boot` option set to `reset` cannot be migrated. For more information, see Intellicache.
- Time to completion of VM migration depends on the memory footprint of the VM, and its activity. In addition, the size of the VDI and the storage activity of the VDI can affect VMs being migrated with storage live migration.
- You cannot use storage live migration to migrate VMs that have changed block tracking enabled. Disable changed block tracking before attempting storage live migration. For more information, see Changed Block Tracking.
- Storage live migration cannot be used with VMs created by Machine Creation Services.
- Storage migration cannot be used with non-persistent VMs.

VMs which have VDIs on a GFS2 or XFS SR are subject to the following additional limitations:

- Storage live migration cannot be used either within the same pool or between pools.
    - Within a pool it is possible to use the Move VM operation if the VM is shut-down.

For step-by-step instructions on using live migration or storage live migration to migrate your VMs, see the section *To Migrate or Move a VM*.

Move VMs

XenCenter® allows you to move shut-down VMs to a new storage repository in the same pool by using the **Move VM** wizard. For step-by-step instructions, see the following section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Moving a shut-down VM between SRs has the same restrictions as performing storage migration. For more information, see the preceding section.

To migrate or move a VM

1. In the Resources pane, select the VM and do one of the following depending on the status of your VM.

   - To migrate a running or suspended VM using live migration or storage live migration: On the **VM** menu, select **Migrate to Server** and then **Migrate VM wizard**. This action opens the **Migrate VM** wizard.

     NOTE:

     For pools with 16 or fewer members, the right-click menu displays the list of available servers to migrate the VM to. However, for larger pools, the servers are not listed in the menu. Instead you must open the **Migrate to Server** wizard.

   - To move a stopped VM: On the **VM** menu, select **Move VM**. This action opens the **Move VM wizard**.

2. Select a standalone server or a pool from the **Destination** list.
3. Select a server from the **Home Server** list to assign a home server for the VM and select **Next**.
4. On the **Storage** page, specify a storage repository to place the virtual disks of the migrated VM on. Select **Next**.

   - The **Place all migrated virtual disks on the same SR** option is selected by default and displays the default shared SR on the destination pool.
   - Select **Place migrated virtual disks onto specified SRs** to specify an SR from the **Storage Repository** list. This option allows you to select different SR for each virtual disk on the migrated VM.

5. On the **Networking** page, map the virtual network interfaces in the selected VM to networks in the destination pool or server. Specify your options using the **Target Network** list and select **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Select a storage network on the destination pool that is to be used for the migration of the VM's virtual disks. Select **Next**.

   NOTE:

   Due to performance reasons, it is recommended that you do not use the management network for live migration.

7. Review the configuration settings and select **Finish** to start migrating or moving the VM.

If you are migrating from an older version of XenServer or Citrix Hypervisor™, you might need to restart all VMs after migrating your VMs, to ensure that new virtualization features are picked up.

Related documentation

XenServer Current Release

- Migrate VMs

Delete a VM

Deleting a virtual machine removes its configuration and its filesystem from the server. When you delete a VM, you can choose to delete or preserve any virtual disks attached to the VM, in addition to any snapshots of the VM.

To delete a VM:

1. Shut down the VM.
2. Select the stopped VM in the **Resources** panel, right-click, and select **Delete** on the shortcut menu. Alternatively, on the **VM** menu, select **Delete**.
3. To delete an attached virtual disk, select its check box.

   IMPORTANT:

   Any data stored in the VM's virtual disk drives is lost.

4. To delete a snapshot of the VM, select its check box.
5. Click **Delete**.

   When the delete operation is completed, the VM is removed from the **Resources** pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> VM snapshots whose parent VM has been deleted (*orphan snapshots*) can still be accessed from the **Resources** pane. These snapshots can be exported, deleted, or used to create VMs and templates. To view snapshots in the **Resources** pane, select **Objects** in the Navigation pane and then expand the **Snapshots** group in the Resources pane.

Related documentation

XenServer Current Release

- VMs

Changed Block Tracking

The XenServer® changed block tracking feature offers incremental backup capabilities for customers using XenServer. This feature is available only for XenServer Premium Edition.

When you enable changed block tracking for the virtual disk images (VDIs) of a VM, any blocks that are changed in a VDI are recorded in a log file. Every time you take a snapshot of the VDI, this log file can be used to identify the blocks that have changed since the last snapshot of the VDI. With this feature, you can back up only those blocks that have changed.

Changed block tracking can be enabled by using the CLI or API. The third-party product that you use to take incremental backups usually enables this feature. When changed block tracking is enabled for a VDI, additional information is calculated and stored that lists the changed blocks for the VDI. This process uses resources such as memory and space.

For more information about changed block tracking, see the developer documentation.

For a list of third-party solutions that use the changed block tracking feature, see Third-party backup solutions.

Disabling changed block tracking on a VM

You can disable changed block tracking for all VDIs associated with a VM by using XenCenter. Before disabling changed block tracking for a VM or VMs, consider the following:

- To use storage live migration to move a VM, you must disable changed block tracking on that VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Disabling changed block tracking prevents your backup solution from taking incremental backups of the VDIs associated with the VM. To take another set of incremental backups, you must enable changed block tracking again.
- Changed block tracking cannot be enabled again by using XenCenter.

To disable changed block tracking, complete the following steps:

1. In the left panel, choose the VM or VMs that you want to disable changed block tracking on.
2. From the main menu, select **VM** then **Disable Changed Block Tracking**.
3. In the confirmation dialog that opens, select **Yes** to continue.

Viewing the changed block tracking status for a VDI

You can see whether changed block tracking is enabled for a VDI on the **Storage** tab for an SR.

If the SR is part of a pool where changed block tracking is available, XenCenter displays the **Changed Block Tracking** column. This column shows whether changed block tracking is **Enabled** or **Disabled** for a VDI.

Secure Boot Certificates

For UEFI Secure Boot enabled VMs, XenCenter® indicates the status of the Secure Boot certificates, and allows for updates where available, for example to remediate certificate expiry.

For more information on UEFI Secure Boot certificate remediation, please review the appropriate XenServer 8.4 or XenServer 9 documentation.

Review certificate state in XenCenter

You can review the certificate state for a specific VM or template using the following process:

1. In the left panel, choose the VM or template you wish to check.
2. On the General tab, expand the Boot Options section.
3. Review the **Secure boot certificates** field:
    - **Update available** - The VM is eligible for remediation and can be flagged for update on the next boot.
    - **OK** - The VM does not require remediation.
    - **Update flagged** - The VM is scheduled for certificate update on the next boot.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also use the search functionality to identify VMs where an update is available using the following process:

1. Start a new search.
2. Select to search for VMs.
3. Select to filter on **Secure Boot Certificates**
4. Select the **Update available** value

Flag or unflag VMs for certificate update

To flag one or more VMs for certificate update at their next boot, use the following process:

1. In the left panel, choose the VM or VMs that you wish to flag for certificate update.
2. From the main menu, select **VM**, then **Secure Boot Certificates**, then **Flag for certificates update**. Alternatively, right-click and select **Secure Boot Certificates** > **Flag for certificates update**.

To unflag one or more VMs for certificate update at their next boot, use the following process:

1. In the left panel, choose the VM or VMs that you wish to unflag for certificate update.
2. From the main menu, select **VM**, then **Secure Boot Certificates**, then **Unflag for certificates update**. Alternatively, right-click and select **Secure Boot Certificates** > **Unflag for certificates update**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Importing and Exporting VMs

You can import VMs from OVF/OVA packages, from disk images, and from XenServer XVA files. VMs can be exported as OVF/OVA packages and as XenServer XVA files. Import and export VMs in XenCenter using the **Import** and **Export** wizards.

You can import or export a UEFI-enabled VM created on a XenServer® server as an OVA, OVF, or an XVA file. Importing a UEFI-enabled VM from other hypervisors is not supported.

NOTES:

- It is not guaranteed that you can import a VM that was exported from a more up-to-date system onto a less up-to-date system. For example, if you export a VM from a host that is at the latest level on the Early Access update channel, you might not be able to import this VM into a host that is at the latest level on the Normal update channel straight away. Before you can import the VM in to that host, the host on the Normal channel must reach the same level of updates as the Early Access channel had when the VM was exported.

  This behavior is caused by additional metadata that might be added in later updates, which earlier versions do not understand.
- VM group settings are not retained when a VM is exported.

Supported import and export formats

FORMAT	DESCRIPTION
Open Virtualization Format (OVF and OVA)	OVF is an open standard for packaging and distributing a virtual appliance consisting of one or more VMs. For more information about XenCenter support for OVF and OVA file formats, see Open Virtualization Format.
Disk image formats	Virtual Hard Disk (VHD) and Virtual Machine Disk (VMDK) format disk image files can be imported using the **Import** wizard. You might want to import a disk image when only a virtual

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FORMAT	DESCRIPTION
	disk image is available, but there is no OVF metadata associated with it. For more information about supported disk image formats, see Disk Image Formats (VHD and VMDK).
XenServer XVA format	XVA is a format specific to Xen-based hypervisors for packaging a single VM as a single file archive of a descriptor and disk images. Its file name extension is `.xva`.

Which format to Use?

Use OVF/OVA to:

- Share XenServer vApps and VMs with other hypervisors that support OVF.
- Save more than one VM.
- Secure a vApp or VM from corruption and tampering.
- Include a license agreement.
- Simplify vApp distribution by storing an OVF package in an OVA.

Use XVA to:

- Import and export VMs from a script with a command line interface (CLI).

(Windows VMs only) Installing XenServer VM Tools for Windows

If the pool contains Conversion Manager version 8.5.0 or later, after Windows VMs are created successfully from an imported file, a fixup process begins. The fixup process uninstalls VMware Tools, if they are present. If you selected this option, it also installs the XenServer VM Tools.

(Linux VMs only) Operating System Fixup

For imports of Linux VMs that were created on another hypervisor, XenCenter® includes an advanced hypervisor interoperability feature Operating System Fixup. This feature aims to ensure a basic level of interoperability for some Linux VMs created on hypervisors other than XenServer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Operating System Fixup is supplied as an automatically booting ISO image that is attached to the imported VM's DVD drive. It performs the necessary configuration changes when the Linux VM is first started, and then shuts down the VM. The next time the new Linux VM is started, the boot device is reset, and the VM starts normally.

NOTE:

Operating System Fixup does not convert the guest operating system from one hypervisor to another.

The Operating System Fixup ISO is located in your XenCenter installation in the directory `C:\Program Files (x86)\XenServer\XenCenter\External Tools`.

To use Operating System Fixup on imported disk images and OVF/OVA packages, you enable the feature on the **OS Fixup Settings** page of the XenCenter **Import** wizard. Specify a location to copy the Fixup ISO to so that XenServer can use it.

Operating System Fixup requirements

Operating System Fixup requires an ISO SR with 40 MB of free space and 256 MB of virtual memory.

Open Virtualization Format (OVF and OVA)

OVF is an open standard, specified by the Distributed Management Task Force (DMTF), for packaging and distributing a virtual appliance consisting of one or more virtual machines (VMs).

An **OVF Package** contains metadata and file elements that describe VMs, plus additional information important to the deployment and operation of the applications in the OVF package. Its file name extension is `.ovf`.

An **Open Virtual Appliance (OVA)** is an OVF Package in a single file archive with the `.ova` extension.

In XenServer environments where Role-Based Access Control (RBAC) is implemented, only users with the RBAC role of Pool Admin or Pool Operator can import OVF and OVA packages. To export OVF and OVA packages, you must have the Pool Admin, Pool Operator, VM Power Admin, or VM Admin role. For more information about RBAC roles, see RBAC overview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's in an OVF package?

An **OVF Package** always includes a descriptor file (`*.ovf`) and might also include several other files.

FILE TYPE	DESCRIPTION
Descriptor	The descriptor specifies the virtual hardware requirements of the service. This descriptor can also include information such as virtual disks descriptions, the service itself, guest OSes, a EULA, instructions to start and stop appliance VMs, and instructions to install the service. The descriptor file name extension is `.ovf`.
Manifest	The manifest is an SHA-1 digest of every file in the package, allowing the package contents to be verified by detecting any corruption. The manifest file name extension is `.mf`.
Signature	The signature is the digest of the manifest signed with the public key from the X.509 certificate included in the package. It allows the package author to be verified. The signature file name extension is `.cert`.
Virtual disks	OVF does not specify a disk image format. An OVF package includes files comprising virtual disks in the format defined by the virtualization product that exported the virtual disks. XenServer produces OVF packages with disk images in Dynamic VHD format; VMware products and Virtual Box produce OVF packages with virtual disks in Stream-Optimized VMDK format.

An **OVA package** is a single archive file, in the Tape Archive (tar) format, containing the files that comprise an OVF Package.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Which format do I use?

OVF packages contain a series of uncompressed files that make it easier to access individual disk images in the file. OVA packages are just one large file. While you can compress this file, it doesn't have the flexibility of a series of files like OVF.

OVA is better for specific applications where it is beneficial to have a single file, making the package easier to handle, such as creating packages for Web downloads. Exporting and importing OVA packages takes longer than OVF.

You cannot use OVA/OVF to export virtual machines with an attached vTPM.

(Windows VMs only) Installing XenServer® VM Tools for Windows

If you also have the Conversion Manager virtual appliance version 8.5.0 or later running in your pool, you can choose to install XenServer VM Tools for Windows as part of an import. If you choose not to install XenServer VM Tools for Windows as part of the import process, ensure that you install them manually later for the VM to be fully supported. For more information, see Install XenServer VM Tools.

(Linux VMs only) Using Operating System Fixup

XenCenter® includes an advanced hypervisor interoperability feature Operating System Fixup. This feature aims to ensure a basic level of interoperability for Linux VMs created on hypervisors other than XenServer. If you select a Linux template when importing a disk image that was created on another hypervisor, you can instead choose to run Operating System Fixup as part of the import.

To find out more, see About VM Import and Export.

More information about OVF

For more information about OVF, see the following documents on the DMTF website:

Open Virtualization Format Specification

Related documentation

XenServer Current Release

- Import and export VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Disk Image Formats (VHD, VHDX, AVHDX, and VMDK)

Using the **Import** wizard, you can import a disk image into a resource pool or into a specific host as a VM.

You might want to import a disk image when only a virtual disk image is available, but there is no OVF metadata associated with it. Situations when this scenario might occur include:

- The OVF metadata is not readable. However, it is still possible to import the disk image.
- You have a virtual disk that is not defined in an OVF package.
- You are moving from a platform that does not let you create an OVF appliance (for example, older platforms or images).
- You want to import an older VMware appliance that does not have any OVF information.
- You want to import a standalone VM that does not have any OVF information.

When available, Citrix® recommends importing appliance packages that contain OVF metadata and not just importing an individual disk image. The OVF data provides information that the **Import** wizard needs to recreate a VM from its disk image. This information includes the number of disk images associated with the VM, the processor, storage, and memory requirements, and so on. Without this information, it can be much more complex and error-prone trying to recreate the VM.

In XenServer environments where Role-Based Access Control (RBAC) is implemented, only users with the RBAC role of Pool Admin can import disk images. For more information, see RBAC overview.

Supported disk image formats

The following disk image formats can be imported using the XenCenter® **Import** wizard:

Format	Description
Virtual Hard Disk (VHD)	VHD is a group of virtual disk image formats specified by Microsoft as part of their Open Specification Promise. Their file name extension is `.vhd`. XenCenter imports and exports the Dynamic VHD format – a thinly provisioned virtual disk image that allocates space only when used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual Hard Disk (VHDX)	Successor format to VHD. The file name extension is `.vhdx`.
Automatic Virtual Hard Disk (AVHDX)	A disk image checkpoint for a particular state of a VHDX file. The file name extension is `.avhdx`.
Virtual Machine Disk (VMDK)	VMDK is a group of virtual disk image formats specified by VMware. Their file name extension is `.vmdk`. XenCenter imports stream-optimized and monolithic flat VMDK formats. Stream-optimized VMDK is the format used by OVF packages produced for VMware and Virtual Box hypervisors. Monolithic flat VMDK is a common format of a virtual disk available for download by VMware management clients.

(Windows VMs only) Installing XenServer® VM Tools for Windows

If you also have the Conversion Manager virtual appliance version 8.5.0 or later running in your pool, you can choose to install XenServer VM Tools for Windows as part of an import. If you choose not to install XenServer VM Tools for Windows as part of the import process, ensure that you install them manually later for the VM to be fully supported. For more information, see Install XenServer VM Tools.

(Linux VMs only) Using Operating System Fixup

XenCenter includes an advanced hypervisor interoperability feature Operating System Fixup. This feature aims to ensure a basic level of interoperability for Linux VMs created on hypervisors other than XenServer. If you select a Linux template when importing a disk image that was created on another hypervisor, you can instead choose to run Operating System Fixup as part of the import.

To find out more, see About VM Import and Export.

Related documentation

XenServer Current Release

- Import and export VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Import VMs From OVF/OVA

You can import virtual machines (VMs) that have been saved as OVF/OVA files using the **Import** wizard. The wizard takes you through many of the usual steps needed to create a VM in XenCenter: configuring storage and networking for the new VMs, plus some additional steps required as part of the OVF import process, including:

- Reviewing/accepting any EULAs.
- Specifying security settings if the OVF package includes a certificate or a manifest.
- Specifying **Operating system fixup** settings if importing Linux VMs that were built on a hypervisor other than a XenServer® host.

For detailed information about each of these steps, see Creating a New VM.

Imported OVF packages appear as vApps when imported using XenCenter. When the import is complete, the new VMs appear in the XenCenter **Resources** pane and the new vApp appears in the Managing vApps dialog box.

NOTE:

It might not always be possible to run an imported VM that was exported from another server with a different CPU type. For example, a Windows VM created on a server with an Intel VT CPU, then exported, might not run when imported to a server with an AMD-V CPU.

Prerequisites

- To be able to import VMs from an OVF/OVA package, you require certain permissions. The **Import** wizard performs checks to ensure that you have a required role in the destination pool before allowing you to continue. For more information about the RBAC roles that are required, see Definitions of RBAC roles and permissions.

Import an OVF package

1. In the **Resources** pane, select the host or pool to import the package into.
2. On the **File** menu, select **Import**. The **Import** wizard opens.
3. On the first page of the wizard, locate the OVA/OVF file you want to import, then click **Next** to continue.
    - If you select a compressed OVA file (`*.ova.gz`), on clicking **Next**, the file is decompressed to an OVA file and the old `*.ova.gz` file is deleted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you enter a URL location (HTTP, HTTPS, file, FTP) in the **Filename** box, on clicking **Next**, a **Download Package** dialog opens. In this dialog, specify a folder on your XenCenter host where the OVA/OVF is to be copied.

4. (Optional) **Review and accept the EULA.** If the OVF/OVA includes a EULA, the **EULA** page displays the EULA text. If you want to accept the EULA, choose **Accept** and continue.
5. **Specify a template.** In the **Template** page, choose the template to use for the VM or VMs that you are importing from the OVA/OVF file. Only the default templates provided with XenServer are supported. Do not use a custom template.

   On this panel, you can also choose whether to use Windows Update to update the I/O drivers.

   Click **Next** to continue.
6. (Optional) **Install the XenServer VM Tools** (Windows VMs only) If the Conversion Manager virtual appliance version 8.5.0 or later is running in your pool, you can choose to install XenServer VM Tools for Windows as part of the import. This tools installation process happens after the imported VMs first start. For this option to be available, the VM disks must be on shared storage or on the same host as the Conversion Manager.

   a. Select **Install the XenServer® VM Tools**.

   b. Choose which version of the tools to install. One or more of the following options are available:

      - The version of the tools uploaded into the Conversion Manager
      - The latest version downloaded from the internet
      - A tools installation file in a location accessible from XenCenter®

   c. Click **Next** to continue.
7. (Optional) **Specify the VM location.** On the **Location** page, choose a server if you want to place the VMs you are importing on the server's local storage.

   Click **Next** to continue.
8. **Configure storage for the new VMs.**

   On the **Storage** page, select a storage repository (SR) where the imported virtual disk is placed. If you have selected to install the XenServer VM Tools as part of the import, ensure that VM disks are on shared storage or on the same host as the Conversion Manager.

   Click **Next** to continue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. **Configure networking for the new VMs.**

   On the **Networking** page, select a target network in the destination pool/standalone server for the new VMs' virtual network interface.

   Click **Next** to continue.

10. (Optional) **Specify security settings.** If the selected OVF/OVA package is configured with security features such as certificates or a manifest, specify the necessary information on the **Security** page. Select **Next** to continue. Different options appear on this page depending on which security features have been configured on the OVF package:

    - If the package is signed, a **Verify digital signature** check box appears here; select this check box if you want to verify the signature. Click **View Certificate** to display the certificate used to sign the package. If the certificate appears as untrusted, it is likely that either the Root Certificate or the Issuing Certificate Authority is not trusted on the local computer.
    - If the package includes a manifest, a **Verify manifest content** check box appears here. Select this check box to have the wizard verify the list of files in the package.

    When the package is digitally signed, the associated manifest is verified automatically and so the **Verify manifest content** check box does not appear on the **Security** page.

    Click **Next** to continue.

11. (Optional) **Enable Operating System Fixup.** (Linux VMs only) If all your VMs are Windows VMs, this panel is not shown.

    If the Linux VMs that you are importing are built on a hypervisor other than XenServer, select **Use Operating System Fixup**. Choose an ISO SR where the Fixup ISO can be copied so that XenServer can use it. For more information, see About VM Import and Export.

    Click **Next** to continue.

12. On the **Finish** page, review all the import settings. Click **Finish** to begin the import process and close the wizard.

When the import is finished, the newly imported VMs appear in the **Resources** pane and the new vApp appears in the Managing vApps dialog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If Conversion Manager virtual appliance version 8.5.0 or later is running in your pool, it automatically removes the VMware tools, if they are present, after the imported Windows VMs first start.

Errors when trying to start an imported VM

If you cannot boot the VMs imported from an OVF package, try importing the package again without using the Operating System Fixup feature: in the **OS Fixup Settings** page of the **Import** wizard, clear the **Use Operating System Fixup** checkbox. For more information, see About VM Import and Export.

Related documentation

XenServer Current Release

- Import and export VMs

Import VMs From Disk Images

You can import virtual machines (VMs) that have been saved as disk images by using the XenCenter® **Import** wizard. The wizard takes you through many of the usual steps needed to create a VM in XenCenter: nominating a home server, and configuring storage and networking for the new VMs, plus some additional steps required as part of the disk image import process, including:

- Specifying a name for the new VM and allocating it some vCPUs and memory resources.
- Specifying **Operating system fixup** settings if importing VMs that were built on a hypervisor other than a XenServer® host.

For detailed information about each of these steps, see Creating a New VM.

Prerequisites

- To be able to import a VM from a disk image, you require certain permissions. The **Import** wizard performs checks to ensure that you have a required role in the destination pool before allowing you to continue. For more information about the RBAC roles that are required, see Definitions of RBAC roles and permissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you are importing a disk image with Windows 11 installed in it, ensure that BitLocker is disabled and remove the vTPM device.

Import a disk image

1. In the **Resources** pane, select the host or pool to import the package into.
2. On the **File** menu, select **Import**. The **Import** wizard opens.
3. On the first page of the wizard, locate the disk image file you want to import, then click **Next** to continue.

   If you enter a URL location (HTTP, HTTPS, file, FTP) in the **Filename** box, on clicking **Next**, a **Download Package** dialog opens. In this dialog, specify a folder on your XenCenter host where the disk image is to be copied.
4. **Specify a template.** Choose the template to use for the VM that you are importing the disk image for. Only the default templates provided with XenServer are supported. Do not use a custom template.

   On this panel, you can also choose whether to copy the BIOS strings to the VM and whether to use Windows Update to update the I/O drivers.

   Click **Next** to continue.
5. (Optional) **Install the XenServer VM Tools** (Windows VMs only) If the Conversion Manager virtual appliance version 8.5.0 or later is running in your pool, you can choose to install XenServer VM Tools for Windows as part of the import. This tools installation process happens after the imported VM first starts. For this option to be available, the disk image must be on shared storage or on the same host as the Conversion Manager.

   a. Select **Install the XenServer VM Tools**.

   b. Choose which version of the tools to install. One or more of the following options are available:

      - The version of the tools uploaded into the Conversion Manager
      - The latest version downloaded from the internet
      - A tools installation file in a location accessible from XenCenter

   c. Click **Next** to continue.
6. **Specify the VM name.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On the **Name** page, enter the name of the new VM to be created from the imported disk image. This value can be adjusted later, after the new VM has been created. VM names are not checked for uniqueness within XenCenter, so it makes it easier for you to manage different VMs if you give them meaningful, memorable names. For more information, see VM Name and Description.

Click **Next** to continue.

7. **Allocate CPU and memory resources.**

   On the **CPU & Memory** page, allocate CPU and initial memory resources. These values can be adjusted later, after the new VM has been created. For more information, see VM CPU and Memory Allocation.

   Click **Next** to continue.

8. (Optional) **Specify the VM location.** On the **Location** page, choose a server if you want to place the VM you are importing on the server's local storage.

   Click **Next** to continue.

9. **Configure storage for the new VM.**

   On the **Storage** page, select a storage repository (SR) where the imported virtual disk is placed. If you have selected to install the XeNServer VM Tools as part of the import, ensure that disk image is on shared storage or on the same host as the Conversion Manager.

   Click **Next** to continue.

10. **Configure networking for the new VM.**

    On the **Networking** page, select a target network in the destination pool/standalone server for the new VM's virtual network interface.

    Click **Next** to continue.

11. **Specify the boot option.**

    On the **Boot options** page, specify the boot mode for the new VM. Only the options that are supported with the guest operating system can be selected.

    - **BIOS Boot**: Select this option to boot the VM in legacy BIOS mode. Legacy BIOS boot is not supported for Windows 11 VMs.
    - **UEFI Boot**: Select this option to boot the VM in UEFI mode. XenServer supports this boot mode only for certain guest operating systems. For more information about the guest

© 1997–2026 Citrix Systems, Inc. All rights reserved.

operating systems that are supported for UEFI boot, see Guest UEFI boot and Secure Boot.

- **UEFI Secure Boot**: Select this option to boot the VM in UEFI Secure Boot mode. Secure Boot prevents unsigned, incorrectly signed or modified binaries from being run during boot. XenServer supports this boot mode only for certain guest operating systems. For more information about the guest operating systems that are supported for UEFI Secure Boot, see Guest UEFI boot and Secure Boot.

(VHDX/AVHDX only) When importing a VM from a VHDX/AVHDX file, the **Import** wizard attempts to automatically detect the boot mode from the VHDX/AVHDX file you are importing. Review the settings and ensure that the same boot mode that was originally configured for the VM is selected.

Click **Next** to continue.

12. (Optional) **Enable Operating System Fixup.** If you have selected a Windows template, this panel is not shown.

    If the disk image that you are importing is built on a hypervisor other than XenServer, select **Use Operating System Fixup**. Choose an ISO SR where the Fixup ISO can be copied so that XenServer can use it. For more information, see About VM Import and Export.

    IMPORTANT:

    If you are importing a VHDX/AVHDX file from Citrix Provisioning (PVS) on VMware vSphere, select **Don't use Operating System Fixup**. Enabling Operating System Fixup for VHDX/AVHDX from PVS might result in a boot failure.

    Click **Next** to continue.

13. On the **Finish** page, review all the import settings. Click **Finish** to begin the import process and close the wizard.

    The import progress is displayed on the status bar at the bottom of the XenCenter window and also on the **Events** view under **Notifications**.

The import process might take some time. The time it takes depends on the size of the imported virtual disks, the available network bandwidth, and the disk interface speed of the XenCenter host. When the import is finished, the newly imported VM appears in the **Resources** pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If Conversion Manager virtual appliance version 8.5.0 or later is running in your pool, it automatically removes the VMware tools, if they are present, after the imported VM first starts.

Next steps

Ensure the XenServer VM Tools for Windows are fully installed:

- If you chose to install XenServer VM Tools for Windows as part of the import process, restart the VM after the import to complete the tools installation.
- If you chose not to install XenServer VM Tools for Windows as part of the import process, ensure that you install them manually later for the VM to be fully supported. For more information, see Install XenServer VM Tools.

Related documentation

XenServer Current Release

- Import and export VMs

Import VMs From XVA

You can import VMs, templates, and snapshots that have been exported and stored locally in XVA format (`.xva`) by using the XenCenter **Import** wizard. The wizard takes you through many of the usual steps needed to create a VM in XenCenter: nominating a home server and configuring storage and networking for the new VMs. For detailed information about each of these steps, see Creating a New VM.

NOTE:

It might not always be possible to run an imported VM that was exported from another server with a different CPU type. For example, a Windows VM created on a server with an Intel VT CPU, then exported, might not run when imported to a server with an AMD-V CPU.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

- To be able to import a VM from an XVA package, you require certain permissions. The **Import** wizard performs checks to ensure that you have a required role in the destination pool before allowing you to continue. For more information about the RBAC roles that are required, see Definitions of RBAC roles and permissions.

Import an XVA package

1. Open the **Import** wizard by doing one of the following:
   - In the **Resources** pane, right-click, and then select **Import** on the shortcut menu.
   - On the **File** menu, select **Import**.
2. On the first page of the wizard, locate the XVA file you want to import, then click **Next**. If you enter a URL location (HTTP, HTTPS, file, FTP) in the **Filename** box, on clicking **Next**, a **Download Package** dialog opens. In this dialog, specify a folder on your XenCenter® host where the files are to be copied.
3. On the **Home Server** page, specify where to put the new VM:
   - To place the imported VM in a pool without assigning it a home server, select the destination pool in the list. Click **Next** to continue.
   - To place the imported VM in a pool and assign it to a specific server (or to place it on a standalone server), select a server.

   Click **Next** to continue.
4. On the **Storage** page, select a storage repository (SR) where the imported virtual disks are to be placed, then click **Next** to continue.
5. On the **Networking** page, map the virtual network interfaces in the VM you are importing to target networks in the destination pool/standalone server. The Network and MAC address shown in the list on this page are stored as part of the definition of the original (exported) VM in the export file. To map an incoming virtual network interface to a target network, select a network from the list in the **Target network** column.

   Click **Next** to continue.
6. On the last page of the **Import** wizard, review the configuration options you have selected. To have the imported VM start up when the import process has finished and the new VM is provisioned, select the **Start VM after import** check box.
7. Click **Finish** to begin importing the selected file and close the wizard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The import progress is displayed on the status bar at the bottom of the XenCenter window and also on the **Events** view under **Notifications**.

The import process can take some time. The time it takes depends on the size of the imported VM's virtual disks, the available network bandwidth, and the disk interface speed of the XenCenter host. When the newly imported VM is available, it appears in the **Resources** pane.

Related documentation

XenServer Current Release

- Import and export VMs

Export VMs as OVF/OVA

You can export one or more VMs as an OVF or OVA package using the XenCenter® **Export** wizard. To open the wizard, select the VM you want to export and on the **VM** menu, select **Export**. The VMs must be shut down or suspended before they can be exported.

You need an RBAC role of Pool Admin to export to OVF/OVA. The **Export** wizard performs checks when it starts up to ensure that you have a Pool Admin role before allowing you to continue. For more information, see RBAC overview.

NOTE:

It might not always be possible to run an imported VM that was exported from another server with a different CPU type. For example, a Windows VM created on a server with an Intel VT CPU, then exported, might not run when imported to a server with an AMD-V CPU.

You cannot use OVA/OVF to export virtual machines with an attached vTPM.

Prerequisites

- To be able to export a VM as an OVF/OVA package, you require certain permissions. The **Export** wizard performs checks to ensure that you have a required role in the destination pool before allowing you to continue. For more information about the RBAC roles that are required, see Definitions of RBAC roles and permissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Export an OVF/OVA package

1. Open the **Export** wizard: select the pool or server containing the VMs you want to export, then on the **VM** menu, select **Export**.
2. On the first page of the wizard, enter the name of the export file. Specify the folder where you want the files to be saved. Select **OVF/OVA Package (*.ovf, *.ova)** from the **Format** list. Select **Next**.
3. Select the VMs you want to export. Select **Next**.
4. On the **EULAs** page, you can add previously prepared End User Licensing Agreement (EULA) documents (`.rtf`, `.txt`) in the package. To view the contents of a EULA in a text editor, select it in the list and select **View**. If you do not want to include a EULA in the package, select **Next** to continue.
5. On the Advanced options page, specify any manifest, signature, and output file options, or select **Next** to continue:

    a. To create a manifest for the package, select the **Create a manifest** check box. The manifest provides an inventory or list of the other files in a package. The manifest is used to ensure the files originally included when the package was created are the same files present when the package arrives. When the files are imported, a checksum is used to verify that the files have not changed since the package was created.

    b. To add a digital signature to the package, select the **Sign the OVF package** check box. Browse to locate a certificate. Enter the private key associated with the certificate in the **Private key password** box. When a signed package is imported, the user can verify the package creator's identity by using the certificate's public key to validate the digital signature. Use an X.509 certificate that you have already created from a Trusted Authority and exported as either a `.pem` or `.pfx` file that contains the signature of the manifest file and the certificate used to create that signature.

    c. To output the selected VMs as a single (`tar`) file in OVA format, select the **Create OVA Package** check box. For more information on the different file formats, see Open Virtualization Format (OVF and OVA).

    d. To compress the virtual hard disk images (`.VHD` files) included in the package, select the **Compress OVF files** check box. By default, when you create an appliance package, the virtual hard disk images that are exported consume the same amount of space that was allocated to the VM. For example, a VM that is allocated 26 GiB of space has a hard disk image that consumes 26 GiB of space, regardless of whether the VM actually requires that much space. Compressing the VHD files makes the export process take longer to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

complete, and importing a package containing compressed VHD files takes longer as the **Import** wizard must extract the VHD images as it imports them.

If both the **Create OVA Package** and **Compress OVF files** options are checked, the result is a compressed OVA file `*.ova.gz`.

6. On the final page of the wizard, review the settings you have selected on the previous pages. To have the wizard verify the exported package, select the **Verify export on completion** check box. Select **Finish** to begin exporting the selected VMs and close the wizard.

   The export process can take some time. The export speed depends on the size of the virtual disks, the available network bandwidth, and the disk interface speed of the XenCenter host. Progress is displayed on the status bar at the bottom of the XenCenter window and on the **Events** view under **Notifications**.

   To cancel an export in progress, select **Notifications** > **Events**, find the export in the list of events, and select **Cancel**.

Export VMs as XVA

You can export a single VM as an XVA file using the **Export** wizard. Shut down or suspended before you attempt to export them.

NOTE:

It might not always be possible to run an imported VM that was exported from another server with a different CPU type. For example, a Windows VM created on a server with an Intel VT CPU, then exported, might not run when imported to a server with an AMD-V CPU.

Prerequisites

- To be able to export a VM as an XVA package, you require certain permissions. The **Export** wizard performs checks to ensure that you have a required role in the destination pool before allowing you to continue. For more information about the RBAC roles that are required, see Definitions of RBAC roles and permissions.

Export an XVA package

1. Select the VM you want to export and on the **VM** menu, select **Export**.
2. On the first page of the wizard, enter the name of the export file, specify the folder where you want the file to be saved. Select **XVA File (*.xva)** from the **Format** list. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Virtual Machines** page, the VM to be exported is selected in the list. When exporting as XVA, you can only select one VM from this list. Click **Next** to continue.
4. On the final page of the wizard, review the settings you have selected on the previous pages. To have the wizard verify the exported XVA file, check **Verify export on completion**. Click **Finish** to begin exporting the selected VM and close the wizard.

   The export process can take some time. The speed of the export depends on the size of the VM's virtual disks, the available network bandwidth, and the disk interface speed of the XenCenter® host. Progress is displayed in the status bar at the bottom of the XenCenter window and on the **Events** view under **Notifications**.

   To cancel an export in progress, select **Notifications** > **Events**. Find the export in the list of events. Select **Cancel**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

About Snapshots

A virtual machine (VM) snapshot is a record of a running VM at a point in time. When you take a snapshot of a VM, its storage information (the data on the hard drive) and metadata (configuration information) is also saved. Where necessary, I/O on the VM temporarily halts while you take the snapshot to ensure that the snapshot captures a self-consistent disk image.

You can create snapshots without first shutting down the VM. This behavior is different to VM exports. A snapshot is similar to a normal VM template but it contains all the storage and configuration information for the original VM, including networking information. Snapshots provide a fast way of creating templates to export for backup purposes and then restore, or to use to quickly create VMs.

Snapshots are supported on all storage types.

Types of snapshots

XenCenter® supports the following types of VM snapshot:

- disk-only
- disk and memory

For more information, see Take a VM Snapshot.

Disk-only snapshots

Disk-only snapshots store a VM's configuration information (metadata) and disks (storage), allowing them to be exported and restored for backup purposes. This type of snapshot is crash-consistent and can be performed on all VM types, including Linux VMs.

Disk and memory snapshots

In addition to saving the VM's metadata and disks, disk and memory snapshots also save the VM's memory state (RAM). Reverting to a disk and memory snapshot does not require a reboot of the VM, and VMs can be running or suspended when the snapshot is taken. Disk and memory snapshots can be useful in the following cases:

- If you are upgrading or patching software

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you want to test a new application, but also want the option to be able to get back to the current, pre-change state (RAM) of the VM

Accessing orphaned snapshots

If you take snapshots of a VM and later delete the original VM, you can still access those snapshots in the **Resources** pane. Switch to **Objects** view in the **Navigation** pane and then expand the **Snapshots** group to see all available snapshots.

Related documentation

XenServer Current Release

- VMs

Take a VM Snapshot

Perform the following steps to take a snapshot of a Virtual Machine:

1. Select the VM in the **Resources** pane and then click the **Snapshots** tab.
2. Click **Take Snapshot**. Alternatively,
   - Right-click in the **Properties** pane and select **Take Snapshot**.
   - On the **VM** menu, select **Take Snapshot**.
3. Enter the name of the new snapshot and an optional description.
4. Under **Snapshot** mode, choose the type of snapshot to create:
   - To create a disk-only snapshot, select **Snapshot the virtual machine's disks**.
   - To create a disk and memory snapshot, select **Snapshot the virtual machine's disks and memory**.
5. Click **OK** to begin creating the snapshot. Progress is displayed on the status bar and on the **Events** view under **Notifications**.

   When the new snapshot has been created, it appears on the VM's **Snapshots** tab and under the Snapshots group in the **Resources** pane in **Folder** View:

   - A disk-only snapshot

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A disk and memory snapshot



Related documentation

XenServer Current Release

- VMs

Revert to a Snapshot

Reverting to a snapshot restores the VM to the state it was in at the point in time when you created the snapshot. Changes made to the VM since the snapshot was taken are discarded. The current state of the VM is lost with the following exception: when you revert a VM to a previous snapshot, the VM retains its current VM group setting. This setting does not change to the value it had when you took the snapshot.

The **Revert to Snapshot** dialog box includes an option to take a snapshot of the current VM state before you revert to the earlier snapshot. This option allows you to easily restore the VM to its current state again if you need to.

1. On the **Snapshots** tab, select the snapshot and select **Revert To**.

   If the snapshot you want to revert to is a scheduled snapshot, make scheduled snapshots visible on the **Snapshots** tab before you can select it. To make these snapshots visible, select **View** > **Scheduled Snapshots**.
2. To take a new snapshot of the current state of the VM before reverting it back to the earlier snapshot, select the check box.
3. Select **Yes**.

Related documentation

XenServer Current Release

- VMs

Create a New VM From a Snapshot

You create a VM from a snapshot in the same way as you create a VM from a regular VM template, by using the **New VM** wizard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To create a VM from a snapshot

1. On the **Snapshots** tab, select the snapshot you want to use, then right-click and select **New VM from Snapshot** on the shortcut menu.

   The **New VM** wizard opens, with your snapshot pre-selected on the **Templates** page.

2. Follow the steps in the **New VM** wizard to create the VM. For more information, see Creating a new VM.

To create a VM from an orphan snapshot

If the original VM used to create the snapshot has been deleted, you can select the snapshot and start the **New VM** wizard as follows:

1. In the **Resources** pane, switch to Folder View.
2. Select to expand the **Objects by Type** group and then expand the **Snapshots** group.
3. Select the snapshot, then right-click and select **New VM from Snapshot** on the shortcut menu.

Related documentation

XenServer Current Release

- VMs

Create a New Template From a Snapshot

While you cannot copy a VM snapshot directly, you can create a VM template from a snapshot and then use that to make copies of the snapshot. Templates are a "gold image" - ordinary VMs that you use as original copies from which to create VMs. After you have set up a VM the way you want it and taken a snapshot of it, save the snapshot as a new template. Use this new template to create copies of your specially configured VM in the same resource pool. The snapshot's memory state is not saved when you do this action.

To save a snapshot as a new template

1. On the **Snapshots** tab, select the snapshot, right-click, and select **Create Template from Snapshot** on the shortcut menu.
2. Enter the name of the new template and then click **OK**.

   After the new template has been successfully created, it appears as a custom template in the **Resources** pane. It also appears on the **Templates** page in the **New VM** wizard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To save an orphan snapshot as a new template

If the original VM used to create the snapshot has been deleted, you can save it as a new template as follows:

1. In the **Resources** pane, switch to Folder View.
2. Select to expand the **Objects by Type** group and then expand the **Snapshots** group.
3. Select the snapshot, right-click, and select **Create Template from Snapshot** on the shortcut menu.

Related documentation

XenServer Current Release

- VMs

Export a Snapshot to a File

When you export a VM snapshot, it is saved as a VM template in an XVA file in the location of your choice. This template contains a complete copy of the snapshot (including disk images). You can then import the template and use it to create a VM in the same or in a different resource pool.

To export a snapshot to a file

1. On the **Snapshots** tab, select the snapshot, select **Actions**, and then select **Export Snapshot as Template**.
2. On the page **Export File Details** of the wizard, enter the XVA file name and browse to locate the folder where you want to create the file. Click **Next** to continue.
3. On the **Finish** page, review the settings you have selected. To have XenCenter verify the exported package, select the **Verify export on completion** check box. Then select **Finish** to begin the export.

To export an orphan snapshot

If the original VM used to create the snapshot has been deleted, you can export the snapshot as follows:

1. In the **Resources** pane, switch to Folder View.
2. Select to expand the **Objects by Type** group and then expand the **Snapshots** group.
3. Select the snapshot then right-click and select **Export to File** on the context menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. On the page **Export File Details** of the wizard, enter the XVA file name and browse to locate the folder where you want to create the file. Click **Next** to continue.
5. On the **Finish** page, review the settings you have selected. To have XenCenter verify the exported package, select the **Verify export on completion** check box. Then select **Finish** to begin the export.

Related documentation

XenServer Current Release

- VMs

Delete a Snapshot

To delete a snapshot

1. On the **Snapshots** tab, select the snapshot. Select **Delete**.
2. Select **OK** to confirm.

To delete an orphan snapshot

If the original VM used to create the snapshot has been deleted, you can delete the snapshot as follows:

1. In the **Resources** pane, switch to Folder View.
2. Select to expand the **Objects by Type** group and then expand the **Snapshots** group.
3. Select the snapshot, right-click and then select **Delete Snapshot** on the shortcut menu.

Related documentation

XenServer Current Release

- VMs

Scheduled Snapshots

The scheduled snapshots feature provides a simple backup and restore utility for your critical service VMs. Regular scheduled snapshots are taken automatically and can be used to restore individual VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scheduled snapshots work by having pool-wide snapshot schedules for selected VMs in the pool. When a snapshot schedule is enabled, snapshots of the specified VM are taken at the scheduled time each hour, day, or week.

Several scheduled snapshots can be enabled in a pool, covering different VMs and with different schedules. A VM can be assigned to only one snapshot schedule at a time.

XenCenter® provides a range of tools to help you use this feature:

- To define a Scheduled Snapshot, use the **New snapshot schedule** wizard.
- To enable, disable, edit, and delete scheduled snapshots for a pool, use the **VM Snapshot Schedules** dialog box.
- To edit a snapshot schedule, open its Properties dialog box from the **VM Snapshot Schedules** dialog box.
- To revert a VM to a scheduled snapshot, select the snapshot on the **Snapshots** tab and revert the VM to it.

Related documentation

XenServer Current Release

- VMs

Create Scheduled Snapshots

Use the **New snapshot schedule** wizard to create a **Snapshot Schedule** that lets you specify the following information:

- The VMs in the pool to snapshot
- The type of snapshot to be created (disk-only or disk and memory)
- The snapshot schedule.

To open the **New snapshot schedule** wizard: on the **Pool** menu, select **VM Snapshot Schedules**, and then select **New** to start the wizard.

- **Schedule name**: Enter a name for the snapshot schedule. Optionally, provide a description.
- **VMs in the snapshot schedule**: Select the VMs you would like to add to the snapshot schedule.
- **Snapshot Type**: Choose the type of snapshot you would like to take.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scheduled snapshots can be either disk-only snapshots or disk and memory snapshots.

- Disk-only snapshots store the VM's disks (storage) and metadata. They are crash-consistent and can be performed on all VM types, including Linux VMs.
- Disk and memory snapshots save the VM's disks (storage), metadata, and its current memory state (RAM). This type of snapshot can be large.

- **Snapshot schedule**: Choose how often you would like to schedule a snapshot.

  Snapshot schedule options:

  - **Hourly snapshots**: A snapshot of the specified VM or VMs is taken each hour at the specified time.
  - **Daily snapshots**: A snapshot of the specified VM or VMs is taken each day at the specified time.
  - **Weekly snapshots**: A snapshot of the specified VM or VMs is taken at the specified time on the specified days of the week. You can select one or more days.

  In the **Number of snapshots to keep** section, specify the number of snapshot schedules to retain. When the number of scheduled snapshots taken exceeds this value, the oldest snapshot is deleted automatically.

  NOTE:

  You can take up to 10 scheduled snapshots per VM.

Related documentation

XenServer Current Release

- VMs

Manage scheduled snapshots

To enable, disable, edit, and delete **scheduled snapshots** for a pool, use the **VM Snapshot Schedules** dialog box on the **Pool** menu, select **VM Snapshot Schedules**.

Enabling a snapshot schedule

When you enable a **Snapshot Schedule**, you turn it "on". Automated snapshots of the specified VMs are generated at the scheduled time. Scheduled snapshots are taken until the schedule is disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To enable a snapshot schedule:

1. Select the pool or any server or VM in the pool in the **Resources** pane and on the **Pool** menu, select **VM Snapshot Schedules**.
2. Select a snapshot schedule from the list of snapshot schedules defined in the pool and select **Enable**.

Disabling a snapshot schedule

If you want to stop automated snapshots from being taken, you can disable the **Snapshot Schedules** using the **VM Snapshot Schedules** dialog box: a disabled snapshot schedule can be enabled again at any time.

To disable a snapshot schedule:

1. Select the pool or any server or VM in the pool in the **Resources** pane and on the **Pool** menu, select **VM Snapshot Schedules**.
2. Select the snapshot schedule from the list of snapshot schedules defined in the pool and select **Disable**.

Editing a snapshot schedule

You can change the properties of a snapshot schedule, for example, to add more VMs or to change the snapshot schedule:

1. Select the pool or any server or VM in the pool in the **Resources** pane. From the **Pool** menu, select **VM Snapshot Schedules**.
2. Select the snapshot schedule from the list of snapshot schedules defined in the pool.
3. Click **Properties** and go to the tab you need:
    - **General** Change the name and description of the snapshot schedule.
    - **Custom Fields** Define extra text and date/time fields for your snapshot schedules.
    - **VMs in the snapshot schedule** Select a VM from the list to add it to the snapshot schedule.
    - **Snapshot Type** Change the type of snapshot to create.
    - **Snapshot Schedule** Change the schedule used to take VM snapshots and change the snapshot retention value.
4. Click **OK** to save your changes and close the **Properties** window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deleting a snapshot schedule

To delete a Snapshot Schedule:

1. Select the pool, or any server or VM in the pool in the **Resources** pane. On the **Pool** menu, select **VM Snapshot Schedules**.
2. Select schedule from the list of snapshot schedules and select **Delete**.

Related documentation

XenServer Current Release

- VMs

Revert VMs to Snapshots

To revert a VM to a scheduled snapshot:

1. Select the VM and select the **Snapshots** tab.
2. To view scheduled snapshots, select **View** and then select **Scheduled Snapshots**. The Snapshots tab does not display scheduled snapshots by default.
3. Select the scheduled snapshot you want to revert the VM to and then select **Revert To**.
4. To take a new snapshot of the current state of the VM before reverting it back to the snapshot schedule, select the check box.
5. Click **Yes** to revert the VM back to the selected snapshot.

Related documentation

XenServer Current Release

- VMs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenServer® vApps

XenServer vApp: A logical group of one or more related virtual machines (VMs) which can be managed as a single entity. The VMs within a vApp do not have to reside on one XenServer server and are distributed within a pool using the normal rules.

When a vApp is started, the VMs contained within it start in a user-defined order, allowing VMs which depend upon one another to be automatically sequenced. This capability means that you do not need to manually sequence the startup of dependent VMs when the whole service requires a restart.

Using the Manage vApps dialog box

Use the XenCenter® **Manage vApps** dialog box you can create, delete and modify vApps, start and shutdown vApps, and import and export vApps within the selected pool. When you select a vApp in the list, the VMs it contains are listed in the details pane on the right.

CONTROL	FUNCTION
 **New vApp**	Opens the **New vApp** wizard. See Create a vApp.
 **Delete**	Deletes the selected vApp. The VMs in the vApp are not deleted.
 **Properties**	Opens a **Properties** dialog box for the selected vApp. Here you can change its name or description, add or remove VMs from the vApp, and change their start order and delay interval. See Modify vApps.
 **Start**	Starts up all VMs in the selected vApp in the sequence specified by the start order and delay interval values set on each individual VM. See Start and shut-down vApps.
 **Shut Down**	Shut down all VMs in the selected vApp. See Start and shut-down vApps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONTROL	FUNCTION
 **Import**	Open **Import** wizard and import an OVF/OVA package as a vApp. See Export and import vApps.
 **Export**	Open the **Export** wizard and export a vApp as an OVF/OVA package. See Export and import vApps.

Related documentation

XenServer Current Release

- vApps

Create a vApp

To create a vApp, use the Manage vApps dialog box.

1. Select the pool and, from the **Pool** menu, select **Manage vApps**.

   Alternatively, right-click in the **Resources** pane and select **Manage vApps** on the shortcut menu.
2. Select **New vApp...** on the top left corner of the Manage vApps dialog box.
3. Enter the name of the new vApp and (optionally) a description, then select **Next**. You can choose any name you like, but a descriptive name is best. Although it is advisable to avoid having multiple vApps with the same name, it is not a requirement. XenCenter® does not enforce any uniqueness constraints on vApp names. It is not necessary to use quotation marks for names that include spaces.
4. Choose which virtual machines to include in the new vApp and then select **Next**. You can use the **Search** box to list only VMs with names that include the specified string.
5. Specify the startup sequence for the VMs in the vApp, and then select **Next**.

Value	**Description**
Start order	Specifies the order in which individual VMs are started up within the vApp, allowing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	certain VMs to be restarted before others. VMs with a start order value of 0 (zero) start first, then VMs with a start order value of 1, and so on.
Attempt to start next VM after	This value is a delay interval that specifies how long to wait after the VM starts before the next group of VMs in the startup sequence start.

NOTE:

The shutdown order of VMs in a vApp is always the reverse of the configured start order.

6. On the final page of the wizard, you can review the vApp configuration. Select **Previous** to go back and modify any settings, or **Finish** to create the vApp and close the wizard.

Related documentation

XenServer Current Release

- vApps

Modify vApps

You can use the **Manage vApps** dialog to take the following actions:

- Change the name or description of a vApp
- Add or remove VMs from the vApp
- Change the startup sequence of the VMs in the vApp

Using the Manage vApps dialog

1. Select the pool and, on the **Pool** menu, select **Manage vApps**.

   Alternatively, right-click in the **Resources** pane and select **Manage vApps** on the shortcut menu.

2. Select the vApp and select **Properties** to open its **Properties** dialog box.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select the **General** tab to change the vApp name or description.
4. Select the **Virtual Machines** tab to add or remove VMs from the vApp.
5. Select the **VM Startup Sequence** tab to change the start order and delay interval values for individual VMs in the vApp.

Control	Description
Start order	Specifies the order in which individual VMs are started up within the vApp, allowing certain VMs to be restarted before others. VMs with a start order value of 0 (zero) start first, then VMs with a start order value of 1, and so on.
Attempt to start next VM after	This value is a delay interval that specifies how long to wait after the VM starts before the next group of VMs in the sequence start.

NOTE:

The shutdown order of VMs in a vApp is always the reverse of the configured start order.

6. Select **OK** to save your changes and close the **Properties** dialog box.

Related documentation

XenServer Current Release

- vApps

Delete a vApp

To delete a vApp from a pool, use the **Manage vApps** dialog box.

1. Select the pool and, on the **Pool** menu, select **Manage vApps**.

   Alternatively, right-click in the **Resources** pane and select **Manage vApps** on the shortcut menu.
2. Select the vApp you want to delete from the list, then select **Delete**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The VMs in the vApp are not deleted.

Related documentation

XenServer Current Release

- vApps

Start and Shut Down vApps

To start or shut down a vApp, use the **Manage vApps** dialog box, accessed from the **Pool** menu.

When you start a vApp, all the VMs within it are started up automatically in sequence. The start order and delay interval values specified for each individual VM control the startup sequence. You can set these values when you create the vApp and change them at any time from the **vApp Properties** dialog or from the individual **VM Properties** dialog.

For more information, see:

- Create vApps
- vApp Properties
- VM Properties

The shutdown order of VMs in a vApp is always the reverse of the configured start order.

To start a vApp

1. Open the **Manage vApps** dialog box: select the pool where the VMs in the vApp are located and, on the **Pool** menu, select **Manage vApps**.

   Alternatively, right-click in the **Resources** pane and select **Manage vApps** on the shortcut menu.

2. Select the vApp and select **Start** to start all the VMs it contains.



To shut down a vApp

1. Open the **Manage vApps** dialog box: select the pool where the VMs in the vApp are located and, on the **Pool** menu, select **Manage vApps**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alternatively, right-click in the Resources pane and select **Manage vApps** on the shortcut menu.

2. Select the vApp and select **Shut Down** to shut down all VMs in the vApp.

   A soft shutdown is attempted on all VMs. If a soft shutdown is not possible, then a forced shutdown is performed. For more information about soft and forced VM shutdowns, see Shut down a VM.

Related documentation

XenServer Current Release

- vApps

Export and Import vApps

To export a vApp

vApps can be exported as OVF/OVA packages.

1. Open the **Manage vApps** dialog box: on the **Pool** menu, select **Manage vApps**.
2. Select the vApp you want to export in the list and select **Export**.

3. Follow the procedure described in Export VMs as OVF/OVA.

   Exporting a vApp can take some time.

To import a vApp

OVF/OVA packages are imported as vApps.

1. Open the **Manage vApps** dialog box: on the **Pool** menu, select **Manage vApps**.
2. Select **Import** to open the **Import** wizard.

3. Follow the procedure described in Import VMs from OVF/OVA.

   When the import is complete, the new vApp appears in the list of vApps in the **Manage vApps** dialog box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- vApps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Protecting VMs and vApps

XenServer® offers a range of features to enable you to protect your VMs and vApps.

High Availability

High availability protects against downtime of critical VMs caused by the failure of individual servers in a pool. This feature guarantees that VMs are automatically restarted on an alternate server in the same pool, with minimal service interruption. XenServer constantly replicates the pool database across all nodes. The pool database is also backed up to shared storage on the heartbeat SR for extra safety.

For more information, see the following articles:

- About high availability
- High availability requirements
- VM startup settings
- Configure high availability
- Disable high availability
- Change high availability settings

Disaster recovery

Disaster recovery (DR) provides protection against the loss of multiple servers at your primary data site. With DR enabled, the pool database is constantly replicated through mirrored storage. If a disaster occurs at your primary site, DR can recover your VMs and vApps from the mirrored storage to a pool on a secondary (DR) site.

For more information, see the following articles:

- About XenServer DR
- Configuring DR
- Failover
- Failback
- Test Failover

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- High availability
- Disaster recovery

© 1997–2026 Citrix Systems, Inc. All rights reserved.

High availability

XenServer® high availability enables VMs to restart automatically in the event of an underlying hardware failure or loss of any server. High availability is about making sure important VMs are always running in a resource pool. With high availability enabled, if one of your servers fails, its VMs restart on other servers in the same pool. This capability allows essential services to be restored with minimal service interruption in the event of system or component failure.

If the pool coordinator server fails, XenServer high availability selects a new server to take over as pool coordinator. Any server in a pool can be a pool coordinator server. XenServer replicates the pool database constantly across all nodes. It also backs up the database to shared storage on the heartbeat SR for extra safety.

There are two key aspects to XenServer high availability:

- Reliably detecting server failure
- Computing a failure plan to enable swift recovery

Heartbeats for availability

Detecting server failure reliably is difficult since you need to remotely distinguish between a server disappearing for a while versus catastrophic failure. If high availability incorrectly decides a pool coordinator server has broken down and elects a new pool coordinator, there might be unpredictable results if the original server returns. Similarly, if a network issue causes the pool to split into two equal halves, we must ensure only one half accesses the shared storage and not both simultaneously. XenServer solves all these problems by having two mechanisms: a storage heartbeat and a network heartbeat.

When you enable high availability in a pool, you nominate an iSCSI, Fibre Channel or NFS storage repository to be the heartbeat SR. XenServer automatically creates a couple of small virtual disks in this SR. The first disk is used by every server in the resource pool as a shared quorum disk. Each server allocates itself a unique block in the shared disk and regularly writes to the block to indicate that it is alive. When high availability starts up, all servers exchange data over both storage channels and network channels. The network heartbeat uses a UDP transport over port 694. This action indicates which servers they can see over both channels and demonstrates which I/O paths are working and which are not. This information is exchanged until a fixed point is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

reached and all servers in the pool agree about what they can see. When this agreement happens, high availability is enabled and the pool is protected. This high availability arming process can take a few minutes to settle for larger pools, but is only required when you first enable high availability.

After high availability is active, each server regularly writes storage updates to the heartbeat virtual disk, and network packets over the management interface. Ensure that network adapters are bonded for resilience, and that storage interfaces are using dynamic multipathing where it is supported. This configuration ensures that any single adapter or wiring failures do not result in any availability issues.

For more information, see:

- Network bonding
- Storage multipathing

Server fencing

The worst-case scenario for high availability is one where a server is thought to be off-line but is still writing to the shared storage. This scenario can result in corruption of persistent data. XenServer uses server fencing to prevent this situation. The server is automatically powered off and isolated from accessing any shared resources in the pool. Fencing prevents the failing server from writing to shared disks. This behavior prevents damage to the stored data during an automated failover, when protected virtual machines are being moved to other servers in the pool.

Servers self-fence (that is, power off and restart) in the event of any heartbeat failure unless any of the following hold true:

- The storage heartbeat is present for all servers but the network has partitioned (so that there are now two groups of servers). In this case, all servers that are members of the largest network partition stay running, and the servers in the smaller network partition self-fence. The assumption here is that the network outage has isolated the VMs, and they must be restarted on a server with working networking. If the network partitions are the same size, then only one of them self-fences according to a stable selection function.
- If the storage heartbeat goes away but the network heartbeat remains, the servers check to see if they can see all other servers over the network. If this condition holds true, the servers remain running on the assumption that the storage device has failed. This action doesn't compromise VM safety, but any loss of network heartbeat results in fencing, since that would mean both heartbeats have disappeared.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Capacity planning for failure

The heartbeat system gives us reliable notification of server failure, and so we move onto the second step of high availability: capacity planning for failure.

A resource pool consists of several servers (say, 32), each with potentially different amounts of memory and a different number of running VMs. XenServer high availability dynamically computes a failure plan that calculates the actions to be taken on any server failure. This failure plan ensures that no single server failure makes it impossible to restart its VMs on another server (for example, due to insufficient memory on other servers). In addition to dealing with failure of a single server, XenServer high availability can deal with the loss of multiple servers in a pool. For example, high availability can handle when failure of a network partition takes out an entire group of servers.

In addition to calculating what actions are taken, the failure plan considers the number of server failures that can be tolerated in the pool. There are two important considerations involved in calculating the high availability plan for a pool:

- Maximum failure capacity. This value is the maximum number of servers that can fail before there are insufficient resources to run all the protected VMs in the pool. To calculate the maximum failure capacity, XenServer considers:
  - The restart priorities of the VMs in the pool
  - The number of servers in the pool
  - The server CPU and memory capacity
- Server failure limit. You can define this value as part of the high availability configuration which specifies the number of server failures to allow in the pool, within the plan. For example, when the server failure limit for a pool is 3, XenServer calculates a failover plan that allows any 3 servers to fail and all protected VMs can still run in the pool. You can configure the server failure limit to a value that is lower than the maximum failure capacity, making it less likely that the pool becomes overcommitted. This configuration can be useful in an environment with RBAC enabled. For example, this setting allows RBAC users with lower permissions than Pool Operator to bring more VMs online without breaking the high availability plan. For more information, see the *High availability and Role-Based Access Control (RBAC)* section.

A system alert is generated when the maximum failure capacity value falls below the value specified for the server failure limit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Overcommit protection

When high availability is first enabled on a pool, a failure plan is calculated based on the resources available then. XenServer high availability dynamically calculates a new failure plan in response to events which would affect the pool, for example, starting a new VM. If a new plan cannot be calculated due to insufficient resources across the pool, the pool becomes overcommitted. Examples of insufficient resources might be not enough free memory or changes to virtual disks and networks that affect which VMs might be restarted on which servers.

High availability restart priority is used to determine which VMs to start when a pool is overcommitted. When you configure the restart priority for the VMs you want to protect in the **HA Configuration** dialog box or in the **Configure HA** wizard, the maximum failure capacity for the pool is recalculated dynamically. This information enables you to try various combinations of VM restart priorities depending on your business needs. You can see if the maximum failure capacity is appropriate to the level of protection you need for the critical VMs in the pool.

If you attempt to start or resume a VM and that action would cause the pool to be overcommitted, a warning is displayed in XenCenter. The message can also be sent to an email address, if configured. You are given the option to cancel the operation, or proceed anyway, causing the pool to become overcommitted.

Working with an HA-enabled pool

The best practice for high availability is not to make configuration changes to the pool while high availability is enabled. Instead, it is intended to be the "2am safeguard" which restarts servers in the event of a problem when there isn't a human administrator nearby. If you are actively making configuration changes in the pool such as applying software updates, disable high availability during these changes.

- If you try to shut down a protected VM from XenCenter, XenCenter offers the option of removing the VM from the failure plan and then shutting it down. This option ensures that accidental VM shutdowns do not result in downtime, but that you can still stop a protected VM if you really want to.
- If you must reboot a server when high availability is enabled, XenCenter automatically uses the VM restart priorities to determine if this reboot invalidates the pool failure plan. If it doesn't affect the plan, then the server is shut down normally. If the plan is violated, but the maximum failure capacity is greater than 1, XenCenter provides the option of lowering the pool's server failure limit by 1. This action reduces the overall resilience of the pool, but always ensures that

© 1997–2026 Citrix Systems, Inc. All rights reserved.

at least one server failure is tolerated. When the server comes back up, the plan is automatically recalculated and the original server failure limit is restored if appropriate.

- When you install software updates using the **Install Updates** wizard, you must disable high availability on the pool by selecting **Turn HA off**. You can re-enable high availability after the update has been installed. If you do not disable high availability, the update does not proceed. Monitor the pool manually while updates are being installed to ensure that server failures do not disrupt the operation of the pool.
- When high availability is enabled, some operations that can compromise the plan for restarting VMs might be disabled, such as removing a server from a pool. To perform these operations, temporarily disable high availability or you can shut down the protected VMs before continuing.

High availability and role-based access control (RBAC)

In XenServer environments where role-based access control (RBAC) is implemented, not all users are permitted to change a pool's high availability configuration settings. For example, VM Operators do not have sufficient permissions to adjust the failover capacity for an HA-enabled pool. If starting a VM reduces the maximum number of allowed server failures to a value lower than the current value, a VM Operator cannot start the VM. Only Pool Administrator or Pool Operator-level users can configure the number of server failures allowed.

In this case, the Pool Administrator or Pool Operator can set the server failure limit to a number that is lower than the maximum number of failures allowed. This setting creates slack capacity and so ensures that less privileged users can start up new VMs. It reduces the pool's failover capacity without threatening the failure plan.

Related documentation

XenServer Current Release

- High availability

High availability Requirements

Before you can configure high availability on a resource pool, you must ensure that the following requirements are satisfied for all servers and virtual machines in the pool:

- Shared storage must be available. The shared storage must include at least one iSCSI, Fibre Channel or NFS LUN of at least 4 GiB that is used for the heartbeat SR. If you are using a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetApp or EqualLogic storage array, manually provision an iSCSI LUN on the array to use for the heartbeat SR.

- We strongly recommend that you use a bonded management interface on the servers in the pool.
- We strongly recommend that you use multipath storage for the heartbeat SR.
- Adequate licenses must be installed on all servers.
- All the virtual machines you want to protect with high availability must be agile. This means:
  - Virtual disks must be on shared storage. You can use any type of shared storage to store the virtual disks. The iSCSI, Fibre Channel or NFS LUN is only required for the storage heartbeat. These SRs can be used for virtual disk storage, if you prefer, but it is not necessary.
  - Virtual network interfaces must be on pool-wide networks.
  - Do not configure a connection to any local DVD drive.

  VMs that are not agile can be assigned only **Restart if possible** restart priority. These VMs are tied to one server. For example, a VM with a physical CD drive mapped in from a server can only run on the server with the CD drive.

Related documentation

XenServer Current Release

- High availability

VM Restart Settings

If more servers fail than have been planned for, then a high availability recovery operation begins. The **HA restart priority** is used to determine which VMs are restarted. The start order and delay interval values determine the order in which individual VMs are started. These settings ensure that the most important VMs are restarted first.

High availability restart priority

The **HA restart priority** specifies which VMs restart under the high availability failure plan for a pool:

- **Restart** - VMs with this priority are guaranteed to be restarted if sufficient resources are available within the pool. They restart before VMs with a **Restart if possible** priority.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

All VMs with this restart priority are considered when calculating a failure plan. If no plan exists for which all VMs with this priority can reliably restart, the pool is overcommitted.

- **Restart if possible** - VMs with this restart priority are not considered when calculating a failure plan. However, an attempt to restart these VMs is made if a server that is running them fails. This restart is attempted after all higher-priority VMs are restarted. If the attempt to start a restart-if-possible VM fails because there is not capacity to start the VM, it is not retried.

  This setting is useful for test/development VMs which aren't critical to keep running, but would be nice to do so.

- **Do not restart** - No attempts are made to restart VMs with this priority.

Start order

The **Start order** property specifies the order in which individual VMs start up during a recovery operation. This setting allows certain VMs to be started before others. VMs with a start order value of 0 (zero) start first, then VMs with a start order value of 1, and so on.

Delay interval (Attempt to start next VM after)

The **Attempt to start next VM after** property specifies how long the recovery process waits after the VMs start before starting the next VMs in the startup sequence. The next group of VMs are those VMs with a later start order.

Related documentation

XenServer Current Release

- High availability

Configure high availability

You configure high availability for a resource pool using the **Configure HA** wizard. The wizard takes you through the high availability configuration process, step-by-step. During this process, the wizard calculates the server failure limit for the pool given the available resources and the high availability restart priorities you specify.

To open the **Configure HA** wizard: in XenCenter®, select the pool, select the **HA** tab, and then select **Configure HA**.

Alternatively:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On the **Pool** menu, select **High Availability** > **Configure HA...**.
- Right-click the pool in the **Resources** pane and then select **High Availability** > **Configure HA...** from the context menu.

To configure high availability on a pool:

1. Ensure that the high availability requirements are satisfied. For more information, see High availability requirements.
2. Open the **Configure HA** wizard.
3. Click **Next** on the first page of wizard. The wizard scans the pool for a shared iSCSI, Fibre Channel or NFS LUN to use as the heartbeat SR. If no suitable SR is found, configure some appropriate new storage before you continue.
4. On the **Heartbeat SR** page, choose an SR from the list and then click **Next**.
5. On the **HA Plan** page, select one or more VMs in the list and set the required VM startup settings. For more on these options, see VM startup settings.

   Set the following options:

   - **HA restart priority**: Choose a restart priority for each VM:
     - Choose **Restart** to ensure the selected VMs are restarted if sufficient resources are available within the pool.
     - Choose **Restart if Possible** if it is not essential to restart the VM automatically.
     - Choose **Do Not Restart** if you never want the VM to be restarted automatically.
   - **Start order**: Specifies the order in which individual VMs start during the recovery operation, allowing certain VMs to be started before others. VMs with a start order value of 0 (zero) start first, then VMs with a start order value of 1, and so on.
   - **Attempt to start next VM after**: Set a delay interval to wait after starting the VM before attempting to start the next group of VMs in the startup sequence. The next group of VMs are those VMs with a lower start order.
6. Automatically reboot VMs on internal shutdown.

   If selected, HA will attempt to restart VMs even when the VM stopped due to a clean shutdown triggered by a user within the VM.
7. Also on the **HA Plan** page, under **Server failure limit**, you can set the number of server failures to allow within this high availability plan. Ensure this value is less than or equal to the maximum failure capacity for the pool, shown here as max. If max is 0 (zero), the pool is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

overcommitted, and you cannot continue until you resolve the situation. To stop the pool being overcommitted, either adjust the high availability restart priorities or make more resources available within the pool. For more information, see To increase the maximum failure capacity for a pool. Click **Next** when you have finished high availability plan configuration.

8. On the last page of the wizard, review your high availability configuration settings. Click **Back** to go back and change any of the settings or click **Finish** to enable high availability and close the wizard.

Related documentation

XenServer Current Release

- High availability

Disable high availability

When high availability is enabled, some operations that can compromise the plan for restarting VMs might be disabled, such as removing a server from a pool. To perform these operations, you can temporarily disable high availability.

To disable high availability:

1. Select the pool in the **Resources** pane, select the **HA** tab, and then select **Disable HA**.

   Alternatively, in the **Pool** menu, select **High Availability** > **Disable HA**.

   You can also right-click on the pool in the **Resources** pane and choose **High Availability** > **Disable HA** from the context menu.

2. Click **OK** to confirm. The restart priorities specified for each VM in the pool are stored and remembered if you turn high availability back on again later.

Related documentation

XenServer Current Release

- High availability

Enable high availability

If high availability was previously configured and then disabled, the restart priorities defined for each VM in the pool are saved and retained.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can re-enable high availability to reuse these same settings in one of the following ways:

- Select the pool in the **Resources** pane, select the **HA** tab, and then select **Enable HA**.
- In the **Pool** menu, select **High Availability** > **Enable HA**.
- Right-click on the pool in the **Resources** pane and choose **High Availability** > **Enable HA** from the context menu.

Related documentation

XenServer Current Release

- High availability

Change High Availability settings

When a pool has high availability enabled, use the **Configure HA** dialog box to change VM startup settings and the server failure limit for the pool.

To change high availability restart priority and VM startup sequence settings

1. Select the pool in the **Resources** pane, choose the **HA** tab, and then select **Configure HA**. Alternatively:
   - On the **Pool** menu, select **High Availability**.
   - Right-click in the **Resources** pane and then select **High Availability** on the shortcut menu.
2. Select one or more VMs in the list and set the required VM startup settings. For more on these options, see VM startup settings.

   Set the following options:

   - **HA restart priority**: Choose a restart priority for each VM:
     - Choose **Restart** to ensure the selected VMs are restarted if sufficient resources are available within the pool.
     - Choose **Restart if Possible** if it is not essential to restart the VM automatically.
     - Choose **Do Not Restart** if you never want the VM to be restarted automatically.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Start order** : Specifies the order in which individual VMs start up during the recovery operation, allowing certain VMs to be started before others. VMs with a start order value of 0 (zero) start first, then VMs with a start order value of 1, and so on.

3. Attempt to start next VM after.

   Set the delay interval to wait after starting the VM before starting the next group of VMs in the startup sequence. The next group of VMs are those VMs with a lower start order.

4. Automatically reboot VMs on internal shutdown.

   If selected, HA will attempt to restart VMs even when the VM stopped due to a clean shutdown triggered by a user within the VM.

5. Click **OK** to apply the changes and close the dialog box.

To change the server failure limit for a pool

1. Select the pool in the **Resources** pane, select the **HA** tab, and then click **Configure HA**. Alternatively:

   - On the **Pool** menu, select **High Availability**.
   - Right-click in the **Resources** pane and then select **High Availability** on the shortcut menu.

2. Under **Server failure limit**, enter the number of server failures to allow. Ensure this value is less than or equal to the maximum failure capacity for the pool, shown here as max. If max is 0 (zero), the pool is overcommitted, and you cannot save the change. To be able to save the change, either adjust the high availability restart priorities or make more resources available within the pool. For more information, see the following section.
3. Click **OK** to apply the changes and close the dialog box.

To increase the maximum failure capacity for a pool

To increase the maximum failure capacity for a pool, you need to do one or more of the following:

- Reduce the high availability restart priority of some VMs.
- Increase the amount of RAM on your servers or add more servers to the pool to increase its capacity.
- Reduce the amount of memory configured on some VMs.
- Shut down non-essential VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- High availability

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Disaster Recovery (DR)

The disaster recovery (DR) feature allows you to recover VMs and vApps from a catastrophic failure of hardware which disables or destroys a whole pool or site.

For protection against single server failures, you can use High Availability. High availability restarts VMs on an alternate server in the same pool.

Understanding DR

Disaster recovery stores all the information needed to recover your business-critical VMs and vApps on storage repositories (SRs). These storage repositories are then replicated from your primary (production) environment to a backup environment. When a protected pool at your primary site fails, the VMs and vApps in that pool can be recovered from the replicated storage and recreated on a secondary (DR) site. The result is minimal application or user downtime.

After the recovered VMs are up and running in the DR pool, the DR pool metadata must also be saved on storage that is replicated. This action allows recovered VMs and vApps to be restored back to the primary site when it is back online.

NOTE:

Disaster Recovery can only be used with LVM over HBA or LVM over iSCSI storage types.

XenServer® VMs consist of two components:

- Virtual disks that are being used by the VM, stored on configured storage repositories (SRs) in the pool where the VMs are located.
- Metadata describing the VM environment. The metadata contains all the information required to recreate the VM if the original VM is unavailable or corrupted. Most metadata is written when the VM is created and is updated only when you change the VM configuration. For VMs in a pool, a copy of this metadata is stored on every server in the pool.

In a DR environment, VMs are recreated on a secondary (DR) site from the pool metadata - configuration information about all the VMs and vApps in the pool. The metadata for each VM includes its name, description and Universal Unique Identifier (UUID), and its memory, virtual CPU, networking, and storage configuration. It also includes the VM startup options used when restarting

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the VM in a high availability or DR environment: start order, delay interval, and restart priority. For example, when recovering VMs, the VMs within a vApp restart in the DR pool in the order and with the delay intervals specified in the metadata.

NOTE:

To use Disaster Recovery, you must be logged in as root or have a role of Pool Operator or higher.

Disaster recovery terminology

vApp: A logical group of related VMs which are managed as a single entity.

Site: A physical group of XenServer resource pools, storage, and hardware equipment.

Primary site: A physical site that runs VMs or vApps which must be protected in the event of disaster.

Secondary site, DR site: A physical site whose purpose is to serve as the recovery location for the primary site, in the event of a disaster.

Failover: Recovery of VMs and vApps on a secondary (recovery) site in the event of disaster at the primary site.

Failback: Restoration of VMs and vApps back to the primary site from a secondary (recovery) site.

Test failover: A "dry run" failover where VMs and vApps are recovered from replicated storage to a pool on a secondary (recovery) site but not started up. Test failovers can be run to check that DR is correctly configured and that your processes are effective.

Pool metadata: Information about the VMs and vApps in the pool, such as their name and description. For VMs, the configuration information includes UUID, memory, virtual CPU, networking and storage configuration, and startup options. Pool metadata is used in DR to re-create the VMs and vApps from the primary site in a recovery pool on the secondary site.

Disaster recovery infrastructure

To use Disaster Recovery, set up the appropriate DR infrastructure at both the primary and secondary sites:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The storage used for both the pool metadata and the virtual disks used by the VMs must be replicated from your primary (production) environment to a backup environment. Storage replication, for example using mirroring, varies from device to device. We recommend you use your storage solution to handle storage replication.
- After recovered VMs and vApps are up and running on a pool on your DR site, replicate the SRs containing the DR pool metadata and virtual disks. This action allows the recovered VMs and vApps to be restored back to the primary site (failed back) once the primary site is back online.
- The hardware infrastructure at your DR site does not have to match the primary site. However, the XenServer environment must be at the same release and patch level. Also, sufficient resources must be configured in the target pool to allow all the failed over VMs to be re-created and started.

IMPORTANT:

XenCenter® and the **Disaster Recovery** wizard do not control any storage array functionality. Ensure the pool metadata, and the storage used by the VMs which are to be restarted in the event of a disaster, are replicated to a backup site. Some storage arrays contain mirroring features to achieve the copy automatically. If these features are used, disable the mirror functionality before VMs are restarted on the recovery site.

Failover, failback, and test failover with the Disaster Recovery wizard

The **Disaster Recovery** wizard makes failover and failback simple. The steps involved in these processes are outlined here:

Failover

1. Choose a target pool on your secondary DR site to which you want to recover your VMs and vApps.
2. Provide details of the storage targets containing the replicated SRs from your primary site. The wizard scans the targets and lists all SRs found there.
3. Select the SRs containing the metadata and virtual disks for the VMs and vApps you want to recover. The wizard scans the SRs and lists all the VMs and vApps found.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select which VMs and vApps you want to recover to the DR site. Specify whether you want the wizard to start them up automatically when they have been recovered, or whether you prefer to wait and start them up manually yourself.

   The wizard performs pre-checks to ensure that the selected VMs and vApps can be recovered to the target DR pool. For example, the wizard checks that all the storage required by the selected VMs and vApps is available.

When the pre-checks are complete and any issues resolved, the failover process begins. The selected VMs and vApps are exported from the replicated storage to the DR pool. Failover is now complete.

Failback

1. Choose the target pool on your primary site to which you want to restore the VMs and vApps currently running on the DR site.
2. Provide details of the storage targets containing the replicated SRs from your DR site. The wizard scans the targets and lists all SRs found.
3. Select the SRs containing the metadata and virtual disks for the VMs and vApps you want to restore. The wizard scans the SRs and lists all the VMs and vApps found.
4. Select which VMs and vApps you want to restore back to the primary site. Specify whether you want the wizard to start them up automatically when they have been recovered, or whether you prefer to wait and start them up manually yourself.

   The wizard then performs pre-checks to ensure that the selected VMs and vApps can be recovered to the target pool on the primary site. For example, the wizard checks that all the storage required by the selected VMs and vApps is available.

When the pre-checks are complete and any issues resolved, the failback process begins. The selected VMs and vApps running on your DR site are exported from the replicated storage back to the selected pool at your primary site.

Failback is now complete.

If the **Disaster Recovery** wizard finds information for the same VM in a two or more places, it uses only the most recent information per VM. For example, the information might be stored on the primary site storage, the DR site storage, and in the pool the data is imported into.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP:

To make recovering VMs and vApps easier, name your SRs to indicate how your VMs and vApps are mapped to SRs, and the SRs to LUNs.

You can also use the **Disaster Recovery** wizard to run test failovers for non-disruptive testing of your disaster recovery system. In a test failover, the steps are the same as for failover, but recovered VMs and vApps are started up in a paused state on the DR site. Cleanup is performed when the test is finished to remove all VMs, vApps, and storage recreated on the DR site. For more information, see Test Failover.

Related documentation

XenServer Current Release

- Disaster recovery and backup

Configuring disaster recovery

Use the XenCenter® **Configure DR** dialog box to choose the storage repositories (SRs) to store the metadata for a pool. This metadata includes configuration information about all the VMs and vApps in the pool. Pool metadata is updated whenever you change the VM or vApp configuration.

NOTE:

XenServer® DR supports only LVM over HBA or LVM over iSCSI storage types.

To configure disaster recovery on the primary pool:

1. On your primary site, select the pool that you want to protect.
2. On the **Pool** menu, choose **Disaster Recovery** and click **Configure**.
3. Select up to eight SRs where the pool metadata is stored. A small amount of space is required on this storage for a new LUN which contains the pool recovery information.
4. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

To configure your DR environment fully, replicate the SRs that contain the pool metadata and VM virtual disks from your production environment to a backup environment. Storage replication cannot be configured from within XenCenter. Use your storage solution to handle storage replication, for example using mirroring. The replication varies from device to device.

Related documentation

XenServer Current Release

- Enable Disaster Recovery

Failover

Failover recovers VMs and vApps to a secondary site in the event of disaster at your primary site. To fail over your critical VMs and vApps, use the **Disaster Recovery** wizard.

IMPORTANT:

The **Disaster Recovery** wizard does not control any storage array functionality. Disable duplication (mirroring) of the metadata storage and the storage used by the VMs to be restarted before you attempt failover to your recovery site.

To fail over VMs and vApps to a secondary site:

1. In XenCenter®, select the secondary pool, and on the **Pool** menu, click **Disaster Recovery** to open the **Disaster Recovery** wizard.
2. Select **Failover** and then click **Next**.

   NOTE:

   If you use Fibre Channel shared storage with LUN mirroring to replicate the data to the secondary site, break mirroring before you attempt to recover data. This action gives the secondary site Read/Write access.

3. Select the storage repositories (SRs) containing the pool metadata for the VMs and vApps that you want to recover. By default, the list on this wizard page shows all SRs that are currently

© 1997–2026 Citrix Systems, Inc. All rights reserved.

attached within the pool. To scan for more SRs, choose **Find Storage Repositories** and then select the storage type to scan for:

- To scan for all the available Hardware HBA SRs, select **Find Hardware HBA SRs**.
- To scan for software iSCSI SRs, select **Find Software iSCSI SRs** and then enter the target host, IQN, and LUN details in the dialog box.

When you have selected the required SRs in the wizard, click **Next** to continue.

4. Select the VMs and vApps that you want to recover. Use the **Power state after recovery** option to specify whether you want the wizard to start the recovered VMs and vApps immediately. Alternatively, you can wait and start the VMs and vApps manually after failover is complete.
5. Click **Next** to progress to the next wizard page and begin failover pre-checks.

   The wizard performs pre-checks before starting failover. For example, the wizard ensures all the storage required by the selected VMs and vApps is available. If any storage is missing at this point, you can click **Attach SR** on this page to find and attach the relevant SR.
6. Resolve any issues on the pre-checks page, and then click **Failover** to begin the recovery process.

   A progress page is displayed showing whether recovery was successful for each VM and vApp.

   Failover can take some time depending on the number of VMs and vApps you are recovering. During this process, the following actions occur:

   - Metadata for the VMs and vApps is exported from the replicated storage
   - VMs and vApps are re-created in the primary pool
   - SRs containing the virtual disks are attached to the re-created VMs
   - VMs are started, if specified
7. When the failover is complete, click **Next** to see the summary report.
8. Click **Finish** on the summary report page to close the wizard.

After your primary site is available again, you can return the VMs and vApps to that site. To complete this process, follow the **Disaster Recovery** wizard again, but instead select the **Failback** option. For more information, see Failback.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- Disaster recovery and backup

Failback

Failback restores VMs and vApps from replicated storage back to a pool on your primary site. Failback occurs when the primary site comes back up after a disaster event. To fail back VMs and vApps to your primary site, use the **Disaster Recovery** wizard.

IMPORTANT:

The **Disaster Recovery** wizard does not control any storage array functionality. Disable duplication (mirroring) of the metadata storage and the storage used by the VMs which are to be restored before you attempt failback to your primary site.

To fail back VMs and vApps to your primary site:

1. In XenCenter®, select the target pool on your primary site, and on the **Pool** menu, click **Disaster Recovery** to open the **Disaster Recovery** wizard.
2. Select **Failback** and then click **Next**.

   NOTE:

   If you use Fibre Channel shared storage with LUN mirroring to replicate the data on the DR site, break mirroring before you attempt to recover data. This action gives the primary site Read/Write access.

3. Select the storage repositories (SRs) containing the pool metadata for the VMs and vApps that you want to restore back to your primary site. By default, the list on this wizard page shows all SRs that are currently attached within the pool. To scan for more SRs, choose **Find Storage Repositories** and then select the storage type to scan for:

   - To scan for all the available Hardware HBA SRs, select **Find Hardware HBA SRs**.
   - To scan for software iSCSI SRs, select **Find Software iSCSI SRs** and then enter the target host, IQN, and LUN details in the dialog box.

   When you have selected the required SRs in the wizard, click **Next** to continue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Choose the VMs and vApps that you want to restore. Use the **Power state after recovery** option to specify whether to start the restored VMs and vApps automatically. Alternatively, you can wait and start the VMs and vApps manually after failback is complete.
5. Click **Next** to progress to the next wizard page and begin failback pre-checks.

   The wizard performs pre-checks before starting failback. For example, the wizard ensures all the storage required by the selected VMs and vApps is available. If any storage is missing at this point, you can click **Attach SR** on this page to find and attach the relevant SR.
6. Resolve any issues on the pre-checks page, and then click **Failback** to begin the recovery process.

   A progress page is displayed showing whether restoration was successful for each VM and vApp. Failback can take some time depending on the number of VMs and vApps you are restoring.
7. When the failback is complete, click **Next** to see the summary report.
8. Click **Finish** on the summary report page to close the wizard.

Related documentation

XenServer Current Release

- Disaster recovery and backup

Test Failover

Failover testing is an essential component in disaster recovery planning. You can use the **Disaster Recovery** wizard to perform non-disruptive testing of your disaster recovery system. During a test failover operation, all the steps are the same as for failover. However, instead of starting after they are recovered to the DR site, the VMs and vApps are placed in a paused state. At the end of test failover, the wizard automatically removes all VMs, vApps, and storage recreated on the DR site.

After initial DR configuration, verify that failover works correctly by performing a test failover. We recommend you also do a test failover after you make significant configuration changes in a DR-enabled pool.

To perform a test failover of VMs and vApps to a secondary site:

1. In XenCenter®, select the secondary pool, and on the **Pool** menu, click **Disaster Recovery** to open the **Disaster Recovery** wizard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select **Test Failover** and then click **Next**.

   NOTE:

   If you use Fibre Channel shared storage with LUN mirroring to replicate the data to the secondary site, break mirroring before you attempt to recover data. This action gives the secondary site Read/Write access.

3. Select the storage repositories (SRs) containing the pool metadata for the VMs and vApps that you want to recover. By default, the list on this wizard page shows all SRs that are currently attached within the pool. To scan for more SRs, choose **Find Storage Repositories** and then select the storage type to scan for:

   - To scan for all the available Hardware HBA SRs, select **Find Hardware HBA SRs**.
   - To scan for software iSCSI SRs, select **Find Software iSCSI SRs** and then enter the target host, IQN, and LUN details in the dialog box.

   When you have selected the required SRs in the wizard, click **Next** to continue.

4. Select the VMs and vApps that you want to recover.
5. Click **Next** to progress to the next wizard page and begin failover pre-checks.

   Before beginning the test failover process, the wizard performs pre-checks. For example, the checks ensure all the storage required by the selected VMs and vApps is available.

   a. **Check that storage is available.** If any storage is missing, you can click **Attach SR** on this page to find and attach the relevant SR.

   b. **Check that HA is not enabled on the target DR pool.** To avoid having the same VMs running on both the primary and DR pools, disable high availability on the secondary pool. This action ensures that high availability does not automatically start the recovered VMs and vApps after recovery. To disable high availability on the secondary pool, click **Disable HA** on this page. (If the wizard disables high availability at this point, it is enabled again automatically at the end of the test failover process.)

6. Resolve any issues on the pre-checks page, and then click **Failover** to begin the test failover.

   A progress page is displayed showing whether recovery was successful for each VM and vApp. Failover can take some time depending on the number of VMs and vApps you are recovering. The following actions occur during this process:

   - Metadata for the VMs and vApps is recovered from the replicated storage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VMs and vApps are re-created in the DR pool
- SRs containing the virtual disks are attached to the re-created VMs
- **The recovered VMs are placed in a paused state. The VMs are not started on the secondary site during a test failover.**

7. After you are satisfied that the test failover was performed successfully, click **Next** in the wizard to have the wizard clean up on the DR site:

   - VMs and vApps that were recovered during the test failover are removed.
   - Storage that was recovered during the test failover is detached.
   - If the wizard disabled high availability on the DR pool at the pre-checks stage to allow the test failover to take place, it is enabled again.

   The progress of the cleanup process is displayed in the wizard.

8. Click **Finish** to close the wizard.

Related documentation

XenServer Current Release

- Disaster recovery and backup

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access Control (AD and RBAC)

- Managing Users
- RBAC Overview
- Definitions of RBAC Roles and Permissions
- Join a Domain and Add Users
- Assign Roles to Users and Groups
- Calculating RBAC Roles
- Audit Changes to XenServer

Related documentation

XenServer Current Release

- Users

Managing Users

When you first install XenServer, a user account is added to XenServer automatically. This account is the local super user (LSU), or `root`, which the XenServer system authenticates locally. You can create extra users by adding Active Directory accounts from the **Users** tab in XenCenter.

NOTE:

The term "user" refers to anybody with a XenServer® account, that is, anyone administering XenServer hosts, regardless of the level of their role.

If you want to have multiple user accounts on a server or a pool, you must use Active Directory user accounts for authentication. This feature allows XenServer users to log in to the servers in a pool using their Windows domain credentials.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Mixed-authentication pools are not supported. That is, you cannot have a pool where some servers in the pool use Active Directory and some don't.

When you create a user in XenServer you must first assign a role to the newly created user before they can use the account. XenServer **does not** automatically assign a role to the newly created user. As a result, these accounts do not have any access to the XenServer pool until you assign them a role.

Using the Role Based Access Control (RBAC) feature, you can assign the Active Directory accounts different levels of permissions depending on the user's role. If you do not use Active Directory in your environment, you are limited to the LSU account.

AD authentication in XenServer environment

Even though the XenServer servers are Linux-based, XenServer lets you use Active Directory accounts for XenServer user accounts. To do so, it passes Active Directory credentials to the Active Directory domain controller.

NOTE:

You can enable LDAP channel binding and LDAP signing on your AD domain controllers. For more information, see Microsoft Security Advisory.

When added to XenServer, Active Directory users and groups become XenServer subjects, called users in XenCenter. When a subject is registered with XenServer, users and groups are authenticated with Active Directory on login. These users and groups do not need to qualify their user name with a domain name.

To qualify a user name, you must enter the user name in Down-Level Logon Name format, for example, `mydomain\myuser`.

NOTE:

By default, if you don't qualify the user name, XenCenter attempts to log users in to Active Directory authentication servers using the domain to which it is joined. The exception to this rule is the LSU account, which XenCenter always authenticates locally (that is, on XenServer) first.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The external authentication process works as follows:

1. The credentials supplied when connecting to a server are passed to the Active Directory domain controller for authentication.
2. The domain controller checks the credentials. If they are invalid, the authentication fails immediately.
3. If the credentials are valid, the Active Directory controller is queried to get the subject identifier and group membership associated with the credentials.
4. If the subject identifier matches the one stored in XenServer, the authentication is completed successfully.

When you join a domain, you enable Active Directory authentication for the pool. However, when a pool is joined to a domain, only users in that domain (or a domain with which it has trust relationships) can connect to the pool.

Related documentation

XenServer Current Release

- Users

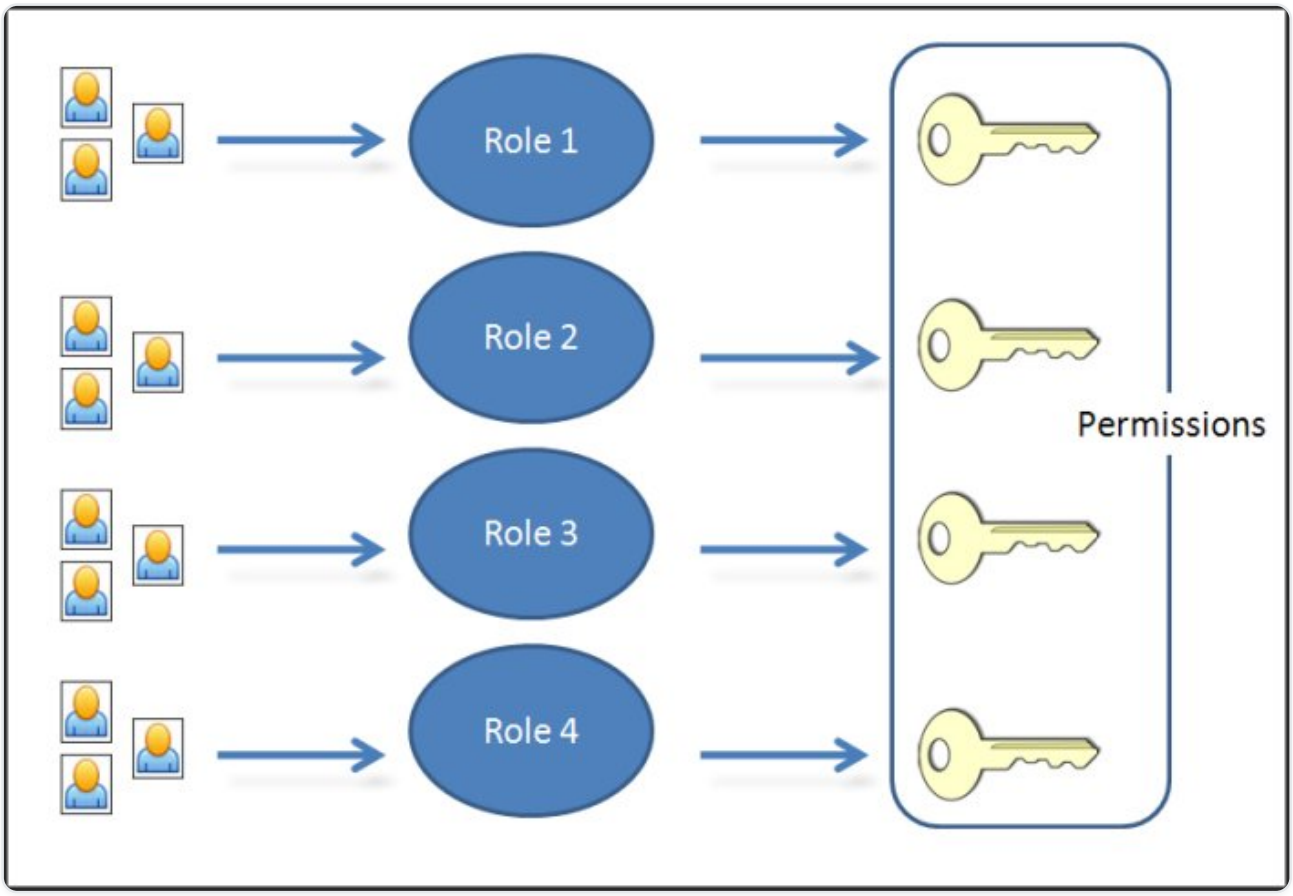
Role Based Access Control overview

The Role Based Access Control (RBAC) feature lets you assign predefined roles or sets of permissions to Active Directory users and groups. These permissions control the level of access XenServer® administrators have to servers and pools. RBAC is configured and deployed at the pool level. Because users acquire permissions through their assigned role, assign a role to a user or their group to give them the required permissions.

Using Active Directory accounts for XenServer user accounts

RBAC lets you restrict which operations different groups of users can perform. This control reduces the likelihood of inexperienced users making disastrous accidental changes. Assigning RBAC roles also helps prevent unauthorized changes to your resource pools for compliance reasons. To facilitate compliance and auditing, RBAC also provides an audit log feature and its corresponding Workload Balancing Pool Audit Trail report. For more information, see Audit Changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



RBAC depends on Active Directory for authentication services. Specifically, XenServer keeps a list of authorized users based on Active Directory user and group accounts. As a result, you must join the pool to the domain and add Active Directory accounts before you can assign roles.

RBAC process

The standard process for implementing RBAC and assigning a user or group a role consists of the following steps:

1. Join the domain.
2. Add an Active Directory user or group to the pool.
3. Assign (or modify) the user or group's RBAC role.

Local super user

The local super user (LSU), or root, is a special user account used for system administration and has all rights or permissions. In XenServer, the local super user is the default account at installation. The LSU is authenticated by XenServer and not an external authentication service. If the external authentication service fails, the LSU can still log in and manage the system. The LSU can always access XenServer physical server through SSH.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RBAC roles

XenServer comes with six pre-established roles that are designed to align with different functions in an IT organization.

- **Pool Administrator (Pool Admin)**. This role is the most powerful role available. Pool Admins have full access to all XenServer features and settings. They can perform all operations, including role and user management. They can grant access to XenServer console. As a best practice, Citrix® recommends assigning this role to a limited number of users.

  NOTE:

  The local super user (root) always has the Pool Admin role. The Pool Admin role has the same permissions as the local root.

  If you remove the Pool Admin role from a user, consider also changing the root password and rotating the pool secret. For more information, see Pool Security.

- **Pool Operator (Pool Operator)**. This role is designed to let the assignee manage pool-wide resources. Management actions include creating storage, managing servers, managing patches, and creating pools. Pool Operators can configure pool resources. They also have full access to the following features: high availability, Workload Balancing, and patch management. Pool Operators cannot add users or modify roles.
- **Virtual Machine Power Administrator (VM Power Admin)**. This role has full access to VM and Template management. They can choose where to start VMs. They have full access to the dynamic memory control features and the VM snapshot feature. In addition, they can set the Home Server and choose where to run workloads. Assigning this role grants the assignee sufficient permissions to provision virtual machines for VM Operator use.
- **Virtual Machine Administrator (VM Admin)**. This role can manage VMs and Templates and access the storage necessary to complete these tasks. However, this role relies on XenServer to choose where to run workloads and must use the settings in templates for dynamic memory control and the Home Server. (This role cannot access the dynamic memory control features, make snapshots, set the Home Server or choose where to run workloads.)
- **Virtual Machine Operator (VM Operator)**. This role can use the VMs in a pool and manage their basic lifecycle. VM Operators can interact with the VM consoles and start or stop VMs, provided sufficient hardware resources are available. Likewise, VM Operators can perform start and stop lifecycle operations. The VM Operator role cannot create or destroy VMs, alter VM properties, or server resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Read-only (Read Only)**. This role can only view resource pool and performance data.

For information about the permissions associated with each role, see Definitions of RBAC roles and permissions. For information about how RBAC calculates which roles apply to a user, see Calculating RBAC roles.

NOTE:

When you create a user, you must first assign a role to the newly created user before they can use the account. XenServer **does not** automatically assign a role to the newly created user.

Related documentation

XenServer Current Release

- Role-Based Access Control

Definitions of RBAC roles and permissions

To see the RBAC roles and permissions in XenServer®, refer to the documentation for the version of XenServer you are using:

- XenServer RBAC roles and permissions

Join a domain and add users

Before you can assign a user or group account an RBAC role, you must add the account to XenServer® through RBAC. This process consists of the following tasks:

1. Join the pool or server to the domain. The domain can be one of the following:
   - The domain that the user or group belongs to
   - A domain that is in the same Active Directory forest
   - A domain that has a trust relationship with the user's domain
2. Add the user's Active Directory account or group to XenServer.

After you add the user's Active Directory account or group to XenServer, the user is assigned a fixed role of Pool Admin. In XenServer Premium Edition, you must assign a role to the user or group manually. For more information, see Assign roles to users and groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To change domains, leave the current domain and then join the new domain.

Secure LDAP (LDAPS)

LDAPS protects LDAP traffic between XenServer and your Active Directory domain controllers by using TLS on port 636.

Before you enable LDAPS, ensure that LDAPS certificates are configured on your domain controllers and that you have the required CA certificates installed in the pool. For the detailed prerequisites and certificate requirements, see Secure LDAP (LDAPS).

When LDAPS is enabled, XenServer validates each domain controller certificate against the trusted CA certificates that you install in the pool.

NOTE:

XenServer validates certificate chains against CA certificates only. Leaf or self-signed (non-CA) certificates are not supported.

To join the XenServer or pool to a domain

1. In the **Resources Pane**, select the pool or server for which you want to grant somebody permissions.
2. Select the **Users** tab.
3. Select **Join Domain**.
4. Enter Active Directory credentials with sufficient privileges to add servers to the domain you want to join. The domain to be joined must be specified as a fully qualified domain name (FQDN) rather than a NetBIOS name. For example, enter `your_domain.net` instead of `your_domain`.
5. To join with LDAPS, select the **Use LDAP over TLS (LDAPS) for secure AD communication** check box, and then click **OK**. This check box appears only when your XenServer version supports LDAPS.

   If a certificate error appears, click **Install Certificate...** in the error dialog, browse to the CA certificate in PEM format, and click **Install**. After the certificate is installed, XenCenter automatically retries the domain join.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When a pool or server is joined to a domain, the **Users** tab shows the access protocol (LDAP or LDAPS). To change the LDAPS setting, click **Configure...**, select or clear the **Use LDAP over TLS (LDAPS) for secure AD communication** check box, and then click **OK**.

To add an Active Directory user or group to a pool

1. After joining the user's domain, in the **Users** tab, click **Add**.
2. In the **Add Users** dialog box, enter one or more user or group names. Separate multiple names by commas. To specify a user in a different trusted domain (other than the one currently joined), supply the domain name with the user name. For example, specify `other_domain\jsmith`. Alternatively, you can enter a fully qualified domain name (FQDN). For example, specify `jsmith@other_domain.com`.
3. Select **Grant Access**.
4. Follow Assign roles to users and groups to assign the account a role and grant access.

To leave the domain

NOTE:

When you leave the domain, any users who authenticated to the pool or server with Active Directory credentials are disconnected.

1. In the **Resources Pane**, select the pool or server that you want to disconnect from its Active Directory domain.
2. Select **Leave Domain** and select **Yes** to continue.
3. Enter Active Directory credentials with sufficient privileges to disable servers in the domain you want to leave.
4. Decide whether to disable the computer accounts in the Active Directory server, and then click one of the following:

   - **Disable**. Removes the pool or server from the domain and disables the computer account for the server or pool coordinator in the Active Directory database.
   - **Ignore**. If you didn't fill the username/password or know an account with sufficient privileges, select this option to remove the server or pool coordinator's computer account from the Active Directory database. This option removes the pool or server from the domain, but leaves the computer account for the server or pool coordinator in the Active Directory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- Users

Assign roles to users and groups

All XenServer® users must have an RBAC role. In XenServer, you must first assign a role to the newly created user before they can use the account. XenServer does not automatically assign a role to the newly created user. As a result, these accounts do not have any access to the XenServer pool until you assign them a role.

NOTE:

Before you can assign a role to a user or group, you must add the user or group's Active Directory account to the XenServer pool. Add the AD account after joining the associated domain. For more information, see Join a domain and add RBAC users.

You can assign a user a different role by one of the following methods:

1. Change the role assigned to the user in the **Select Roles** dialog in XenCenter. This action requires the **Assign/modify role** permission, which is only available to a Pool Administrator.
2. Modify the user's group membership in your Active Directory to make the user part of a group that is assigned a different role.

If an administrator indirectly applies multiple roles to a user, XenServer grants the user the permissions from the highest role that the user is assigned to.

To change or assign a role to a user or group

1. In the **Resources** pane, select the pool or server that contains the user or group.
2. Select the **Users** tab.
3. In the **Users and Groups with Access** pane, select the user or group to which you want to assign permissions.
4. Select **Change Role**.
5. In the **Select Roles** dialog, select the role you want to apply and click **Save**. For information about the permissions associated with each role, see Definitions of RBAC roles and permissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP:

When you are assigning a role, you can select multiple users simultaneously by pressing the **CTRL** key and selecting the user accounts.

6. (Optional) When changing a role, if the user is logged on to the pool and you want them to receive their new permissions immediately, click **Logout User**. This action disconnects the user's sessions on the pool so the user receives a new session with the modified role.

NOTE:

When changing a role, the user must log out and log back in again for the new role to take effect. Force this log out by clicking the **Logout User** button. To force a logout, the user requires the **Logout active user connections** permission. This permission is available to a Pool Administrator or Pool Operator.

NOTE:

If you remove the Pool Admin role from a user, consider also changing the root password and rotating the pool secret. For more information, see Pool Security.

Related documentation

XenServer Current Release

- Assign an RBAC role to a subject

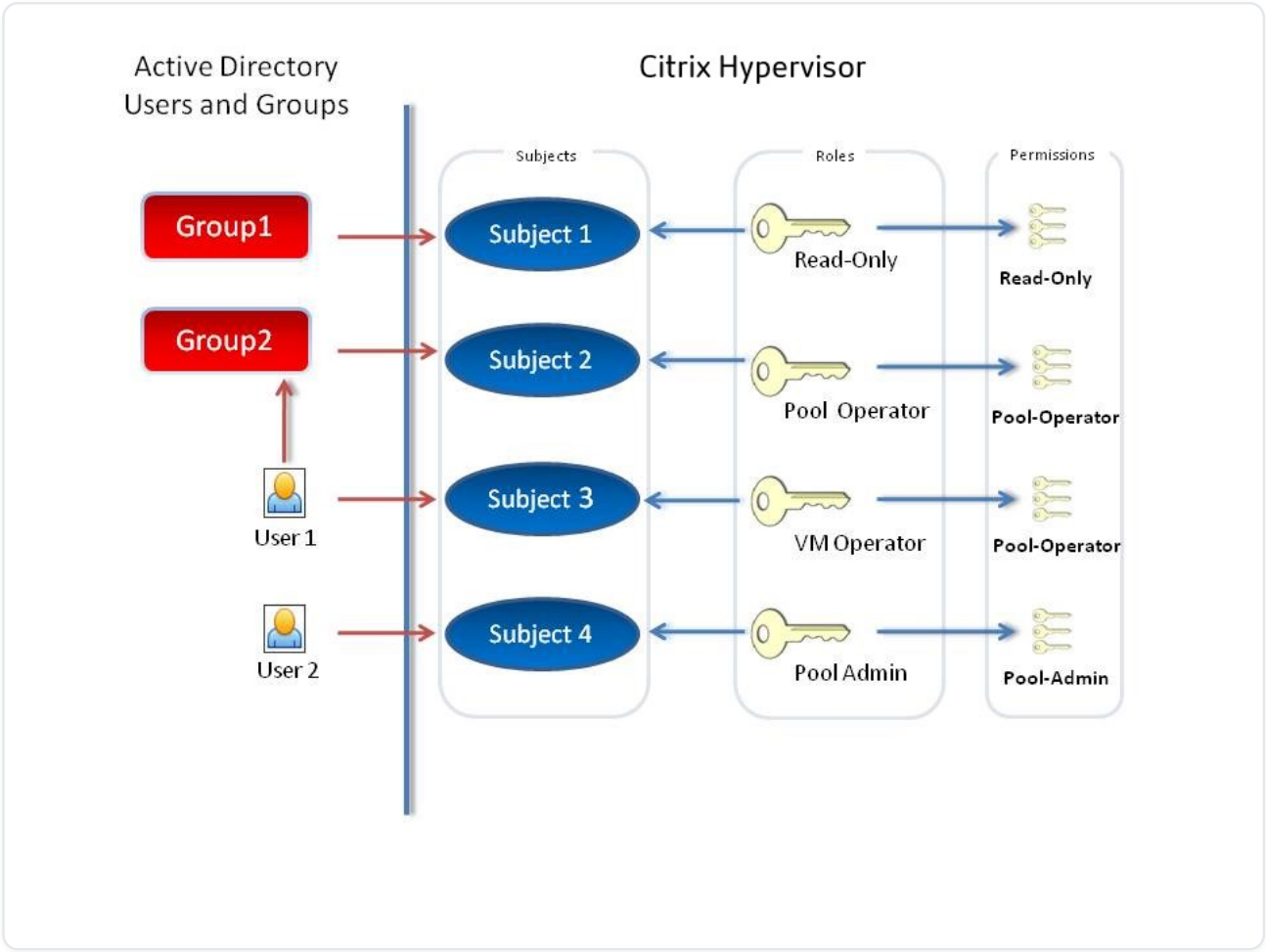
Calculating RBAC roles

When I log in, how does XenServer® compute the roles for the session?

1. The Active Directory server authenticates the subject. During authentication, Active Directory also determines if the subject belongs to any other containing groups in Active Directory.
2. XenServer then verifies the following information:
   - The roles assigned to the subject
   - The roles assigned to any Active Directory groups that the subject is a member of.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. XenServer applies the highest level of permissions to the subject. Because subjects can be members of multiple Active Directory groups, they inherit all permissions of the associated roles.



This illustration shows the following information:

- Subject 2 (Group 2) is the Pool Operator.
- User 1 is a member of Group 2.
- When Subject 3 (User 1) tries to log in, they inherit both Subject 3 (VM Operator) and Group 2 (Pool Operator) roles.
- The Pool Operator role is higher, so the resulting role for Subject 3 (User 1) is Pool Operator and not VM Operator.

Related documentation

XenServer Current Release

- How does XenServer compute the roles for the session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Audit changes

The XenServer® audit log, which is enabled by default, records any operation with side-effects performed by a known user. The operation is recorded whether it is successful or unsuccessful. This audit log includes:

- The user's name who performed the action. If the user's name is not available, XenServer logs the user ID instead.
- The server name that the action targeted.
- The status of the action - if it was successful or unsuccessful and if it was authorized. if the operation failed then the error code is logged.

The audit logging feature is enabled by default. The audit log can be backed up by using the XenServer `syslog` command to duplicate the audit log to a safe box. The syslog command is available from the xe CLI and documented in Command line interface.

If you are concerned with auditing, we recommend you implement Role Based Access Control. However, the audit log does not require that users are assigned RBAC roles nor does it require Active Directory integration.

XenServer logs actions on the pool level, and creates a log for each pool on the pool coordinator.

To display the audit log, you have two choices. You can:

- Generate the Pool Audit Trail report, provided you have Workload Balancing enabled.
- Display the audit log by opening it in any text editor. The log is stored on the pool coordinator.

Related documentation

XenServer Current Release

- Auditing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Workload Balancing Overview

Workload Balancing is an appliance that balances your pool by relocating virtual machines onto the best possible servers for their workload in a resource pool. For example, Workload Balancing can:

- Balance virtual-machine workloads across hosts in a resource pool
- Determine the best host on which to start a virtual machine
- Determine the best host on which to power on a virtual machine that you powered off
- Determine the best host for each of the host's virtual machines when you put that host into Maintenance mode

NOTE:

Workload Balancing is available for XenServer Premium Edition customers. For more information about licensing, see About XenServer Licensing.

Depending on your preference, Workload Balancing can accomplish these tasks automatically or prompt you to accept its optimization, consolidation, and placement recommendations. You can also configure Workload Balancing to power off hosts automatically during periods of low usage (for example, to save power at night).

Workload Balancing can send notifications in XenCenter regarding the actions it takes. For more information on how to configure the alert level for Workload Balancing alerts by using the XenAPI, see Configuring Workload Balancing alerts in XenCenter.

Workload Balancing evaluates the utilization of VM workloads across a pool. When a host reaches one of its thresholds, WLB relocates the VM to a different host in the pool.

To ensure the rebalancing and placement recommendations align with your environment's needs, you can configure WLB to optimize workloads for resource performance or to maximize the density. These optimization modes can be configured to change automatically at predefined times or stay the same always. For more granularity, you can fine-tune the weighting of individual resource metrics (CPU, network, memory, and disk).

To help you perform capacity planning, Workload Balancing provides historical reports about host and pool health, optimization and VM performance, and VM motion history.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about Workload Balancing, you can see the XenServer product documentation.

Related documentation

XenServer Current Release

- Workload Balancing

Getting Started with Workload Balancing

You can download the Workload Balancing virtual appliance and get it up and running using the following process:

1. Download the Workload Balancing virtual appliance package from the XenServer downloads page.
2. In XenCenter®, select **File** and then **Import** and follow the on-screen instructions to import the Workload Balancing virtual appliance.
3. Configure the Workload Balancing virtual appliance using the Workload Balancing Configuration wizard, which appears in the appliance's **Console** tab in XenCenter after you import the virtual appliance.
4. Connect your pool to the Workload Balancing virtual appliance as described in Connecting to Workload Balancing.

For more information, see the XenServer product documentation - Get started with Workload Balancing.

NOTE:

The **WLB** tab appears on the **Properties** pane after you license your hosts with XenServer Premium Edition. For more information about licensing, see About XenServer Licensing.

Related documentation

XenServer Current Release

- Workload Balancing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Workload Balancing Basic Concepts

Workload Balancing captures data for resource performance on virtual machines and physical hosts. It uses this data, combined with the preferences you set, to provide optimization and placement recommendations. Workload Balancing stores performance data in an internal database: the longer Workload Balancing runs, the better its recommendations become.

Workload Balancing recommends moving virtual-machine workloads across a pool to get the maximum efficiency, which means either performance or density depending on your goals. Within a Workload Balancing context:

- **Performance** refers to the usage of physical resources on a host (for example, the CPU, memory, network, and disk utilization on a host). When you set Workload Balancing to maximize performance, it recommends placing virtual machines to ensure the maximum amount of resources are available for each virtual machine.
- **Density** refers to the number of virtual machines on a host. When you set Workload Balancing to maximize density, it recommends placing VMs on as few hosts as possible, while ensuring they maintain adequate computing power. This behavior enables you to reduce the number of hosts powered on in a pool.

Workload Balancing lets you modify settings for placement (performance or density), power management, automation, metric weightings, and performance thresholds.

Workload Balancing do not conflict with High Availability settings. High Availability settings always take precedence.

Related documentation

XenServer Current Release

- Workload Balancing

Connecting to Workload Balancing

After importing the Workload Balancing virtual appliance and running the Workload Balancing Configuration wizard, you must connect the pool you want monitored to Workload Balancing. To do so, use either the **Connect to WLB Server** dialog box in XenCenter® or the xe CLI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The **WLB** tab appears on the **Properties** pane after you license your hosts with XenServer Premium Edition. For more information about licensing, see About XenServer Licensing.

Prerequisites

To complete the XenCenter procedure that follows, you need the:

- IP address, hostname, or Fully Qualified Domain Name (FQDN) and port of the Workload Balancing virtual appliance.
- Credentials for the resource pool (that is, the pool coordinator) you want Workload Balancing to monitor.
- Credentials for the account you created on the Workload Balancing appliance. This account is often known as the Workload Balancing user account. XenServer® uses this account to communicate with Workload Balancing. (You created this account on the Workload Balancing virtual appliance during Workload Balancing Configuration.)

If you want to specify the Workload Balancing virtual appliance's FQDN when connecting to the Workload Balancing server, first manually add its host name to your DNS. If you want to configure Trusted Authority certificates, Citrix® recommends specifying either an FQDN or an IP address that does not expire.

When you first connect to Workload Balancing, it uses the default thresholds and settings for balancing workloads. Automatic features, such as Automated Optimization Mode, Power Management, and Automation, are disabled by default.

IMPORTANT:

If you don't receive optimal placement recommendations after WLB runs for a time, Citrix recommends you evaluate your performance thresholds. For more information, see Evaluating the Effectiveness of Your Optimization Thresholds. It is critical to set the correct thresholds for your environment for Workload Balancing recommendations to be optimal.

To connect to the Workload Balancing virtual appliance

1. In the **Resources** pane of XenCenter, select **XenCenter** > **your-resource-pool**.
2. In the **Properties** pane, select the **WLB** tab. The WLB tab appears in the Properties pane after licensing your XenServer hosts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the **WLB** tab, select **Connect**. The **Connect to WLB Server** dialog box appears.
4. In the **Server Address** section, dialog box, enter the following:

   - In the **Address** box, type the IP address, hostname, or FQDN of the Workload Balancing server. An example of an FQDN is `WLB-appliance-computername.yourdomain.net`.
   - Enter the port number in the **Port** box. XenServer uses this port to communicate with Workload Balancing.

     By default, XenServer connects to Workload Balancing (specifically the Web Service Host service) on port 8012. If you changed the port number during Workload Balancing Configuration, you must enter that port number in the **Port** box.

     IMPORTANT:

     Change the default port number only if you changed the default port during Workload Balancing Configuration. The port number specified during Configuration, in any firewalls, and in the **Connect to WLB Server** dialog must match.

5. In the **WLB Server Credentials** section, enter the user name (for example, `wlbuser`) and password that XenServer uses to connect to the Workload Balancing virtual appliance. This account must be the account you created during Workload Balancing Configuration. By default, the user name for this account is `wlbuser`.
6. In the **XenServer Credentials** section, enter the user name and password for the pool you are configuring. Workload Balancing uses these credentials to connect to each of the hosts in that pool. To use the credentials with which you are currently logged into XenServer, select the **Use the current XenCenter credentials** check box. If you have assigned permissions to the account using the Role Based Access Control feature (RBAC), be sure they are sufficient to use Workload Balancing. See Definitions of RBAC roles and permissions.
7. Click **OK**. XenCenter starts the connection process.
8. Configure certificates:

   - (Workload Balancing 8.4.0 and later, XenCenter 2025.1.0 and later) If certificate verification is enabled for your pool, XenCenter now retrieves the Workload Balancing certificate from the virtual appliance.

     a. If XenCenter displays the new or modified certificate, click **View Certificate** to review the information. You can verify the certificate fingerprint against the information in the Workload Balancing console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Choose to **Accept** the certificate or **Cancel** the action.

- If you choose to **Accept** the certificate, XenCenter installs it in your XenServer pool.
- If you choose **Cancel**, XenCenter aborts the process. The certificate is not installed in the XenServer pool.

- (Earlier versions of Workload Balancing or XenCenter) Certificates are not automatically supported, you must configure XenServer to verify your Workload Balancing certificate. For more information, see Certificates.

After connecting to the Workload Balancing appliance, if you want to change the settings for thresholds or the priority given to specific resources, see Editing Workload Balancing Settings.

Related documentation

XenServer Current Release

- Workload Balancing

Introduction to basic tasks

Workload Balancing is a powerful XenServer® component that includes many features designed to optimize the workloads in your environment. These features include:

- Host power management
- The ability to schedule optimization-mode changes
- Running reports

In addition, you can fine-tune the criteria Workload Balancing uses to make optimization recommendations.

However, when you first begin using Workload Balancing, there are two main tasks you probably use Workload Balancing for on a daily (or regular) basis:

- Determining the best host on which to start a virtual machine
- Accepting Workload Balancing optimization recommendations

Determining the best host on which to start a VM

Workload Balancing can provide recommendations about the host. Determining the host to start a VM on is useful when you want to restart a powered off VM and when you want to migrate a VM to another host. It might also be useful in Citrix Virtual Desktops™ environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Choosing an Optimal Server for VM Initial Placement, Migrate, and Resume.

Accepting Workload Balancing recommendations

After Workload Balancing is running for a while, it begins to make recommendations about ways in which you can improve your environment. For example, if your goal is to improve VM density on hosts, with the appropriate settings, Workload Balancing issues a recommendation to consolidate VMs on a host. Assuming you are not running in automated mode, you can choose to either apply this recommendation or simply ignore it.

For more information, see Accepting Optimization Recommendations.

Both of these tasks, and how you perform them in XenCenter, are explained in more depth in the sections that follow. Another frequently used task is running reports about the workloads in your environment, which is described in Generating and Managing Workload Balancing Reports.

IMPORTANT:

After Workload Balancing is running for some time, if you don't receive optimal placement recommendations, evaluate your performance thresholds as described in the Workload Balancing documentation. It is critical to set Workload Balancing to the correct thresholds for your environment or its recommendations might not be appropriate or occur at the correct times.

Related documentation

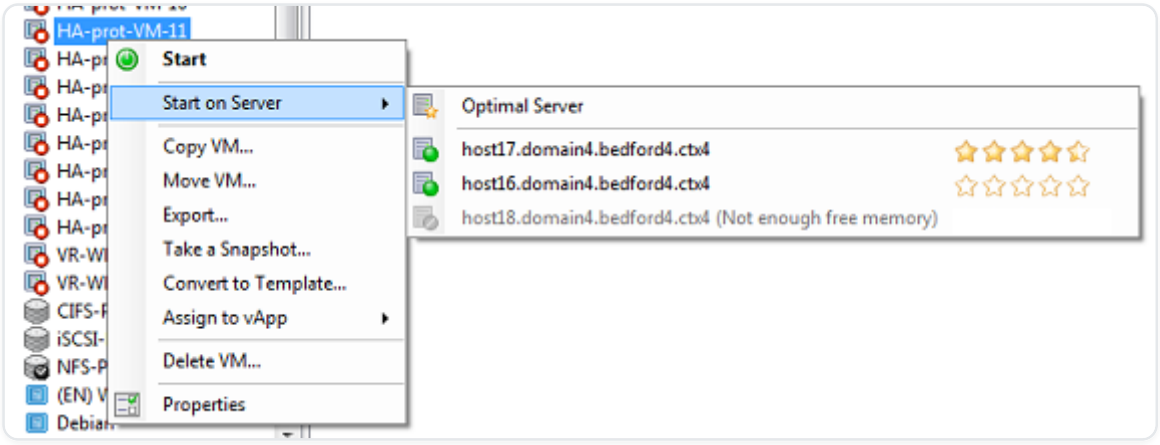
XenServer Current Release

- Workload Balancing

Choosing an optimal server for VM initial placement, migrate, and resume

When Workload Balancing is enabled and you start a VM, XenCenter® provides recommendations to help you determine the optimal host in the pool to start a VM on. The recommendations are also known as star ratings since stars are used to indicate the best host.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



More stars appear beside host17 since this server is the optimal host on which to start the VM. host16 does not have any stars beside it, which indicates that the host is not recommended. However, since this host is enabled the user can select that host. host18 is grayed out due to insufficient memory, so the user cannot select it.

How do placements work?

When Workload Balancing is enabled, XenCenter provides star ratings to indicate the optimal hosts for starting a VM. These ratings also apply when you want to start a VM that is powered off or suspended and when you want to migrate the VM to another server.

When you use these features with Workload Balancing enabled, host recommendations appear as star ratings beside the name of the physical host. Five empty stars indicate the lowest-rated (least optimal) server.

In general, Workload Balancing functions more effectively and makes better, less frequent optimization recommendations if you start VMs on the hosts it recommends. That is, by using one of the placement features to select the host with the most stars beside it.

What does optimal mean?

The term *optimal* refers to the physical server best suited to hosting your workload. There are several factors Workload Balancing uses when determining which host is optimal for a workload:

- The amount of resources available on each host in the pool. When a pool runs in Maximum Performance mode, Workload Balancing tries to balance the VMs across the hosts in the pool so that all VMs have good performance. When a pool is running in Maximum Density mode, Workload Balancing tries to place VMs onto hosts as densely as possible while ensuring the VMs have sufficient resources.
- The optimization mode in which the pool is running (Maximum Performance or Maximum Density). When a pool is running in Maximum Performance mode, Workload Balancing tries to place VMs on hosts with the most resources available of the type the VM requires. In Maximum

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Density mode, Workload Balancing tries to place VMs on hosts that already have VMs running so that VMs are running on as few hosts as possible.

- The amount and type of resources the VM requires. After WLB monitors a VM for a while, it uses the VM metrics it gathered to make placement recommendations according to the type of resources the VM requires. For example, WLB might select a host with less available CPU but more available memory if it is what the VM requires (based on its past performance history). However, Workload Balancing only makes a recommendation if it determines the current host is under resource pressure.

To start a virtual machine on the optimal server

1. In the **Resources** pane of XenCenter, select the virtual machine you want to start.
2. From the **VM** menu, select **Start on Server** and then select one of the following:

    - **Optimal Server**. The optimal server is the physical host that is best suited to the resource demands of the virtual machine you are starting. Workload Balancing determines the optimal server based on its historical records of performance metrics and your placement strategy. The optimal server is the server with the most stars.
    - One of the servers with star ratings listed under the **Optimal Server** command. Five stars indicate the most-recommended (optimal) server and five empty stars indicates the least-recommended server.

To resume a virtual machine on the optimal server

1. In the **Resources** pane of XenCenter, select the suspended virtual machine you want to resume.
2. From the **VM** menu, select **Resume on Server** and then select one of the following:

    - **Optimal Server**. The optimal server is the physical host that is best suited to the resource demands of the virtual machine you are starting. Workload Balancing determines the optimal server based on its historical records of performance metrics and your placement strategy. The optimal server is the server with the most stars.
    - One of the servers with star ratings listed under the **Optimal Server** command. Five stars indicate the most-recommended (optimal) server and five empty stars indicates the least-recommended server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

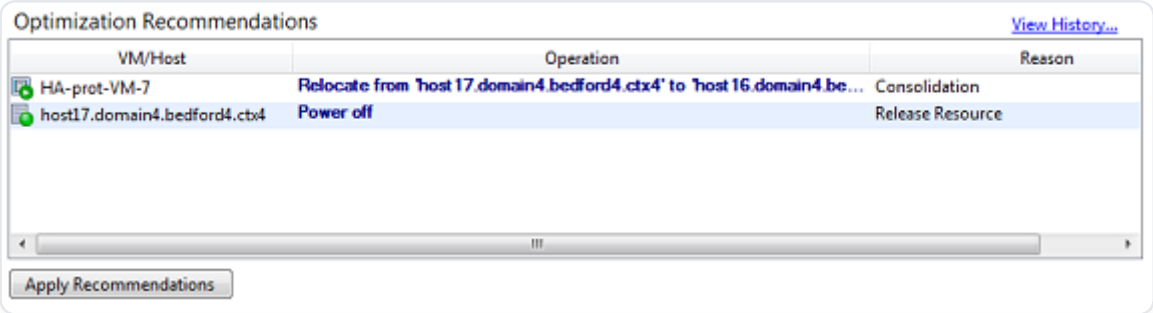
Related documentation

XenServer Current Release

- Workload Balancing

Accepting Optimization Recommendations

Workload Balancing provides recommendations about ways you can migrate virtual machines to optimize your environment. Optimization recommendations appear in the **WLB** tab in XenCenter.



This illustration shows a screen capture of the Optimization Recommendations list, which appears on the **WLB** tab. The **Reason** column displays the purpose of the recommendation. The **Operation** column displays the behavior change suggested for that optimization recommendation. This screen capture shows an optimization recommendation for a virtual machine, `HA-prot-VM-7`, and a host, `host17.domain4.bedford4.ctx4`.

Basis for optimization recommendations

Optimization recommendations are based on the following factors:

- Placement strategy you select (that is, the placement optimization mode), as described in Adjusting the Optimization Mode
- Performance metrics for resources such as a physical host's CPU, memory, network, and disk utilization
- The role of the host in the resource pool. When making placement recommendations, Workload Balancing considers only the pool coordinator if no other host can accept the workload. (Likewise, when a pool is operating in Maximum Density mode, Workload Balancing considers the pool coordinator last when determining the order in which to fill hosts with VMs.)

The optimization recommendations display the following information:

- The name of the VM that Workload Balancing recommends relocating
- The host it currently resides on
- The host Workload Balancing recommends as the machine's new location

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The reason Workload Balancing recommends moving the VM

  For example, "CPU" to improve the CPU utilization.

After you accept an optimization recommendation, XenServer® relocates all virtual machines listed as recommended for optimization.

TIP:

You can find out the optimization mode for a resource pool by selecting the pool in XenCenter and checking the **Configuration** section of the **WLB** tab.

To accept an optimization recommendation

1. Select the pool for which you want to display recommendations in the **Resources** pane and then select the **WLB** tab. If there are any recommended optimizations for any virtual machines on the selected resource pool, they display on the **WLB** tab.
2. To accept the recommendations, select **Apply Recommendations**. XenServer begins moving all virtual machines listed in the **Optimization Recommendations** section to their recommended servers.

   After you select **Apply Recommendations**, you can select **Notifications** and then **Events** tab to display the progress of the virtual machine migration.

Understanding WLB recommendations under High Availability

If you have Workload Balancing and the XenServer High Availability feature enabled in the same pool, it is helpful to understand how the two features interact. Workload Balancing is designed not to interfere with High Availability. If there is a conflict between a Workload Balancing recommendation and a High Availability setting, the **High Availability** setting always takes precedence. In practice, this means:

- Workload Balancing will not automatically power off any hosts beyond the number specified in the **Failures allowed** box in the **Configure HA** dialog.
  - However, Workload Balancing might still make recommendations to power off more hosts than the number of host failures to tolerate. (For example, Workload Balancing still makes a recommendation to power off two hosts when High Availability is only configured to tolerate one host failure.) However, when you attempt to apply the recommendation, XenCenter might display an error message stating that High Availability is no longer guaranteed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When Workload Balancing is running in automated mode and has power management enabled, any recommendations that exceed the number of host failures to tolerate are ignored. In this situation, if you look in the Workload Balancing log, you see a message that says a power-management recommendation was not applied because High Availability is enabled.

Related documentation

XenServer Current Release

- Workload Balancing

Working with Workload Balancing Reports

Workload Balancing provides reporting on three types of objects: physical hosts, resource pools, and virtual machines. At a high level, Workload Balancing provides two types of reports:

- Historical reports that display information by date
- "Roll up" style reports

Workload Balancing provides some reports for auditing purposes, so you can determine, for example, the number of times a virtual machine moved.

Types of reports

Workload Balancing offers several different reports about the pool, hosts, and VMs. For more information, see Workload Balancing Report Glossary.

Generating reports

Workload Balancing lets you generate reports, export them as PDFs or spreadsheets, and print them out. For more information, see Generating and Managing Workload Balancing reports.

Related documentation

XenServer Current Release

- Workload Balancing

Using Workload Balancing Reports for Tasks

The Workload Balancing reports can help you perform capacity planning, determine virtual-machine health, and evaluate the effectiveness of your configured threshold levels.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Evaluating the effectiveness of your performance thresholds

You can use the Pool Health report to evaluate the effectiveness of your optimization thresholds. Workload Balancing provides default threshold settings. However, you might need to adjust these defaults for them to provide value in your environment. If you do not have the thresholds adjusted to the correct level for your environment, the Workload Balancing recommendations might not be appropriate for your environment.

Troubleshooting administrative changes

You can use the Pool Audit Trail report to determine the source (that is, user account) of problematic changes and the event or task that user performed.

Related documentation

XenServer Current Release

- Workload Balancing

Generating and Managing Workload Balancing Reports

This topic provides basic instructions for using Workload reports, including how to generate, navigate in, print, and export reports.

To generate a Workload Balancing report

1. In the **Resources** pane of XenCenter®, select **your-resource-pool**.
2. From the **Pool** menu, select **View Workload Reports**.

   TIP:

   You can also display the Workload Reports screen from the **WLB** tab by clicking the **Reports** button.

3. From the Workload Reports screen, select a report from the left pane.
4. Select the **Start Date** and the **End Date** for the reporting period. Depending on the report you select, you might have to specify other parameters such as **Host**, **User**, and **Object**.
5. Click **Run Report**. The report displays in the report window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To navigate in a Workload Balancing report

After generating a report, you can use the toolbar buttons in the report to navigate and perform certain tasks. To display the name of a toolbar button, pause your mouse over the toolbar icon.

Report Toolbar Buttons:

	**Document Map**. Displays a document map that helps you navigate through long reports.
	**Page Forward/Back**. Moves one page ahead or back in the report.
	**Back to Parent Report**. Returns to the parent report when working with drill-through reports. **Note:** This button is only available in drill-through reports, such as the Pool Health report.
	**Stop Rendering**. Stops the report generation.
	**Print**. Prints a report and specify general printing options, such as the printer, the number of pages, and the number of copies.
	**Print Layout**. Displays a preview of the report before you print it. To exit Print Layout, select the **Print Layout** button again.
	**Page Setup**. Specifies printing options such as the paper size, page orientation, and margins.
	**Export**. Exports the report as an Acrobat (`.pdf`) file or as an Excel file with an `.xls` extension.
	**Find**. Searches for a word in a report, such as the name of a virtual machine.

To print a Workload Balancing report

Before you can print a report, you must first generate it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. (Optional) To preview the printed document, select **Print Layout**.



2. (Optional) To change the paper size/source, page orientation, or margins, select **Page Setup**.



3. Click **Print**.



To export a Workload Balancing report

You can export a report in Microsoft Excel and Adobe Acrobat (`.pdf`) formats.



After generating the report, select **Export** and select one of the following:

- Excel
- Acrobat (`.pdf`) file

NOTE:

The amount of data included when you export a report might differ depending on the export format. Reports exported to Excel include all the data available for the report, including "drilldown" data. Whereas reports displayed in XenCenter or exported as `.pdf` only contain the data that you selected when you generated the report.

Related documentation

XenServer Current Release

- Workload Balancing

Workload Balancing Report Glossary

Workload Balancing provides the following reports.

Chargeback utilization analysis

You can use the Chargeback Utilization Analysis report ("chargeback report") to determine how much of a resource (such as a physical server) a department within your organization used. Specifically, the report shows information about all the virtual machines in your pool, including their

© 1997–2026 Citrix Systems, Inc. All rights reserved.

availability and resource utilization. Since this report shows virtual machine availability ("up time"), it can help you demonstrate Service Level Agreements compliance and availability.

The chargeback report can help you implement a simple chargeback solution and facilitate billing. To bill customers for usage of a specific resource, generate the report, save it as Excel. You can then customize the spreadsheet data to include your price per unit or import the Excel data into your billing system.

If you know that you want to bill internal or external customers for virtual machine usage, consider incorporating department or customer names in your VM naming conventions. This convention makes reading chargeback reports easier.

The resource reporting in the chargeback report is, sometimes, based on the allocation of physical resources to individual VMs.

Likewise, because XenServer® lets you allocate fixed or automatic allocations of memory, the average memory data in this report is based on the amount of memory currently allocated to the VM, whether it is through a fixed memory allocation or an automatically adjusting memory allocation (Dynamic Memory Control).

The chargeback report contains the following columns of data:

- **VM Name**. The name of the virtual machine to which the data in the columns in that row applies.
- **VM Uptime**. The number of minutes the virtual machine was powered on (or, more specifically, appears with a green icon beside it in XenCenter®).
- **vCPU Allocation**. The number of virtual CPUs configured on the virtual machine. Each virtual CPU receives an equal share of the physical CPUs on the host. For example, if you configured eight virtual CPUs on a host that contains two physical CPUs and this column had "1" in it, then this value is equal to 2/16 of the total processing power on the host.
- **Minimum CPU Usage (%)**. The lowest recorded value for the virtual CPU utilization in the reporting period. This value is expressed as a percentage of the VM's virtual CPU capacity. The capacity is based on the number of virtual CPUs allocated to the VM. For example, if you allocated one virtual CPU to the VM, Minimum CPU Usage represents the lowest percentage of virtual CPU usage XenServer recorded. If you allocated two virtual CPUs to the VM, the value in this column represents the lowest usage of the combined capacity of both virtual CPUs. The value is expressed as a percentage.

  Ultimately, the percentage of CPU usage represents the lowest recorded workload that the virtual CPU handled. For example, if you allocate one virtual CPU to a VM and the physical

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CPU on the host is 2.4 GHz, you are allocating one-eighth of 2.4 GHz to the VM. This behavior means that if the VM's allocated capacity is 0.3 GHz, or 300 MHz, and the Minimum CPU Usage for the virtual machine was 20%, the VM's lowest usage of the physical host's CPU during the reporting period was 60 MHz.

- **Maximum CPU Usage (%)**. The highest percentage of the virtual machine's virtual CPU capacity that the virtual machine consumed during the reporting period. The CPU capacity consumed is a percentage of the virtual CPU capacity you allocated to the virtual machine. For example, if you allocated one virtual CPU to the VM, the Maximum CPU Usage represents the highest recorded percentage of virtual CPU usage during the time reported. If you allocated two virtual CPUs to the virtual machine, the value in this column represents the highest utilization from the combined capacity of both virtual CPUs.
- **Average CPU Usage (%)**. The average amount, expressed as a percentage, of the virtual machine's virtual CPU capacity that was in use during the reporting period. The CPU capacity is the virtual CPU capacity you allocated to the virtual machine. If you allocated two virtual CPUs to the virtual machine, the value in this column represents the average utilization from the combined capacity of both virtual CPUs.
- **Total Storage Allocation (GB)**. The amount of disk space that is currently allocated to the virtual machine at the time the report was run. Frequently, unless you modified it, this disk space is the amount of disk space you allocated to the virtual machine when you created it.
- **Virtual NIC Allocation**. The number of virtual interfaces (VIFs) allocated to the virtual machine.
- **Current Minimum Dynamic Memory (MB)**.
    - **Fixed memory allocation**. If you assigned a virtual machine a fixed amount of memory (for example, 1,024 MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).
    - **Dynamic memory allocation**. If you configured XenServer to adjust a VM's memory automatically based on a range, this column shows the minimum amount of memory specified in the range. For example, if in the **Memory Settings** dialog box in XenCenter, you selected the **Automatically allocate memory within this range** option for this virtual machine and then specified the range values as 1,024 MB as the minimum memory and 2,048 MB as the maximum memory, then 1,024 MB appears in the **Current Minimum Dynamic Memory (MB)** column.
- **Current Maximum Dynamic Memory (MB)**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **Dynamic memory allocation**. If XenServer is set to adjust a VM's memory automatically based on a range, this column shows the maximum amount of memory specified in the range. For example, if the memory range you provided was 1,024 MB minimum and 2,048 MB maximum, then 2,048 MB appears in the Current Maximum Dynamic Memory (MB) column.
  - **Fixed memory allocation**. If you assign a VM a fixed amount of memory (for example, 1,024 MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).

- **Current Assigned Memory (MB)**.

  - **Dynamic memory allocation**. When Dynamic Memory Control is configured, this value indicates the amount of memory XenServer is allocating to the virtual machine when the report is run.
  - **Fixed memory allocation**. If you assign a virtual machine a fixed amount of memory (for example, 1,024 MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).

> **NOTE:**
>
> If you change the virtual machine's memory allocation immediately before running this report, the value reflected in this column reflects the new memory allocation you configured.

- **Average Assigned Memory (MB)**.

  - **Dynamic memory allocation**. When Dynamic Memory Control is configured, this value indicates the average amount of memory XenServer allocated to the virtual machine over the reporting period.
  - **Fixed memory allocation**. If you assign a virtual machine a fixed amount of memory (for example, 1,024 MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> If you change the virtual machine's memory allocation immediately before running this report, the value displayed in this column might not change from what it would have previously displayed. The value in this column reflects the average over the time period.

- **Average Network Reads (BPS)**. The average amount of data (in bits per second) the virtual machine received during the reporting period.
- **Average Network Writes (BPS)**. The average amount of data (in bits per second) the virtual machine sent during the reporting period.
- **Average Network Usage (BPS)**. The combined total (in bits per second) of the Average Network Reads and Average Network Writes. For example, if a virtual machine sent, on average, 1,027 bits per second and received, on average, 23,831 bits per second over the reporting period, then the Average Network Usage would be the combined total of these two values: 24,858 bits per second.
- **Total Network Usage (BPS)**. The total of all network read and write transactions in bits per second over the reporting period.

Host health history

This report displays the performance of resources (CPU, memory, network reads, and network writes) on a specific host in relation to threshold values.

The colored lines (red, green, yellow) represent your threshold values. You can use this report with the Pool Health report for a host to determine how a particular host's performance might be affecting overall pool health. When you are editing the performance thresholds, you can use this report for insight into the host performance.

You can display resource utilization as a daily or hourly average. The hourly average lets you see the busiest hours of the day, averaged, for the time period.

To view report data grouped by hour, expand **+ Click to view report data grouped by house for the time period** under the **Host Health History** title bar.

Workload Balancing displays the average for each hour for the time period you set. The data point is based on a utilization average for that hour for all days in the time period. For example, in a report for May 1, 2009, to May 15, 2009, the Average CPU Usage data point represents the resource utilization of all 15 days at 12:00 hours combined as an average. That is, if CPU utilization

© 1997–2026 Citrix Systems, Inc. All rights reserved.

was 82% at 12 PM on May 1, 88% at 12 PM on May 2, and 75% on all other days, the average displayed for 12 PM is 76.3%.

Pool optimization performance history

The optimization performance report displays optimization events (that is, when you optimized a resource pool) against that pool's average resource usage. Specifically, it displays resource usage for CPU, memory, network reads, and network writes.

The dotted line represents the average usage across the pool over the period of days you select. A blue bar indicates the day on which you optimized the pool.

This report can help you determine if Workload Balancing is working successfully in your environment. You can use this report to see what led up to optimization events (that is, the resource usage before Workload Balancing recommended optimizing).

This report displays average resource usage for the day. It does not display the peak utilization, such as when the system is stressed. You can also use this report to see how a resource pool is performing if Workload Balancing is not making optimization recommendations.

In general, resource usage declines or remains steady after an optimization event. If you do not see improved resource usage after optimization, consider readjusting threshold values. Also, consider whether the resource pool has too many virtual machines and whether new virtual machines were added or removed during the time frame you specified.

Pool audit trail

This report displays the contents of Audit Log, a feature designed to log attempts to perform unauthorized actions and select authorized actions. These actions include import/export, host and pool backups, and guest and host console access. The report gives more meaningful information when XenServer administrators are given their own user accounts with distinct roles assigned to them using the Role-Based Access Control feature. For information about the Audit Log feature, see the audit log documentation in the Workload Balancing documentation.

IMPORTANT:

To run the audit log report, the Audit Logging feature must be enabled. By default, Audit Log is always enabled in the Workload Balancing virtual appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The enhanced Pool Audit Trail feature allows you to specify the granularity of the audit log report. You can also search and filter the audit trail logs by specific users, objects, and by time. The Pool Audit Trail Granularity is set to **Minimum** by default. This option captures limited amount of data for specific users and object types. You can modify the setting at any time based on the level of detail you would require in your report. For example, set the granularity to **Medium** for a user-friendly report of the audit log. If you require a detailed report, set the option to **Maximum**.

To modify the **Pool Audit Trail Granularity** setting:

1. Select the pool in the **Infrastructure** view, select the **WLB** tab, and then select **Settings**.
2. In the left pane, select **Advanced**.
3. On the Advanced page, select the **Pool Audit Trail Report Granularity** list and select an option from the list.

   IMPORTANT:

   Select the granularity based on your audit log requirements. For example, if you set your audit log report granularity to **Minimum**, the audit report only captures limited amount of data for specific users and object types. If you set the granularity to **Medium**, the report provides a user-friendly report of the audit log. If you choose to set the granularity to **Maximum**, the report contains detailed information about the audit log report. Setting the audit log report to Maximum can cause the Workload Balancing server to use more disk space and memory.

4. Click **OK** to confirm your changes.

This report displays the following:

- **Time**. The time XenServer recorded the user's action.
- **User Name**. The name of the person who created the session in which the action was performed. Sometimes, this value might be the User ID.
- **Event Object**. The object that was the subject of the action (for example, a virtual machine).
- **Event Action**. The action that occurred. For definitions of these actions, see Audit Log Event Names.
- **Access**. Whether the user had permission to perform the action.
- **Object Name**. The name of the object (for example, the name of the virtual machine).
- **Object UUID**. The UUID of the object (for example, the UUID of the virtual machine).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Succeeded**. This value provides the status of the action (that is, whether it was successful).

Pool Health

The pool health report displays the percentage of time a resource pool and its hosts spent in four different threshold ranges: Critical, High, Medium, and Low. You can use the Pool Health report to evaluate the effectiveness of your performance thresholds.

A few points about interpreting this report:

- Resource utilization in the Average Medium Threshold (blue) is the optimum resource utilization regardless of the placement strategy you selected. Likewise, the blue section on the pie chart indicates the amount of time that the host used resources optimally.
- Resource utilization in the Average Low Threshold Percent (green) is not necessarily positive. Whether Low resource utilization is positive depends on your placement strategy. For example, if your placement strategy is Maximum Density and most of the time your resource usage was green, Workload Balancing might not be fitting the maximum number of virtual machines possible on that host or pool. If so, adjust your performance threshold values until most of your resource utilization falls into the Average Medium (blue) threshold range.
- Resource utilization in the Average Critical Threshold Percent (red) indicates the amount of time average resource utilization met or exceeded the Critical threshold value.

If you double-click on a pie chart for a host's resource usage, XenCenter displays the Host Health History report for that resource on that host. Clicking the **Back to Parent Report** toolbar button returns you to the Pool Health history report. Note: This button is only available in drill-through reports, such as the Pool Health report.

If you find most of your report results are not in the Average Medium Threshold range, you probably need to adjust the Critical threshold for this pool. While Workload Balancing provides default threshold settings, these defaults are not effective in all environments. If you do not have the thresholds adjusted to the correct level for your environment, Workload Balancing's optimization and placement recommendations might not be appropriate. For more information, see Changing the Critical Thresholds.

NOTE:

The High, Medium, and Low threshold ranges are based on the Critical threshold value.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pool health history

This report provides a line graph of resource utilization on all physical hosts in a pool over time. It lets you see the trend of resource utilization - if it tends to be increasing in relation to your thresholds (Critical, High, Medium, and Low). You can evaluate the effectiveness of your performance thresholds by monitoring the trends of the data points in this report.

Workload Balancing extrapolates the threshold ranges from the values you set for the Critical thresholds. Although similar to the Pool Health report, the Pool Health History report displays the average utilization for a resource on a specific date rather than the amount of time overall the resource spent in a threshold.

Except for the Average Free Memory graph, the data points never average above the Critical threshold line (red). For the Average Free Memory graph, the data points never average below the Critical threshold line (which is at the bottom of the graph). Because this graph displays free memory, the Critical threshold is a low value, unlike the other resources.

A few points about interpreting this report:

- When the Average Usage line in the chart approaches the Average Medium Threshold (blue) line, it indicates the pool's resource utilization is optimum regardless of the placement strategy configured.
- Resource utilization approaching the Average Low Threshold (green) is not necessarily positive. Whether Low resource utilization is positive depends on your placement strategy. For example, if your placement strategy is Maximum Density and most days the Average Usage line is at or below the green line, Workload Balancing might not be placing virtual machines as densely as possible on that pool. If so, adjust the pool's Critical threshold values until most of its resource utilization falls into the Average Medium (blue) threshold range.
- When the Average Usage line intersects with the Average Critical Threshold Percent (red), this intersection indicates the days when the average resource utilization met or exceeded the Critical threshold value for that resource.

If you find the data points in most of your graphs are not in the Average Medium Threshold range, but you are satisfied with the performance of this pool, you might need to adjust the Critical threshold for this pool. For more information, see Changing the Critical Thresholds.

Pool optimization history

The Pool Optimization History report provides chronological visibility into the Workload Balancing optimization activity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Optimization activity is summarized graphically and in a table. Drilling into a date field within the table displays detailed information for each pool optimization performed for that day.

This report lets you see the following information:

- **VM Name**: The name of the virtual machine that Workload Balancing optimized.
- **Reason**: The reason for the optimization.
- **Status**: Whether the optimization was successful.
- **From Host**: The physical server where the virtual machine was originally hosted.
- **To Host**: The physical server where the virtual machine was moved.
- **Time**: The time when the optimization occurred.

TIP:

You can also generate a Pool Optimization History report from the **WLB** tab, by clicking the **View History** link.

Virtual machine motion history

This line graph displays the number of times virtual machines moved on a resource pool over a period. It indicates if a move resulted from an optimization recommendation and to which host the virtual machine moved. This report also indicates the reason for the optimization. You can use this report to audit the number of moves on a pool.

Some points about interpreting this report:

- The numbers on the left side of the chart correspond with the number of moves possible, which is based on how many VMs are in a resource pool.
- You can look at details of the moves on a specific date by expanding the + sign in the **Date** section of the report.

Virtual Machine Performance history

This report displays performance data for each virtual machine on a specific host for a time period you specify. Workload Balancing bases the performance data on the amount of virtual resources allocated for the virtual machine. For example, if the Average CPU Usage for your VM is 67%, your VM was using, on average, 67% of its vCPU for the specified period.

The initial view of the report displays an average value for the resource utilization over the period you specified.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Expanding the + sign displays line graphs for individual resources. You can use these graphs to see trends in resource utilization over time.

This report displays data for CPU Usage, Free Memory, and Network Reads/Writes.

Related documentation

XenServer Current Release

- Workload Balancing

Audit Log Events

The Audit Log report logs XenServer events, event objects, and actions. These actions include import/export, host and pool backups, and guest and host console access. The following table defines some of the typical events that appear frequently in the XenServer Audit Log and Pool Audit Trail report. The table also specifies the granularity of these events.

In the Pool Audit Trail report, the events listed in the **Event Action** column apply to a pool, VM, or host. To determine what the events apply to, see the **Event Object** and **Object Name** columns in the report. For extra event definitions, see the Management API. To know more about the **Pool Audit Trail granularity** settings, see Advanced Settings.

POOL AUDIT TRAIL GRANULARITY	EVENT ACTION	USER ACTION
Minimum	VM.start	Started a virtual machine.
Minimum	VM.copy	Copied the specified VM, making a new VM.
Minimum	host.reboot	Restarted XenServer host.
Minimum	host.disable	Put the host into a state in which no new VMs can be started.
Minimum	pool.join	Instructed host to join a new pool.
Minimum	pool.join_force	Instructed (forced) host to join a new pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POOL AUDIT TRAIL GRANULARITY	EVENT ACTION	USER ACTION
Medium	SR.destroy	Destroyed the storage repository.
Medium	SR.create	Created a storage repository.
Medium	VDI.snapshot	Took a read-only snapshot of the VDI, returning a reference to the snapshot.
Medium	VDI.clone	Took an exact copy of the VDI and returned a reference to the new disk.
Medium	VIF.plug	Hot plugged the specified VIF, dynamically attaching it to the running VM.
Medium	VIF.unplug	Hot-unplugged the specified VIF, dynamically detaching it from the running VM.
Maximum	auth.get_subject_identifier	Queried the external directory service to obtain the subject identifier as a string from the human-readable subject name.
Maximum	task.cancel	Requested that a task is canceled.
Maximum	VBD.insert	Inserted new media into the device.
Maximum	VIF.get_by_uuid	Got a reference to the VIF instance with the specified UUID.
Maximum	VDI.get_sharable	Got the sharable field of the given VDI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POOL AUDIT TRAIL GRANULARITY	EVENT ACTION	USER ACTION
Maximum	SR.get_all	Returned a list of all the SRs known to the system.
Maximum	pool.create_new_blob	Created a placeholder for a named binary blob of data that is associated with this pool.
Maximum	host.send_debug_keys	Injected the given string as debugging keys into Xen.
Maximum	VM.get_boot_record	Returned a record describing the VM's dynamic state. This record is initialized when the VM boots and updated to reflect runtime configuration changes, for example, CPU hotplug.

Related documentation

XenServer Current Release

- Workload Balancing

Editing Workload Balancing Settings

After connecting to the Workload Balancing virtual appliance, you can edit the settings Workload Balancing uses to calculate placement and optimization recommendations. You can perform tasks such as the following:

- Adjusting the Optimization Mode
- Setting Automation and Power Management
- Changing the Critical Thresholds
- Tuning Metric Weightings
- Excluding Hosts from Recommendations
- Advanced Settings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configuring Workload Balancing alerts in XenCenter

NOTE:

After connecting or reconnecting to Workload Balancing, wait at least 60 seconds (until the Workload Balancing (/var/log/wlb/LogFile.log) shows discovery is finished) before changing settings.

How Workload Balancing settings apply

Workload Balancing settings apply collectively to all virtual machines and hosts in the pool.

Provided the network and disk thresholds align with the hardware in your environment, consider using most of the defaults in Workload Balancing initially.

After Workload Balancing is enabled for a while, Citrix® recommends evaluating your performance thresholds and determining if you need to edit them. For example, consider if you are:

- Getting optimization recommendation when they are not yet required. If so, try adjusting the thresholds until Workload Balancing begins providing suitable optimization recommendations.
- Not getting recommendations when you think your network has insufficient bandwidth. If so, try lowering the network critical thresholds until Workload Balancing begins providing optimization recommendations.

Before you edit your thresholds, you might find it handy to generate a Host Health History report for each physical host in the pool.

You can use either the **Workload Balancing Configuration** properties in XenCenter® or the xe CLI to modify the configuration settings.

To update the credentials that XenServer and the Workload Balancing server use to communicate, see Updating Workload Balancing Credentials.

For more detailed guidance about tuning Workload Balancing settings, see the Workload Balancing documentation.

To display the Workload Balancing settings dialog box

1. In the **Resources** pane of XenCenter, select **your-resource-pool**.
2. In the **Properties** pane, click the **WLB** tab.
3. In the **WLB** tab, click **Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- Workload Balancing

Adjusting the Optimization Mode

Workload Balancing makes recommendations to rebalance, or optimize, the virtual machine workload in your environment based on a strategy for placement you select known as the optimization mode.

You can select one of two optimization modes:

- **Maximize Performance**. (Default.) Workload Balancing attempts to spread the workload evenly across all physical hosts in a resource pool. The goal is to minimize CPU, memory, network, and disk pressure for all hosts. When Maximize Performance is your placement strategy, Workload Balancing recommends an optimization when a virtual machine reaches the High threshold.
- **Maximize Density**. Workload Balancing attempts to fit as many virtual machines as possible onto a physical host. The goal is to minimize the number of physical hosts that must be online.

  When you select Maximize Density as your placement strategy, you can specify rules similar to the ones in Maximize Performance. However, Workload Balancing uses these rules to determine how it can pack virtual machines onto a host. When Maximize Density is your placement strategy, Workload Balancing recommends an optimization when a virtual machine reaches the Critical threshold.

Workload Balancing also lets you apply these optimization modes always, *Fixed*, or switch between modes for specified time periods, *Scheduled*.

- **Fixed**. Fixed optimization modes always set Workload Balancing to a specific optimization behavior - either to try to create the best performance or the highest density.
- **Scheduled**. Scheduled optimization modes let you schedule for Workload Balancing to apply different optimization modes depending on the time of day. For example, you can configure Workload Balancing to optimize for performance during the day when you have users connected. Then you can save energy by specifying for Workload Balancing to optimize for Maximum Density at night.

  When you configure Scheduled optimization modes, Workload Balancing automatically changes to the optimization mode at the beginning of the time period that you specified.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To set an optimization mode for all time periods

1. Select the pool in the **Resources** pane, select the **WLB** tab, and then select **Settings**.
2. In the left pane, select **Optimization Mode**.
3. Select **Fixed**, and select one of these optimization modes:

   - **Maximize Performance**. (Default.) Attempts to spread the workload evenly across all physical hosts in a resource pool. The goal is to minimize CPU, memory, network, and disk pressure for all hosts.
   - **Maximize Density**. Attempts to fit as many virtual machines as possible onto a physical host. The goal is to minimize the number of physical hosts that must be online. (Workload Balancing considers the performance of consolidated VMs and issues a recommendation to improve performance if a resource on a host reaches a Critical threshold.)

To specify times when the optimization mode changes automatically

1. Select the pool in the **Resources** pane, select the **WLB** tab, and then select **Settings**.
2. In the left pane, select **Optimization Mode**.
3. Select **Scheduled**.
4. Select **Add New** to open the **Optimization Mode Scheduler** dialog box.
5. Select an optimization mode in the **Change to** list box:

   - **Maximize Performance**. Attempts to spread the workload evenly across all physical hosts in a resource pool. The goal is to minimize CPU, memory, network, and disk pressure for all hosts.
   - **Maximize Density**. Attempts to fit as many virtual machines as possible onto a physical host. The goal is to minimize the number of physical hosts that must be online.

6. Select the day of the week and the time when you want Workload Balancing to begin operating in this mode.
7. Create more scheduled mode changes (that is, "tasks") until you have the number you need. If you only schedule one task, Workload Balancing switches to that mode and never switch back.
8. Select **OK**.

To delete or pause a scheduled optimization mode task

1. Select the pool in the **Resources** pane, select the **WLB** tab, and then select **Settings**.
2. Select **Optimization Mode**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select a scheduled task and select one of the following:

   - **Delete the task permanently**. Select the **Delete** button.
   - **Stop the task from running temporarily**. Right-click the task and select **Disable**.

   To re-enable a task, right-click the task in the **Scheduled Mode Changes** list.

To edit a scheduled optimization mode task

1. Select the pool in the **Resources** pane, select the **WLB** tab, and then select **Settings**.
2. Select a scheduled task.
3. Select **Edit**.
4. In the **Change to** box, select a different mode or make other changes as desired.

Related documentation

XenServer Current Release

- Workload Balancing

Optimizing and Managing Power Automatically

You can configure Workload Balancing to accept optimization recommendations automatically (Automation) and turn servers on or off automatically (Power Management).

Accepting optimization recommendations automatically

Workload Balancing lets you configure for it to accept optimization recommendations on your behalf and perform the optimization actions it recommends automatically. You can use this feature, which is known as Automation, to apply any recommendations automatically, including ones to improve performance or power down hosts. However, to power down hosts as virtual-machines usage drops, you must configure automation, power management, and Maximum Density mode.

By default, Workload Balancing does not accept optimizations automatically. Enable Automation if you want Workload Balancing to accept recommendations automatically. If you do not, Workload Balancing still prompts you to accept recommendations manually.

Workload Balancing does not automatically apply recommendations to hosts or virtual machines when the recommendations conflict with High Availability settings. If a pool becomes overcommitted by applying Workload Balancing optimization recommendations, XenCenter® prompts you whether you want to continue applying the recommendation. When Automation is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

enabled, Workload Balancing does not apply any power-management recommendations that exceed the number of host failures to tolerate in the High Availability plan.

It is possible to tweak how Workload Balancing applies recommendations in automated mode. For information, see Advanced Settings.

Enabling Power Management

Power management is the ability to turn the power on or off for physical hosts. In a Workload Balancing context, this term refers to powering hosts in a pool on or off based on the pool's total workload.

Configuring Workload Balancing power management on a host requires that:

- The hardware for the host server has remote power on/off capabilities
- The Host Power On feature is configured for the host
- The host has been explicitly selected as a host to participate in (Workload Balancing) Power Management

In addition, if you want Workload Balancing to power off hosts automatically, you also need to configure:

- Workload Balancing is configured to apply recommendations automatically
- Workload Balancing is configured to apply Power Management recommendations automatically

When the pool is in Maximum Density mode, if Workload Balancing detects unused resources, it recommends powering off hosts until it eliminates all excess capacity in the pool. If WLB detects the pool has insufficient host capacity to shut down servers, it recommends leaving the servers on until the pool workload decreases enough. When you configure Workload Balancing to power off extra servers automatically, it applies these recommendations automatically and, therefore, behaves in the same way.

When a host is set to participate in Power Management, Workload Balancing makes power-on/off recommendations as needed. If you turn on the option to apply Power Management recommendations automatically, you do so at the pool level. However, you can specify which hosts from the pool you want to participate in Power Management.

Understanding Power Management behavior

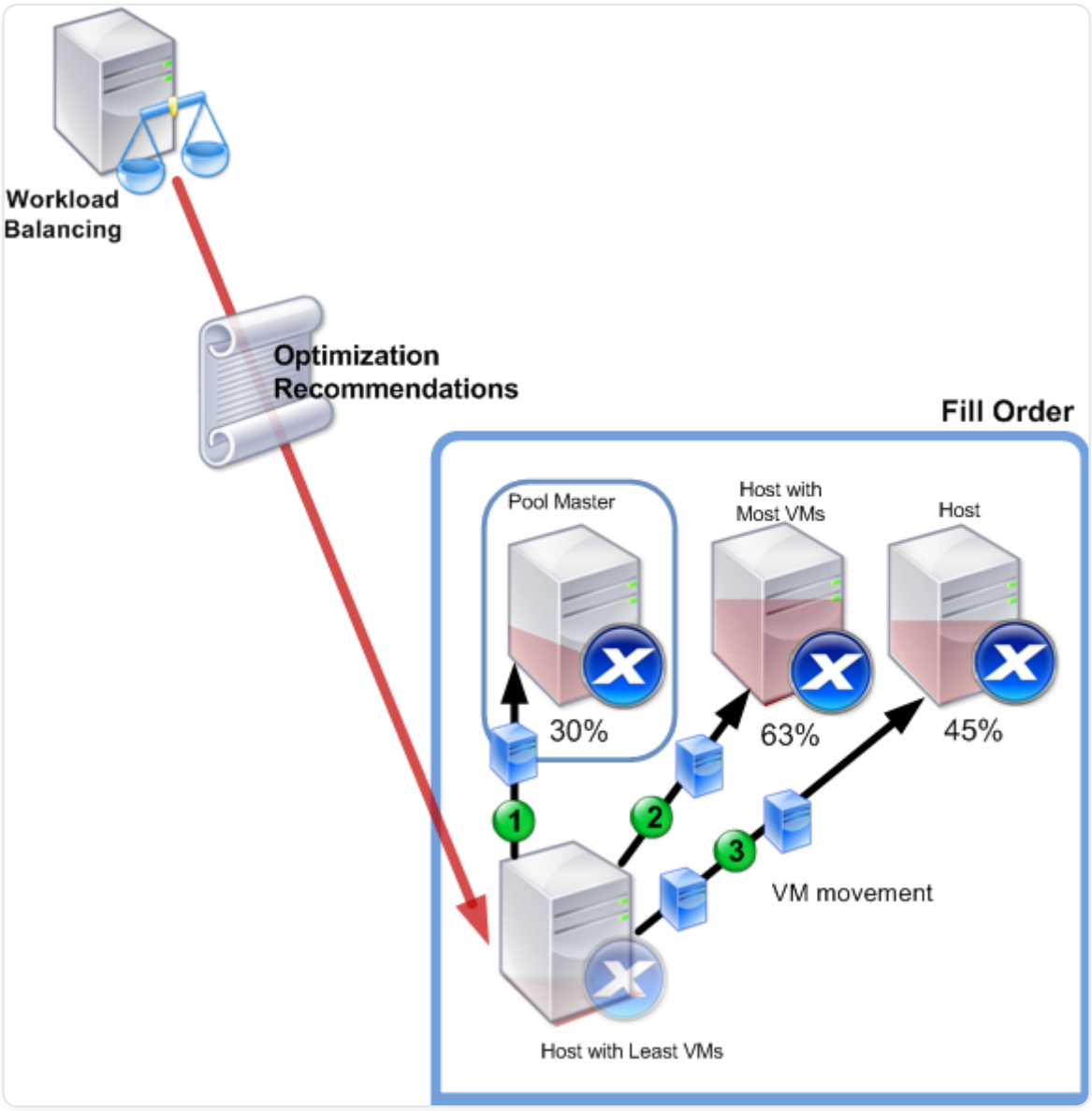
Before Workload Balancing recommends powering hosts on or off, it selects the hosts to transfer virtual machines to (that is, to "fill"). It does so in the following order:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Filling the pool coordinator since it is the host that cannot be powered off.
2. Filling the host with the most virtual machines.
3. Filling subsequent hosts according to which hosts have the most virtual machines running.

When Workload Balancing fills the pool coordinator, it does so assuming artificially low (internal) thresholds for the pool coordinator. Workload Balancing uses these low thresholds as a buffer to prevent the pool coordinator from being overloaded.

Workload Balancing fills hosts in this order to encourage density.



This illustration shows how, when consolidating VMs on hosts in Maximum Density mode, XenServer® fills the pool coordinator first, the most loaded server second, and the least loaded server third.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If Workload Balancing detects a performance issue while the pool is in Maximum Density mode, it addresses the issue by recommending migrating workloads among the powered-on hosts. If Workload Balancing cannot resolve the issue using this method, it attempts to power on a host. (Workload Balancing determines which hosts to power on by applying the same criteria it would if the optimization mode was set to Maximum Performance.)

When WLB runs in Maximum Performance mode, it powers on hosts until resource utilization on all hosts in the pool falls below the High threshold.

While migrating one or more VMs, if WLB determines that increasing capacity would benefit the pool's overall performance, it powers on hosts automatically or recommends doing so.

IMPORTANT:

Workload Balancing only recommends powering on a host that Workload Balancing powered off.

Designing environments for Power Management and VM consolidation

When you are planning XenServer implementations and you intend to configure automatic VM consolidation and power management, consider your workload design. For example, you might want to:

- **Place Different Types of Workloads in Separate Pools.** If you have distinct types of workloads or types of applications that perform better with certain types of hardware, consider whether to locate the VMs hosting these workloads in different pools.

  Because power management and VM consolidation are managed at the pool level, design pools so they contain workloads that you want consolidated at the same rate. Factor in considerations such as those discussed in the Advanced Settings topic.
- **Exclude Hosts from Workload Balancing.** Some hosts might have to be always on. For more information, see Excluding Hosts from Recommendations.

To apply optimization recommendations automatically

1. In the **Resources** pane of XenCenter, select **XenCenter** > your resource pool.
2. In the **Properties** pane, select the **WLB** tab.
3. In the **WLB** tab, select **Configure WLB**.
4. In the left pane, select **Automation**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Select one or more of the following check boxes:

   - **Automatically apply Optimization recommendations.** When you select this option, you do not need to accept optimization recommendations manually. Workload Balancing automatically accepts the optimization and placement recommendations it makes.
   - **Automatically apply Power Management recommendations.** The behavior of this option varies according to the pool's optimization mode:

     - **Maximum Performance Mode.** When **Automatically apply Power Management recommendations** is enabled, Workload Balancing automatically powers on hosts when doing so improves the host performance.
     - **Maximum Density Mode.** When **Automatically apply Power Management recommendations** is enabled, Workload Balancing automatically powers off hosts when resource utilization drops below the Low threshold. That is, Workload Balancing powers off hosts automatically during low usage periods.

6. Do one of the following:

   - If you want to configure power management, select **Automation/Power Management** and proceed to the following section.
   - If you do not want to configure power management and you are finished configuring automation, select **OK**.

To select servers for power management

1. In the Power Management section, select the hosts that you want Workload Balancing to power on and off automatically.

   NOTE:

   Selecting hosts for power management recommendations without selecting **Automatically apply Power Management recommendations** results in Workload Balancing suggesting power management recommendations but not applying them automatically for you.

2. Click **OK**. If none of the physical servers in the resource pool support remote power management, Workload Balancing displays the message, **No hosts support Power Management**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- Workload Balancing

Changing the Critical Thresholds

This topic provides guidance about how to modify the default Critical thresholds and how to set values for the Critical threshold alter **High**, **Medium**, and **Low** thresholds.

This information is only provided for reference while changing thresholds. To understand the concepts discussed in this topic, it is important to read them in the fuller context of the information provided in the Workload Balancing documentation.

Overview

When evaluating utilization, Workload Balancing compares its daily average to four thresholds: low, medium, high, and critical. After you specify (or accept the default) critical threshold, Workload Balancing sets the other thresholds relative to the critical threshold on a pool. You might want to change Critical thresholds as a way of controlling when optimization recommendations are triggered.

Workload Balancing evaluates CPU, Memory, Network Read, Network Write, Disk Read, and Disk Write utilization for physical hosts in a resource pool.

Workload Balancing determines whether to recommend relocating a workload and whether a physical host is suitable for a virtual-machine workload by evaluating:

- Whether a resource's critical threshold is met on the physical host
- (If the critical threshold is met) the importance assigned to a resource

NOTE:

To prevent data from appearing artificially high, Workload Balancing evaluates the daily averages for a resource and smooths utilization spikes.

Workload Balancing determines whether to produce recommendations based on if the averaged historical utilization for a resource violates its threshold. **Workload Balancing** recommendations are triggered when the **High threshold** in **Maximum Performance** mode or Low and Critical thresholds for Maximum Density mode are violated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you specify a new Critical threshold for a resource, **Workload Balancing** resets the resource's other thresholds relative to the new **Critical threshold**. (To simplify the user interface, the **Critical threshold** is the only threshold you can change through XenCenter.)

For more information, see Workload Balancing documentation.

Default settings for thresholds

The following table shows the default values for the Workload Balancing thresholds:

SETTING	DEFAULT	HIGH	MEDIUM	LOW
CPU Utilization	90%	76.5%	45%	22.5%
Free Memory	51 MB	63.75 MB	510 GB	1,020 GB
Network Read	25 MB/s	21.25 MB/s	12.5 MB/s	6.25 MB/s
Network Write	25 MB/s	21.25 MB/s	12.5 MB/s	6.25 MB/s
Disk Read	25 MB/s	21.25 MB/s	12.5 MB/s	6.25 MB/s
Disk Write	26 MB/s	21.25 MB/s	12.5 MB/s	6.25 MB/s

To calculate the values for the High, Medium, and Low resource metrics, Workload Balancing multiplies the new value for the Critical threshold with the following factors:

- High Threshold Factor: 0.85
- Medium Threshold Factor: 0.50
- Low Threshold Factor: 0.25

To calculate threshold values for free memory, Workload Balancing multiplies the Critical threshold with these factors:

- High Threshold Factor: 1.25
- Medium Threshold Factor: 10.0
- Low Threshold Factor: 20.0

This behavior means that if you increase, for example, a Critical threshold to 95%, WLB automatically resets the other thresholds to the following:

- High threshold to 80.75%

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Medium threshold to 47.5%
- Low threshold to 23.75%

To perform this calculation for a specific threshold, multiply the factor for the threshold with the value you entered for the critical threshold for that resource:

```
High, Medium, or Low Threshold = Critical Threshold &ast; Threshold Factor
```

For example, if you change the Critical threshold for Network Reads to 40 MB/s and you want to know its other thresholds:

- To obtain the Low threshold, multiply 40 by 0.25
- To obtain the Medium threshold, multiply 40 by 0.50
- To obtain the High threshold, multiply 40 by 0.85

To prevent the pool coordinator from becoming overloaded, Workload Balancing automatically sets the pool coordinator's Critical Thresholds at lower values.

How other thresholds trigger recommendations

While the Critical threshold triggers many recommendations, other thresholds can also trigger recommendations, as follows:

High threshold

- **Maximum Performance**. Exceeding the High threshold triggers optimization recommendations to relocate a virtual machine to a host with a lower resource utilization.
- **Maximum Density**. Workload Balancing doesn't recommend placing a VM on host if doing so causes the utilization of any host resource to exceed the High threshold value.

Low threshold

- **Maximum Performance**. Workload Balancing does not trigger recommendations from the Low threshold.
- **Maximum Density**. When a metric value drops below the Low threshold, it signals Workload Balancing that hosts are being underutilized. This signal triggers an optimization recommendation to consolidate virtual machines on fewer hosts. Workload Balancing continues to recommend moving virtual machines onto a host until the metric values for one of the host's resources reaches its High threshold.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

However, if after a VM is relocated, utilization of a resource on the new host exceeds its Critical threshold, WLB temporarily uses an algorithm similar to the Maximum Performance algorithm to find a new host for the VMs. Workload Balancing continues to use this algorithm to recommend moving virtual machines until resource utilization on hosts across the pool falls below the High threshold.

To change the critical thresholds

1. Select the pool in the **Resources** pane, select the **WLB** tab, and then select **Settings**.
2. In the left pane, select **Critical Thresholds**.
3. In the **Critical Thresholds** page, accept or enter a new value in the **Critical Thresholds** boxes. Workload Balancing uses these thresholds when making virtual-machine placement and pool-optimization recommendations. Workload Balancing strives to keep resource utilization on a host below the critical values set.

Related documentation

XenServer Current Release

- Workload Balancing

Tuning Metric Weightings

Workload Balancing uses metric weightings, a method of assigning importance to resources, to determine what hosts to optimize first.

NOTE:

Before tuning metric weightings, Citrix recommends reading about the optimization and consolidation process in the Workload Balancing documentation. The information in this article is a subset of that information and is only meant to be used as a reference when changing the user interface.

When **Workload Balancing** is processing optimization recommendations, it creates an optimization order. Workload Balancing determines the optimization order by ranking the hosts to address first according to which hosts have the highest metric values for whatever resource is ranked as the most important in the metric weightings page.

How Workload Balancing uses metric weightings when determining which hosts and VMs to process first varies according to the optimization mode, Maximum Density, or Maximum

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Performance. In general, metric weightings are used when a pool is in Maximum Performance mode. However, when Workload Balancing is in Maximum Density mode, it does use metric weightings if a resource exceeds its Critical threshold.

How metric weightings apply in Maximum Performance mode

In **Maximum Performance** mode, **Workload Balancing** uses metric weightings to determine:

- Which hosts' performance to address first
- Which VMs to recommend migrating first

For example, if you rank Network Writes as the most important resource, Workload Balancing first addresses performance issues and makes optimization recommendations for the host with the most Network Writes per second.

How metric weightings apply in Maximum Density mode

In Maximum Density mode, Workload Balancing only uses metric weightings when a host reaches the Critical threshold. Then Workload Balancing applies a Maximum Performance-like algorithm until no Hosts are exceeding the Critical thresholds. When using the Maximum Performance-like algorithm, Workload Balancing uses metric weightings to determine the optimization order in the same way as it does for Maximum Performance mode.

If two or more hosts have resources exceeding their Critical thresholds, Workload Balancing verifies the importance you set for each resource before determining which host to optimize first and which VMs on that host to relocate first.

For example, your pool contains Host A and Host B, which are in the following state:

- The CPU utilization on Host A exceeds the Critical threshold for CPU. The metric weighting for CPU utilization is set to the far right of the slider **(More Important)**.
- The memory utilization on Host B exceeds the Critical threshold for memory. The metric weighting for memory utilization is set to the far left of the slider **(Less Important)**.

Workload Balancing recommends optimizing Host A first because the resource on it that reached the Critical threshold is the resource assigned the highest weight. After Workload Balancing determines that it needs to address the performance on Host A, Workload Balancing then begins recommending placements for VMs on that host. These recommendations begin with the VM that has the highest CPU utilization, since that CPU utilization is the resource with the highest weight.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After Workload Balancing has recommended optimizing Host A, it makes optimization recommendations for Host B. When it recommends placements for the VMs on Host B, it does so by addressing CPU utilization first, since CPU utilization was assigned the highest weight.

If there are more hosts that need optimization, Workload Balancing addresses the performance on those hosts according to what host has the third highest CPU utilization.

By default, all metric weightings are set to the farthest point on the slider **(More Important)**.

NOTE:

The weighting of metrics is relative. This behavior means that if all metrics are set to the same level, even if that level is **Less Important**, they are all weighted the same. The relation of the metrics to each other is more important than the actual weight at which you set each metric.

To edit metric weighting factors

1. Select the pool in the **Resources** pane, select the **WLB** tab, and then select **Settings**.
2. In the left pane, select **Metric Weighting**.
3. In the **Metric Weighting** page, as desired, adjust the sliders beside the individual resources.

   Moving the slider towards **Less Important** indicates that ensuring virtual machines always have the highest amount of this resource available is not as vital on this resource pool.

Related documentation

XenServer Current Release

- Workload Balancing

Excluding Hosts from Recommendations

When configuring Workload Balancing, you can specify that specific physical hosts are excluded from Workload Balancing optimization and placement recommendations, including Start On placement recommendations.

When to exclude hosts

Situations when you might want to exclude hosts from recommendations include when:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You want to run the pool in Maximum Density mode and consolidate and shut down hosts, but there are specific hosts you want to exclude from this behavior.
- When two VM workloads must always run on the same host (for example, if they have complementary applications or workloads).
- You have workloads that you do not want moved (for example, domain controllers or SQL Server).
- You want to perform maintenance on a host and you do not want virtual machines placed on the host.
- The performance of the workload is so critical that the cost of dedicated hardware is irrelevant.
- Specific hosts are running high-priority workloads (virtual machines), and you do not want to use the High Availability feature to prioritize these virtual machines.
- The hardware in the host is not the optimum for the other workloads in the pool.

Regardless of whether you specify a fixed or scheduled optimization mode, excluded hosts remain excluded even when the optimization mode changes. To prevent Workload Balancing from powering down a host automatically, consider not enabling Power Management for that host. For more information, see Optimizing and Managing Power Automatically.

To exclude hosts from placement and optimization recommendations

1. Select the pool in the **Resources** pane, select the **WLB** tab, and select **Settings**.
2. In the left pane, select **Excluded Hosts**.
3. In the **Excluded Hosts** page, select the hosts for which you do not want Workload Balancing to recommend alternate placements and optimizations.

Related documentation

XenServer Current Release

- Workload Balancing

Excluding VMs from Recommendations

When configuring Workload Balancing, you can specify that specific VMs are excluded from Workload Balancing optimization and placement recommendations.

When to exclude VMs

Situations when you might want to exclude VMs from recommendations include when:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When two VM workloads must always run on the same host (for example, if they have complementary applications or workloads).
- You have workloads that you do not want moved (for example, domain controllers, DNS server, or SQL server).

Regardless of whether you specify a fixed or scheduled optimization mode, excluded VMs remain excluded even when the optimization mode changes.

To exclude VMs from placement and optimization recommendations

1. Select the VM in the **Resources** pane, select the **General** tab, and select **Properties**.
2. In the left pane, select **General**.
3. In the **General** page, in the **Tags:** field, select **Edit tags**.
4. Specify the new tag `wlb_excluded` and click **Create**.

Related documentation

XenServer® 8

- Workload Balancing

Advanced Settings

The settings in the **Advanced** dialog primarily fine-tune how Workload Balancing applies recommendations when it is running in automated mode.

IMPORTANT:

After Workload Balancing is running for a period, if you do not receive optimal placement recommendations, evaluate your performance thresholds as described in the Workload Balancing documentation. It is critical to set Workload Balancing to the correct thresholds for your environment or its recommendations might not be appropriate.

When WLB runs in automated mode, the frequency of optimization and consolidation recommendations and how soon they are automatically applied is a product of multiple factors. These factors include:

- **VM migration interval**: How long you specify Workload Balancing waits before applying another optimization recommendation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Recommendation count**: The number of recommendations Workload Balancing must make before applying a recommendation automatically
- **Recommendation severity**: The severity level a recommendation must achieve before the optimization is applied automatically
- **Optimization aggressiveness**: The level of consistency in recommendations (recommended virtual machines to move, destination hosts) Workload Balancing requires before applying recommendations automatically

VM migration interval

You can specify how many minutes WLB waits after the last time a particular VM was moved, before it generates another optimization recommendation that includes that particular VM.

The recommendation interval is designed to prevent Workload Balancing from generating recommendations for artificial reasons (for example, if there was a temporary utilization spike).

When Automation is configured, it is especially important to be careful when modifying the recommendation interval. If an issue occurs that leads to continuous, recurring spikes, increasing the frequency (that is, setting a lower number) can generate many recommendations and, therefore, relocations.

NOTE:

Setting a recommendation interval does not affect how long Workload Balancing waits to factor recently rebalanced servers into recommendations for Start-On Placement, Resume, and Maintenance Mode.

Recommendation count

Every two minutes, Workload Balancing checks to see if it can generate recommendations for the pool it is monitoring. When you enable Automation, you can specify the number of times a consistent recommendation must be made before Workload Balancing can automatically apply the recommendation. To do so, you configure a setting known as the Recommendation Count. The **Recommendation Count** and the **Optimization Aggressiveness** setting let you fine-tune the automated application of recommendations in your environment.

As described in the overview section, Workload Balancing uses the similarity of recommendations to perform the following checks:

- Vet if the recommendation is truly needed

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Determine if the destination host has stable enough performance over a prolonged period to accept a relocated VM (without needing to move it off the host again shortly).

Workload Balancing uses the Recommendation Count value to determine a recommendation must be repeated before Workload Balancing automatically applies the recommendation.

Workload Balancing uses this setting as follows:

1. Every time Workload Balancing generates a recommendation that meets its consistency requirements, as indicated by the Optimization Aggressiveness setting, Workload Balancing increments the Recommendation Count. If the recommendation does not meet the consistency requirements, Workload Balancing can reset the Recommendation Count to zero, depending on the factors described in the Workload Balancing documentation
2. When Workload Balancing generates enough consistent recommendations to meet the value for the Recommendation Count, as specified in the Recommendations text box, it automatically applies the recommendation.

If you choose to modify this setting, the value to set varies according to your environment. Consider these scenarios:

- If server loads and activity increase quickly in your environment, you can increase the value for the Recommendation Count. Workload Balancing generates recommendations every two minutes. For example, if you set this interval to `3`, then six minutes later Workload Balancing applies the recommendation automatically.
- If server loads and activity increase gradually in your environment, you can decrease the value for the Recommendation Count.

Accepting recommendations uses system resources and affects performance when Workload Balancing is relocating the virtual machines. Increasing the Recommendation Count increases the number of matching recommendations that must occur before Workload Balancing applies the recommendation. This setting encourages Workload Balancing to apply more conservative, stable recommendations and can decrease the potential for spurious virtual machine moves. However, the Recommendation Count is set to a conservative value by default.

Because of the potential impact adjusting this setting might have on your environment, change it with extreme caution. We advise that you test and iteratively change the value, or change it under the guidance of Citrix® Technical Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Recommendation severity

All optimization recommendations include a severity rating (Critical, High, Medium, Low) that indicates the importance of the recommendation. Workload Balancing bases this rating on a combination of factors including the configuration options you set, such as:

- Thresholds and metric tunings
- Resources available for the workload
- Resource-usage history.

When you configure Workload Balancing to apply optimization recommendations automatically, you can set the minimum severity level to associate with a recommendation before Workload Balancing automatically applies it.

Optimization aggressiveness

To provide more assurance when running in automated mode, Workload Balancing has consistency criteria for accepting optimizations automatically to prevent moving VMs due to spikes and anomalies. In automated mode, Workload Balancing does not accept the first recommendation it produces. Instead, Workload Balancing waits to automatically apply a recommendation until a host or VM exhibits consistent behavior over time. The phrase "consistent behavior over time" refers to factors such as whether a host continues to trigger recommendations and whether the same VMs on that host continue to trigger recommendations.

Workload Balancing determines if a behavior is consistent by using criteria for consistency and by having criteria for the number of times the same recommendation is made (that is, the Recommendation Count). You can configure how strictly you want Workload Balancing to apply the consistency criteria using an **Optimization Aggressiveness** setting.

While Citrix primarily designed the **Optimization Aggressiveness** setting for demonstration purposes, you can use this setting to control the amount of stability you want in your environment before Workload Balancing applies an optimization recommendation. The most stable setting (Low aggressiveness) is configured by default. In this context, the term "stable" refers to the similarity of the recommended changes over time, as explained throughout this section.

Workload Balancing uses up to four criteria to ascertain consistency. The number of criteria that must be met varies according to the level you set in the **Optimization Aggressiveness** setting. The lower the level (for example, Low or Medium) the less aggressively Workload Balancing is in accepting a recommendation. In other words, Workload Balancing is stricter about requiring criteria to match (or less cavalier or aggressive) about consistency when the aggressiveness is set to Low.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, if the aggressiveness level is set to Low, Workload Balancing requires that each criterion for Low is met the number of times specified in the **Recommendations** box (where you specify the Recommendation Count value) before automatically applying the recommendation.

For example, if you set the Recommendation Count to `3`, Workload Balancing waits until it sees all the criteria for Low are met and repeated in three consecutive recommendations. This behavior helps ensure that the VM actually needs to be moved and that the destination host Workload Balancing recommends has consistently stable resource utilization over a longer period. It reduces the potential for a recently moved virtual machine to be moved off a host due to host performance changes after the move. By default, this setting is set to a conservative setting (Low) to encourage stability.

For information about the criteria for the Low aggressiveness level, see Workload Balancing documentation.

Citrix does not recommend increasing the **Optimization Aggressiveness** to increase the frequency with which your hosts are being optimized. If you feel that your hosts are not being optimized quickly or frequently enough, try adjusting the Critical thresholds, as described in Changing the Critical Thresholds.

For details about the consistency criteria associated with the different levels of aggressiveness, see the Workload Balancing documentation.

If you find that Workload Balancing is not automatically applying optimization recommendations frequently enough, you might want to increase the aggressiveness setting. However, Citrix strongly recommends reviewing the information in the Workload Balancing documentation before doing so.

To configure virtual machine recommendation intervals

1. Select the pool in the **Infrastructure** view, select the **WLB** tab, and then select **Settings**.
2. In the left pane, select **Advanced**.
3. In the **VM Migration Interval** section, do one or more of the following:

    - In **Minutes to wait**, enter the number of minutes you want Workload Balancing to wait before making another optimization recommendation on a newly rebalanced server.
    - In the **Recommendation Count** box, type a value for the number of optimization recommendations you want Workload Balancing to make before it applies an optimization recommendation automatically.
    - From the **Recommendation Severity** list, select a minimum severity level before optimizations are applied automatically.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- From the **Optimization Aggressiveness** list, specify how aggressively Workload Balancing automatically applies optimization recommendations.

Pool audit trail granularity

Workload Balancing enables you to specify the amount of data to be collected in the Pool Audit Trail report. This functionality also allows you to search and filter the audit trail logs by specific users, objects, and by time.

Pool Audit Trail Granularity is set to **Minimum** by default. This option captures limited amount of data for specific users and object types. You can modify the setting at any time based on the level of detail you would require in your report. For example, set the granularity to **Medium** for a user-friendly report of the audit log. If you require a detailed report, set the option to **Maximum**.

IMPORTANT:

Setting the Pool Audit Trail Granularity to Maximum can cause the Workload Balancing server to use more disk space and memory. If you choose to set the granularity to Maximum, it is recommended that you carefully monitor the WLB server for disk space, memory usage, and CPU usage. If you think the WLB Server is under resource pressure, you can take one of the following actions:

- Change the granularity setting to Medium or Minimum.
- Consider expanding your WLB server's memory.
- Consider expanding the size of the hard disk.

For more information, see Workload Balancing Report Glossary and Audit Log Events.

Related documentation

XenServer Current Release

- Workload Balancing

Administering Workload Balancing

Some administrative tasks you might want to perform on Workload Balancing include:

- Disconnecting from Workload Balancing
- Changing the Workload Balancing virtual appliance that a pool uses

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Changing the credentials Workload Balancing or XenServer use to communicate

You can also administer the Workload Balancing virtual appliance using the Workload Balancing service commands. These commands let you determine Workload Balancing virtual appliance status, change user accounts, and increase logging detail.

NOTE:

For information about configuring Workload Balancing to use a different certificate or configuring XenServer to verify the identity of a certificate, see the Workload Balancing documentation.

Related documentation

XenServer Current Release

- Workload Balancing

Disconnecting from Workload Balancing

If you want to stop Workload Balancing (WLB) from monitoring your pool, you must disable Workload Balancing on the pool by disconnecting the Workload Balancing server.

When you disconnect a pool from the WLB virtual appliance, Workload Balancing permanently deletes pool information from the WLB database and stops collecting data for that pool. If you want to use the same WLB virtual appliance to manage the pool again, reenter the appliance's information in the **Connect to WLB Server** dialog box.

IMPORTANT:

If you only want to stop Workload Balancing temporarily, select the **WLB** tab and select the **Pause** button.

To disconnect from Workload Balancing

1. In the **Resource** pane of XenCenter®, choose the resource pool on which you want to stop Workload Balancing.
2. From the **Pool** menu, select **Disconnect Workload Balancing Server**. The **Disconnect Workload Balancing server** dialog box appears.
3. Click **Disconnect** to stop Workload Balancing from monitoring the pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you disconnected the pool from the Workload Balancing virtual appliance, to re-enable Workload Balancing on that pool, you must reconnect to the appliance.

Related documentation

XenServer Current Release

- Workload Balancing

Reconfiguring a Pool to Use Another WLB Appliance

You can reconfigure a pool to use a different Workload Balancing virtual appliance.

However, to prevent the old Workload Balancing appliance from inadvertently remaining configured and collecting data for the pool, disconnect the pool from the old Workload Balancing appliance **before** connecting the pool to the new Workload Balancing appliance.

Once the pool is disconnected from the old Workload Balancing appliance, reconnect the pool by specifying the new Workload Balancing appliance name.

To use a different Workload Balancing appliance

1. On the pool you want to use a different Workload Balancing appliance, from the **Pool** menu, select **Disconnect Workload Balancing Server** and select **Disconnect** when prompted. For instructions, see Disconnecting from Workload Balancing.
2. In the **WLB** tab, select **Connect**. The **Connect to WLB Server** dialog appears.
3. In the **Address** box, type the IP address or host name (FQDN) name of the new Workload Balancing appliance.

   If the new Workload Balancing appliance uses different credentials, you must also enter the new credentials.

   NOTE:

   Enter all the information that you would normally enter when you initially connect a pool to Workload Balancing. For information, see Connecting to Workload Balancing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- Workload Balancing

Updating Workload Balancing credentials

After initial configuration, to update the credentials the XenServer® server and the Workload Balancing appliance use to communicate, complete the following process:

1. Disconnect from Workload Balancing, as described in a following section.
2. Change the WLB credentials by editing the WlbConfig file (run the `WlbConfig` command in the console on the Workload Balancing virtual appliance). For more information, see the Workload Balancing documentation.
3. Re-enable Workload Balancing and specify the new credentials, as described in a following section.

Situations when you might want to use these steps include:

- If you have to change the user account XenServer uses to communicate with Workload Balancing
- If you receive an error message that the Workload Balancing credentials are no longer valid
- If the service is unavailable

If you want to modify settings for thresholds and change the priority given to specific resources, see Editing Workload Balancing Settings.

To disconnect from Workload Balancing

1. In the **Resource** pane of XenCenter®, select the resource pool on which you want to stop Workload Balancing.
2. From the **Pool** menu, select **Disconnect Workload Balancing Server**. The **Disconnect Workload Balancing server** dialog box appears.
3. Select **Disconnect** to permanently stop Workload Balancing from monitoring the pool.

To reenable Workload Balancing and specify the new credentials

1. After the progress bar completes, select **Connect**. The Connect to WLB Server dialog box appears.
2. Select **Update Credentials**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the Server Address section, modify the following as desired:

   - In the **Address** box, type the IP address or FQDN of the Workload Balancing appliance.
   - (Optional) If you changed the port number during Workload Balancing Configuration, enter that port number. The port number you specify in this box and during Workload Balancing Configuration is the port number XenServer uses to connect to Workload Balancing.

     By default, XenServer connects to Workload Balancing on port 8012.

     NOTE:

     Only edit this port number if you have changed it during Workload Balancing Setup. The port number value specified during Setup and in the **Workload Balancing Configuration** dialog must match.

4. In the **WLB Server Credentials** section, enter the user name (for example, `wlbuser`) and password the systems running XenServer use to connect to the Workload Balancing server.
5. In the **XenServer Credentials** section, enter the user name and password for the pool you are configuring (typically the password for the pool coordinator). Workload Balancing uses these credentials to connect to the computers running XenServer in that pool. To use the credentials with which you are currently logged into XenServer, select the **Use the current XenCenter credentials** check box.

Related documentation

XenServer Current Release

- Workload Balancing

Entering maintenance mode with Workload Balancing Enabled

When WLB is enabled, if you take a host offline for maintenance, XenServer® automatically migrates the VMs running on that host to their optimal servers when available. XenServer migrates them based on Workload Balancing recommendations (performance data, your placement strategy, and performance thresholds).

If an optimal server is not available, the words **Click here to suspend the VM** appear in the **Enter Maintenance Mode** dialog box. In this case, Workload Balancing does not recommend a placement because no host has sufficient resources to run this virtual machine. You can either suspend this virtual machine or exit maintenance mode and suspend a virtual machine on another

© 1997–2026 Citrix Systems, Inc. All rights reserved.

host in the same pool. Then, if you reenter the **Enter Maintenance Mode** dialog box, Workload Balancing might be able to list a host that is a suitable candidate for migration.

NOTE:

When you take a server offline for maintenance and Workload Balancing is enabled, the words "Workload Balancing" appear in the upper-right corner of the **Enter Maintenance Mode** dialog.

To enter maintenance mode with Workload Balancing enabled

1. In the Resources pane, select the server and then do one of the following:
   - Right-click and select **Enter Maintenance Mode** on the shortcut menu.
   - On the **Server** menu, select **Enter Maintenance Mode**.
2. Select **Enter Maintenance Mode**. The VMs running on the server are automatically migrated to the optimal host based on Workload Balancing's performance data, your placement strategy, and performance thresholds.

To take the server out of maintenance mode

1. In the **Resources** pane, select the server and then do one of the following:
   - Right-click and select **Exit Maintenance Mode** on the shortcut menu.
   - On the **Server** menu, select **Exit Maintenance Mode**.
2. Select **Exit Maintenance Mode**.

   When you remove a server from maintenance mode, XenServer automatically restores that server's original virtual machines to that server.

Related documentation

XenServer Current Release

- Workload Balancing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting Workload Balancing

While Workload Balancing usually runs smoothly, this help system provides a series of topics with guidance in case you encounter issues. Extra troubleshooting topics are provided in the Workload Balancing documentation.

Here are a few tips for resolving general Workload Balancing issues:

General troubleshooting tips

Start troubleshooting by reviewing the Workload Balancing log. You can find the log in the Workload Balancing virtual appliance in this location (by default):

```
/var/log/wlb
```

Also, you can also see the event logs in the XenCenter® **Navigation** pane, select **Notifications** and then **Events** for more information.

Error messages

Workload Balancing displays error messages in the **Alerts** view in XenCenter and, sometimes, on the screen as dialog boxes.

Related documentation

XenServer Current Release

- Workload Balancing

Issues Entering Workload Balancing Credentials

If you cannot get Workload Balancing to accept the appliance user account and password when configuring the **Connect to WLB Server** dialog, try the following:

- Ensure the Workload Balancing virtual appliance is imported and was configured correctly and all of its services are running by using the following command: `service workloadbalancing start`
- Using Issues Starting Workload Balancing as a guide, check to make sure you are entering the correct credentials.
- Enter the Workload Balancing server's IP address if you are having trouble entering the Workload Balancing fully qualified domain name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can enter the host name of the Workload Balancing appliance in the **Address** box, but it must be a fully qualified domain name. For example, `yourcomputername.yourdomain.net`.

Related documentation

XenServer Current Release

- Workload Balancing

Issues Starting Workload Balancing

After importing and configuring the Workload Balancing appliance, you might receive an error message that XenServer® and Workload Balancing cannot connect to each other. If so, you might have entered the incorrect credentials in the **Connect to WLB Server** dialog. To isolate this issue, try:

- Verifying the credentials you entered in the **Connect to WLB Server** dialog match the credentials that you created on the Workload Balancing server and on the XenServer server
- Verifying the IP address or FQDN of the Workload Balancing appliance you entered in the **Connect to WLB Server** dialog is correct.
- Verifying the account credentials for the Workload Balancing account you created during Workload Balancing Configuration match the credentials you entered in the **Connect to WLB Server** dialog.

Related documentation

XenServer Current Release

- Workload Balancing

Issues with Workload Balancing certificates

Certificate verification is enabled by default. To connect the Workload Balancing virtual appliance with XenServer®, you must import the Workload Balancing certificate into your XenServer pool.

If your pool can't connect to Workload Balancing, verify whether your certificate configuration is the cause by disabling certificate checking for Workload Balancing:

1. Get the pool UUID:

```
xe pool-list
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Disable certificate verification:

```
xe pool-param-set wlb-verify-cert=false uuid=<uuid_of_pool>
```

If your pool can connect to Workload Balancing with certificate verification turned off, the issue is with your certificate configuration. If it cannot connect, the issue is with either your Workload Balancing credentials or your network connection. Contact Support or see Troubleshoot Workload Balancing for more information.

Ensure that you enable certificate checking again after troubleshooting your issue:

1. Get the pool UUID:

```
xe pool-list
```

2. Enable certificate verification:

```
xe pool-param-set wlb-verify-cert=true uuid=<uuid_of_pool>
```

Related documentation

XenServer Current Release

- Workload Balancing

Workload Balancing Connection Errors

If you receive a connection error in the Workload Balancing Status line on the **WLB** tab, you might need to reconfigure Workload Balancing on that resource pool.

Click the **Connect** button on the **WLB** tab and enter the server credentials again.

Typical causes for this error include changing the credentials of the WLB virtual appliance or pool coordinator, changing the name of the WLB virtual appliance, or having incorrect certificate configuration.

Related documentation

XenServer Current Release

- Workload Balancing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Issues changing Workload Balancing servers

If you connect a pool to a different Workload Balancing virtual appliance without first disconnecting the pool from the original Workload Balancing appliance, both appliances monitor the pool.

To solve this problem, you can do one of the following actions:

- Shut down and delete the old Workload Balancing appliance
- Manually stop the Workload Balancing services (analysis, data collector, and Web service) so that the appliance no longer monitors the pool

Citrix does not recommend using the `pool-initialize-wlb` xe command to remove or change the Workload Balancing server configuration.

Related documentation

XenServer Current Release

- Workload Balancing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Conversion Manager

Transform your VMware ESXi/vCenter VMs to XenServer® quickly and easily with the Conversion Manager virtual appliance. Effortlessly batch-migrate multiple VMs in parallel, streamlining your entire migration process for maximum efficiency.

During the migration, XenCenter® prepares your VMs for networking and storage connectivity. After the conversion, the Conversion Manager automatically uninstalls VMware Tools from your VMs. To ensure full compatibility and optimal performance, we recommend installing XenServer VM Tools. These tools are vital for a fully supported setup, enhancing I/O performance, improving disk and network efficiency, and enabling key features such as clean shutdowns, reboots, suspensions, and live migrations. While VMs can run without XenServer VM Tools, performance might be limited. XenServer VM Tools are installed automatically on Linux VMs, and for Windows VMs, you can configure the Conversion Manager to install them automatically.

Learn more about moving from VMware to XenServer in our Tech Zone article: VMware to XenServer migration guide.

Conversion Manager enables you to:

- Batch convert multiple VMware ESXi/vCenter VMs in parallel using one simple wizard
- Map network settings between VMware and XenServer so your converted VMs can be up and running with the proper network settings
- Select a storage location where you would like your new XenServer VMs to run
- Optionally start each converted VM automatically after its conversion completes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTES:

- XenCenter does not remove or change your existing VMware environment. VMs are duplicated onto your XenServer environment and not removed from VMware. However, when converting Windows VMs with vTPM, the Conversion Manager removes the vTPM device from the original VMware Windows VM during the conversion process.
- Conversion Manager virtual appliance supports converting VMware ESXi/vCenter VMs with different storage such as thin provisioning, thick provisioning, IDE, and SCSI.
- Conversion Manager virtual appliance does not require the source VMs to have VMware Tools installed. You can perform conversion on VMware ESXi/vCenter VMs regardless of whether they have VMware Tools installed.
- Conversion Manager virtual appliance cannot convert VMware ESXi/vCenter Windows VMs with four or more disks into XenServer VMs. Your VMware ESXi/vCenter Windows VMs must have three or fewer disks.

Supported guest operating systems

For details of which guest operating systems can be converted, see Guest OS Feature Support.

Understand XenServer

Before you can convert your environment, it is suggested that you become familiar with XenServer concepts. For more information, see Technical overview.

To successfully convert VMware virtual machines to XenServer, perform the following tasks:

- Set up a basic XenServer environment, including installing XenServer. For more information, see Quick start and Install.
- Create a network in XenServer, assigning an IP address to a NIC. For more information, see Quick start.
- Connect to storage. For more information, see Quick start.

Compare VMware and XenServer terminology

The following table lists the approximate XenServer equivalent for common VMware features, concepts, and components:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VMWARE TERM	XENSERVER EQUIVALENT
VMware vSphere Client	XenCenter (the management console for XenServer)
VMware Tools	XenServer VM Tools (for Windows or Linux)
Cluster / Resource Pool	Resource Pool
Data Store	Storage Repository
vMotion	Live migration
Distributed Resource Scheduling (DRS)	Workload Balancing
High Availability (HA)	High Availability (HA)
vCenter Converter	Conversion Manager
Role Based Access Control (RBAC)	Role Based Access Control (RBAC)

Conversion overview

XenCenter and Conversion Manager virtual appliance create a copy of each targeted VM. After converting the targeted VM to a XenServer VM with comparable networking and storage connectivity, XenCenter imports the VM into your XenServer pool or host.

You can convert as few as one or two VMs or perform batch conversions of an entire environment. Simply select the VMs you want to convert and the Conversion Manager performs the conversions in batches of 10 VMs at a time, automatically selecting the next set of 10 VMs in the queue once the job is complete.

NOTE:

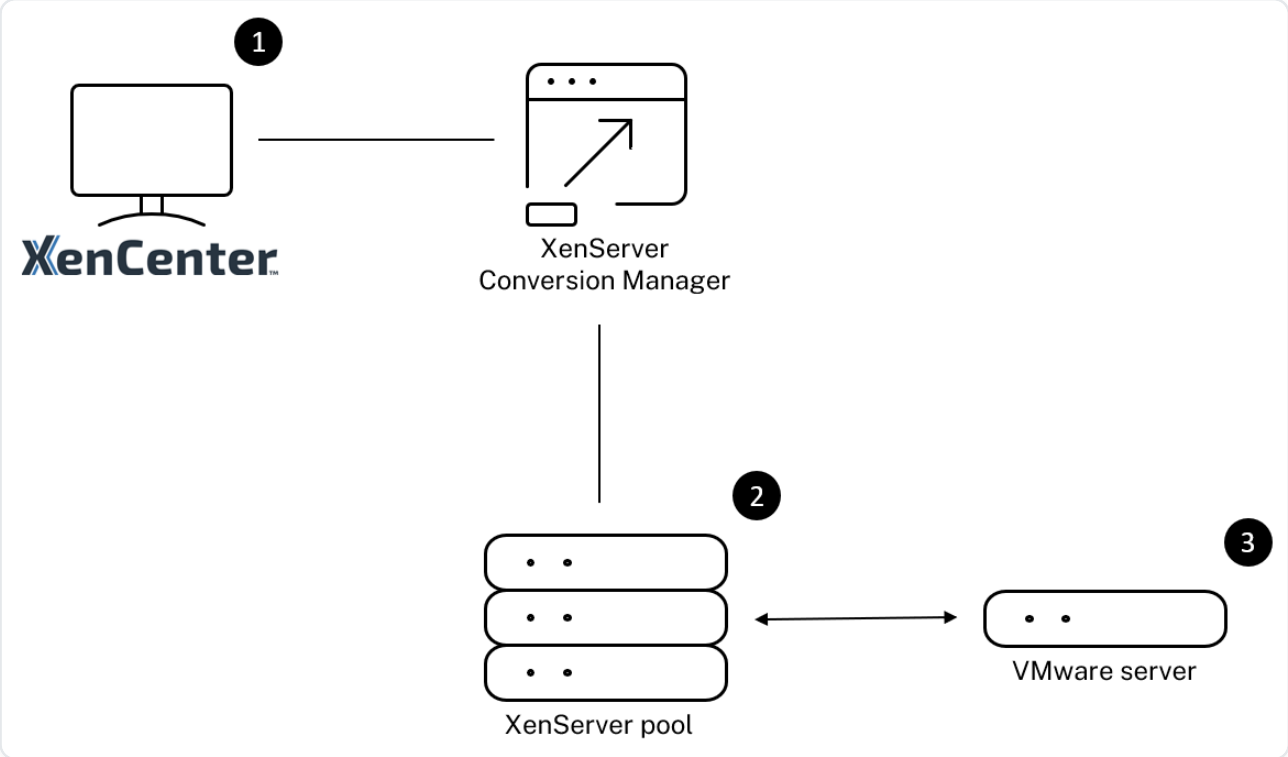
Before converting the VMs from vSphere, you must shut down the VMs (intended for conversion) on vSphere. Conversion Manager virtual appliance does not support converting a running VM using memory copied from vSphere to XenServer.

Also, before converting, ensure that a network and a storage controller exist in your VMware VM. The conversion process requires four items:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **XenCenter** - the XenServer management interface includes a conversion wizard where you set conversion options and control conversion. You can install XenCenter on your Windows desktop. XenCenter must be able to connect to XenServer and the Conversion Manager virtual appliance.
- **Conversion Manager virtual appliance** - a pre-packaged VM you import into the XenServer host or pool where you want to run the converted VMs. The virtual appliance converts the copies of the VMware ESXi/vCenter VMs into XenServer virtual machine format. After conversion, it imports these copies into the XenServer pool or host.
- **XenServer standalone host or pool** - the XenServer environment where you want to run the converted VMs.
- **VMware server** - Conversion Manager requires a connection to a VMware server that manages the VMs you want to convert. This connection can be to a vCenter Server, ESXi Server, or ESX Server. The VMs are not removed from the VMware server. Instead, the Conversion Manager Virtual Appliance makes a copy of these VMs and converts them to XenServer virtual-machine format.

The following illustration shows the relationships between these components:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

This illustration shows:

1. How XenCenter communicates with Conversion Manager virtual appliance.
2. How the Conversion Manager virtual appliance authenticates with the VMware server.
3. How the VMware server responds to the Conversion Manager virtual appliance during conversion.

The VMware server communicates with the Conversion Manager virtual appliance only when the appliance queries the VMware server for environment information and disk data throughout the conversion.

Summary of how to convert VMs

You can configure the Conversion Manager virtual appliance and start to convert VMs in just a few easy steps:

1. Download the latest version of the Conversion Manager virtual appliance from the XenServer Downloads page.
2. Import the Conversion Manager virtual appliance into XenServer using XenCenter.
3. Configure the Conversion Manager virtual appliance by using XenCenter.
4. From XenCenter, launch the conversion wizard and start to convert VMs.

For more information on converting VMware ESXi/vCenter VMs, see Get started with Conversion Manager.

Related documentation

XenServer 9

- Conversion Manager

What's new in Conversion Manager

Download the latest version of the Conversion Manager virtual appliance from the XenServer Downloads page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you already have a previous version of the Conversion Manager virtual appliance installed and want to upgrade to the latest version, there is no automatic upgrade path. Download the latest version of the virtual appliance and remove the older version from your system.

For more information on converting VMware ESXi/vCenter VMs, see Get started with Conversion Manager.

What's new in 2026.1.0

Released Jul 6, 2026

This release includes the following new features:

- Support for converting additional Linux guests: Red Hat Enterprise Linux 9, Rocky Linux 8 and 9, and Ubuntu 22.04 and 24.04.
- Support for converting Linux guests that use the XFS file system or UEFI boot mode.
- Support for converting VMs from VMware 9 to XenServer®.
- Support for converting VMs to XenServer 9.
- Support for converting a single virtual disk of up to 16 TiB on GFS2 storage repositories.
- A new option in XenCenter® to automatically start each VM after its conversion completes.
- (Preview) Support for converting Windows Server 2025 guests.

To use these features, ensure that your XenCenter is updated to the latest version.

Earlier releases

This section summarizes features from previous releases and their resolved issues. These earlier versions are superseded by the latest release, and we recommend updating to the latest version of the Conversion Manager virtual appliance as soon as it becomes available.

Conversion Manager 8.5.0

Released May 27, 2025

This release includes the following new features:

- VM template association: When converting a VM, you can associate it with a XenServer guest template. Using a template in the conversion ensures that the converted VMs have consistent configurations and behave more reliably.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- XenServer VM Tools configuration: As part of the conversion process, you can now configure whether the Windows drivers included in the XenServer VM Tools for Windows are automatically updated.
- Enhanced disk image import: Disk formats like VHD, VHDX, AVHDX, and VMDK are now better supported. The Conversion Manager automatically fixes up the operating system and installs the XenServer VM Tools after import.

To use these features, ensure that your XenCenter is updated to the latest version.

Conversion Manager 8.4.0

Released Dec 5, 2024

This release includes the following new features:

- The Conversion Manager now automatically uninstalls VMware Tools from your VMs and provides the option to install XenServer VM Tools. While VMs can run without XenServer VM Tools, performance might be limited. XenServer VM Tools are installed automatically on Linux VMs, and for Windows VMs, you can configure the Conversion Manager to install them automatically.

  NOTE:

  (Citrix Hypervisor 8.2 CU1 only) Automatic installation of XenServer VM Tools is not supported for Windows 10 (32-bit) Enterprise edition. Install XenServer VM Tools for Windows manually. For more information, see XenServer VM Tools for Windows.

- Support for Windows 11 VMs for conversion.

  NOTE:

  Only UEFI Boot mode or UEFI Secure Boot mode are supported.

- You can now convert Windows VMs that have an attached vTPM. The Conversion Manager automatically removes the existing vTPM and creates a XenServer vTPM for the VM.

This release contains fixes for the following issues:

- Windows VMs converted from VMware to XenServer using the Conversion Manager are incorrectly detected as Linux VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Conversion Manager 8.3.1

Released Feb 01, 2024

This release includes the following improvements:

- You can now batch convert multiple VMware ESXi/vCenter VMs in parallel at the same time.

  Simply select the VMs you want to convert and the Conversion Manager performs the conversions in batches of 10 VMs at a time, automatically selecting the next set of 10 VMs in the queue once the job is complete.

Get started with Conversion Manager

Using the Conversion Manager, you can easily convert your VMware ESXi/vCenter virtual machines (VMs) to XenServer® VMs in just a few steps:

1. Prepare your XenServer environment and review the prerequisite information.
2. Import and configure the Conversion Manager virtual appliance by using XenCenter.

   NOTE:

   If you already have a previous version of the Conversion Manager virtual appliance installed and want to upgrade to the latest version, there is no automatic upgrade path. Download the latest version of the virtual appliance from the XenServer downloads page and remove the older version from your system.

3. From XenCenter, launch the conversion wizard and begin converting your VMware ESXi/vCenter VMs to XenServer.
4. Complete the post-conversion tasks.
5. Review other conversion tasks.

Prepare your environment

Before converting your VMware environment, you must create and prepare the target XenServer standalone host or pool to run the converted VMware ESXi/vCenter VMs. Preparing your environment includes the following activities:

1. Defining a strategy of how you convert your VMware environment. Do you want to convert 1 or 2 VMs? Do you want to convert your entire environment? Do you want to create a pilot first to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ensure that your configuration is correct? Do you run both environments in parallel? Do you want to maintain your existing cluster design when you convert to XenServer?

2. Planning your networking configuration. Do you want to connect to the same physical networks? Do you want to simplify or change your networking configuration?
3. Installing XenServer on the hosts you want in the pool. Ideally, plug the NICs on the hosts into their physical networks before you begin installation.
4. Creating a pool and performing any basic networking configuration. For example, do the following:

   - Configure a network to connect to the VMware cluster on the XenServer host (if the cluster is not on the same network as the XenServer host).
   - Configure a network to connect to the storage array. That is, if you use IP-based storage, create a XenServer network that connects to the physical network of the storage array.
   - Create a pool and add hosts to this pool.

5. (For shared storage and XenServer pools.) Preparing the shared storage where you store the virtual disks and creating a connection to the storage, known as a Storage Repository (SR) on the pool.
6. (Optional) Although not a requirement for conversion, you might want to configure the administrator accounts on the XenServer pool to match those accounts on the VMware server. For information about configuring Role-based Access Control for Active Directory accounts, see Role-based access control.

Install XenServer and create a pool

Before you can convert VMware ESXi/vCenter VMs, ensure that you create a XenServer pool or host where you want to run the converted VMs. This pool must have networking configured so it can connect to the VMware server. You might also want to configure the same physical networks on the XenServer pool that you have in the VMware cluster, or simplify your networking configuration. If you want to run the converted VMs in a pool, create a storage repository before conversion and add the shared storage to the pool.

If you are new to XenServer, you can learn about XenServer basics, including basic installation and configuration, by reading Quick start.

XenServer environment considerations

Before installing XenServer and importing the virtual appliance, consider the following factors that might change your conversion strategy:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Guest operating systems supported for conversion

For details of which guest operating systems can be converted, see Guest OS Feature Support.

Host requirements

Select the host where you want to run the Conversion Manager virtual appliance. This host can be a stand-alone host or a host in the pool where you run the converted VMs.

For pools, you can run the virtual appliance on any host in the pool, provided its storage meets the storage requirements.

NOTE:

We recommend that you run only one Conversion Manager in a pool at a time.

The Conversion Manager virtual appliance requires a minimum of:

- XenServer 8.4 or XenServer 9
- Disk space: 30 GB of disk space
- Memory: 6 GB
- Virtual CPU allocation: 2 vCPU

Networking requirements

To convert VMware ESXi/vCenter VMs, the Conversion Manager virtual appliance needs connectivity to a physical network or VLAN that can contact the VMware server. (In the following sections, this network is referred to as the "VMware network".)

If the VMware server is on a different physical network than the hosts in the XenServer pool, add the network to XenServer before conversion.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- The time it takes for your VMs to be converted depends on the physical distance between your VMware and XenServer networks and also the size of your VM's virtual disk. You can estimate how long the conversion will last by testing the network throughput between your VMware server and XenServer.
- By default, the Conversion Manager uses HTTPS to download the VM's virtual disk during VM conversion. To speed up the migration process, you can switch the download path to HTTP.

MAP YOUR EXISTING NETWORK CONFIGURATION

Conversion Manager virtual appliance includes features that can reduce the amount of manual networking configuration needed after you convert from your existing VMware ESXi/vCenter VMs to XenServer. For example, the Conversion Manager virtual appliance will:

- Preserve virtual MAC addresses on the VMware ESXi/vCenter VMs and reuse them in the resulting XenServer VMs. Preserving the MAC addresses associated with virtual network adapters (virtual MAC addresses) may:
  - Help preserve IP addresses in environments using DHCP
  - Be useful for software programs whose licensing references the virtual MAC addresses
- Map (virtual) network adapters. Conversion Manager virtual appliance can map VMware networks onto XenServer networks so that after the VMs are converted, their virtual network interfaces are connected accordingly.

  For example, if you map VMware 'Virtual Network 4' to XenServer 'Network 0', any VMware VM that had a virtual adapter connected to 'Virtual Network 4' is connected to 'Network 0' after conversion. Conversion Manager virtual appliance does not convert or migrate any hypervisor network settings. The wizard only alters a converted VM\'s virtual network interface connections based on the mappings provided.

  NOTE:

  You do not need to map all of your VMware networks on to the corresponding XenServer networks. However, if you prefer, you can change the networks the VMs use, reduce, or consolidate the number of networks in your new XenServer configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To gain the maximum benefit from these features, we recommend the following:

- Before installing XenServer, plug the hosts into the networks on the switch (that is, the ports) that you would like to configure on the host.
- Ensure that the XenServer pool can see the networks that you would like to be detected. Specifically, plug the XenServer hosts into switch ports that can access the same networks as the VMware cluster.

Though it is easier to plug the XenServer NICs into the same networks as the NICs on the VMware hosts, it is not required. If you would like to change the NIC/network association, you can plug a XenServer NIC into a different physical network.

PREPARE FOR THE CONVERSION MANAGER VIRTUAL APPLIANCE NETWORKING REQUIREMENTS

When you perform a conversion, you must create a network connection to the network where the VMware server resides. Conversion Manager virtual appliance uses this connection for conversion traffic between the XenServer host and the VMware server.

To create this network connection, you must perform two tasks:

- When you import the Conversion Manager virtual appliance, specify the network you added for conversion traffic as a virtual network interface. You can do so by configuring **interface 1** so it connects to that network.
- Before you run the conversion wizard, add the network connecting VMware and XenServer to the XenServer host where you want to run the converted VMs.

By default, when you import the Conversion Manager virtual appliance, XenCenter® creates one virtual network interface associated with Network 0 and NIC0 (eth0). When adding a network for conversion, select a network other than XenServer's management network to improve performance in busy pools. For more information about the management interface, see Networking.

Inside the Conversion Manager, you might see multiple network interfaces (eth0 and eth1). eth0 attaches to the host's internal network that is used to communicate with the local dom0. eth1 attaches to the routable network that is used to communicate with XenCenter.

To add a network to XenServer:

1. In the **Resource** pane in XenCenter, select the pool where you would like to run Conversion Manager virtual appliance.
2. Click the **Networking** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click **Add Network**.
4. On the **Select Type** page, select **External Network**, and click **Next**.
5. On the **Name** page, enter a meaningful name for the network (for example, \"VMware network\") and a description.
6. On the **Interface** page, specify the following:

   - **NIC**. The NIC that you want XenServer to use to create the network. Select the NIC that is plugged in to the physical or logical network of the VMware server.
   - **VLAN**. If the VMware network is a VLAN, enter the VLAN ID (or \"tag\").
   - **MTU**. If the VMware network uses jumbo frames, enter a value for the Maximum Transmission Unit (MTU) between 1500 and 9216. Otherwise, leave the MTU box at its default value of 1500.

   > **NOTE:**
   >
   > Do not select the **Automatically add this network to new virtual machines** checkbox.

7. Click **Finish**.

Storage requirements

Before you convert batches of VMware ESXi/vCenter VMs, consider your storage requirements.

- If the converted VMs run on a single standalone host (not a pool), you can specify either local or shared storage as the location for the converted virtual disks.
- If you want to run the converted VMs in a pool, their virtual disks must be stored on shared storage. Ensure that you add the shared storage to the pool by creating a storage repository.

  This storage repository must be large enough to contain the virtual disks for all the converted VMs you want to run in that pool.

To create a storage repository:

1. In the **Resource** pane in XenCenter, select the pool where you intend to run the Conversion Manager virtual appliance.
2. Click the **Storage** tab.
3. Click **New SR** and follow the instructions in the wizard. For more instructions, press **F1** to display the online help.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenServer requirements

You can run VMs converted with this release of Conversion Manager on the following versions of XenServer:

- XenServer 8.4
- XenServer 9

VMware requirements

Conversion Manager virtual appliance can convert VMware ESXi/vCenter VMs from the following versions of VMware:

- vCenter Server 7.x, 8.x, and 9.x
- vSphere 7.x, 8.x, and 9.x
- ESXi 7.x, 8.x, and 9.x

NOTE:

Conversion Manager virtual appliance cannot convert VMware ESXi/vCenter Windows VMs with four or more disks into XenServer VMs. Your VMware ESXi/vCenter Windows VMs must have three or fewer disks.

Your VMware ESXi/vCenter VMs must also have a network and a storage controller configured.

Import and configure the virtual appliance

The Conversion Manager virtual appliance is a single pre-installed VM designed to run on a XenServer host.

Download the virtual appliance

The Conversion Manager virtual appliance is packaged in XVA format. You can download the virtual appliance from the XenServer downloads page. When downloading the file, save it to a folder on your local hard drive (typically, but not necessarily, on the computer where XenCenter is installed). After the `.xva` file is on your hard drive, you can import it into XenCenter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Conversion Manager virtual appliance is available for XenServer Premium Edition customers or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement or Citrix DaaS entitlement. For more information about XenServer licensing, see Licensing. To upgrade, or to get a XenServer license, visit the Citrix website.

Import the virtual appliance into XenServer

To import the Conversion Manager virtual appliance into the pool or host where you want to run the converted VMs, use the XenCenter **Import** wizard:

1. Open XenCenter. Right-click on the pool (or host) into which you want to import the virtual appliance package, and select **Import**.
2. Browse to locate the virtual appliance package.
3. Select the pool or a *home server* where you want to run the Conversion Manager virtual appliance.

   NOTE:

   A home server is the host that provides the resources for a VM in a pool. While it can, a XenServer attempts to start the VM on that host, before trying other hosts. If you select a host, the Conversion Manager virtual appliance uses this host as its home server. If you select the pool, the virtual appliance automatically starts on the most suitable host in that pool.

4. Choose a storage repository on which to store the virtual disk for the Conversion Manager virtual appliance and then click **Import**. To add a storage repository to the pool, see the section called "Meet Storage Requirements." You can choose either local or shared storage.
5. Ensure the network to be used for conversion (which connects the VMware server to the XenServer host) is selected as the network associated with **interface 1** ("virtual NIC 1").

   - If the correct network does not appear beside interface 1, use the list in the **Network** column to select a different network.
   - If you have not added the VMware network that is on a different physical network than the pool, do the following:

     a. Exit the wizard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Add the network to the pool.

c. Rerun the wizard.

For more information, see **To add a network to XenServer**.

> **WARNING:**
>
> Do NOT configure NIC0 to your customer network. Assign NIC0 only to \"Host internal management network\."

6. Leave the **Start VM after import** checkbox enabled, and click **Finish** to import the virtual appliance.
7. After importing the `.xva` file, the Conversion Manager virtual appliance appears in the **Resources** pane in XenCenter.

Configure the Conversion Manager virtual appliance

Before you can use the Conversion Manager virtual appliance to convert VMware ESXi/vCenter VMs, configure it using the XenCenter **Console** tab:

1. After importing the Conversion Manager virtual appliance, click the **Console** tab.
2. Read the license agreement. To view the contents of the license agreement, open the URL in a web browser. Press any key to continue.
3. Enter and confirm a new root password for the Conversion Manager virtual appliance. We recommend selecting a strong password.
4. Enter a host name for the Conversion Manager virtual appliance.
5. Enter the domain suffix for the virtual appliance. For example, if the fully qualified domain name (FQDN) for the virtual appliance is `citrix-migrate-vm.domain4.example.com`, enter `domain4.example.com`.
6. Enter **y** to use DHCP to obtain the IP address automatically for the Conversion Manager virtual appliance. Otherwise, enter **n** and then enter a static IP address, subnet mask, and gateway for the VM.
7. Review the host name and network setting and enter **y** when prompted. This step completes the Conversion Manager virtual appliance configuration process.
8. When you have successfully configured the appliance, a login prompt appears. Enter the login credentials and press **Enter** to log in to the Conversion Manager virtual appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you do not configure the Conversion Manager correctly, you might have to reconfigure the virtual appliance. For more information, see Reconfigure the Conversion Manager virtual appliance.

Reconfigure the Conversion Manager virtual appliance

If you need to change the configuration of the Conversion Manager after installing the virtual appliance, you can follow these steps to reconfigure it:

1. Log in to the Conversion Manager virtual appliance by using SSH or the XenCenter **Console** tab as the root user.
2. Delete the following file: `/etc/init.d/vpx_startup_setup_done`.
3. Reboot the virtual appliance by using XenCenter.
4. Reconfigure the virtual appliance by using the XenCenter **Console** tab.

Convert VMware ESXi/vCenter VMs

When you convert VMware ESXi/vCenter VMs, they are imported into the XenServer pool or standalone host where you are running the Conversion Manager virtual appliance. Converted VMs retain their original VMware settings for the virtual processor and virtual memory.

Before you start the conversion procedure, ensure that the following requirements are met:

- You have credentials for the XenServer pool or standalone host. Either the root account or an RBAC (Role-Based Access Control) account with the Pool Admin role is acceptable.
- You have credentials for the VMware server hosting the VMs to be converted. These are needed to connect the Conversion Manager Console to the VMware server.
- The VMware virtual machines to be converted:
  - Are powered off.
  - Have both a network and a storage controller configured.
  - For Windows VMs:
    - Log in to the VMware virtual machine as an administrator.
    - Disable the "Use Admin Approval Mode for the built-in Administrator Account" group policy.
- The XenServer pool (or host) that runs the converted VMs is connected to a storage repository. The storage repository must contain enough space for the converted virtual disks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you want to run your newly converted VMs in a pool, the storage repository must be shared storage. However, if the converted VMs run on a single standalone host (not a pool), you can use local storage.
- Each virtual disk of the VM to convert is within the supported maximum size. On a GFS2 storage repository, a single virtual disk can be up to 16 TiB. On other storage repository types, each virtual disk must be less than 2 TiB.
- The XenServer pool (or host) has networks that the converted VMs use.

To convert your VMware ESXi/vCenter VMs into VMs that can run in a XenServer environment:

1. If the VMware VM is encrypted, decrypt it before starting the conversion. If the VM has a vTPM attached, remove the vTPM before decrypting the VM.
2. Ensure that the virtual appliance is installed and running on the XenServer host or pool where you want to import the VMs.
3. In XenCenter, go to **Pool** > **Conversion Manager**.

   The **Conversion Manager** window opens. Wait while the wizard connects to your virtual appliance.
4. Click **New Conversion**.
5. In the **New Conversion** wizard, enter the credentials for the VMware server:

   - **Server**. Enter the IP address or FQDN for the VMware server that contains the VMs you want to convert to XenServer.
   - **Username**. Enter a valid user name for this VMware server. This account must either be a VMware admin account or have a Root role.
   - **Password**. Enter the password for the user account you specified in the **Username** box.

   Click **Next**. XenCenter connects to the VMware server.
6. On the **Virtual Machines** page, select the VMs you want to convert from the list available on the VMware server.

   The conversion fails if the VM name contains unsupported characters such as `%`, `&`, `*`, `$`, `#`, `@`, `!`, `\`, `/`, `:`, `*`, `?`, `"`, `<`, `>`, `|`, `;`, or `'`. Only uppercase and lowercase ASCII characters, numbers, spaces, periods (`.`), hyphens (`-`), underscores (`_`), plus signs (`+`), and parentheses (`()`) are allowed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If BitLocker is enabled on your VM, or if you are converting a VM with an attached vTPM used by BitLocker, we recommend shutting down BitLocker before conversion. This action decrypts the VM disk and enables the Conversion Manager to automatically uninstall VMware Tools and install XenServer VM Tools on your Windows or Linux VMs.

Click **Next**.

7. If you are converting a Windows VM with an attached vTPM, review the mandatory tasks and information on the **vTPM** page. (This page only appears when converting a Windows VM with an attached vTPM.)

   To proceed with the conversion, you must connect to the vCenter Server. vCenter access is necessary for the Conversion Manager to remove the existing vTPM and create a new XenServer vTPM for the VM.

   NOTE:

   If other applications rely on the vTPM, back up your vTPM data before conversion, as the Conversion Manager cannot recover encrypted data from the old vTPM. A new empty vTPM is created on XenServer. After the conversion, manually restore your data to the new vTPM on XenServer.

   Once you have completed all the mandatory tasks, check the agreement checkbox at the bottom of the page to confirm your completion and then click **Next**.

8. On the **Template** page, select the template to use for each of the selected VMs. By default, the recommended template for the VM is selected. For more information, see Template mappings.

   For Windows VMs, this page also lets you choose whether to receive updates to the I/O drivers (a component of the XenServer VM Tools) through Windows Update. By default, this option is enabled. For Citrix Provisioning targets or reset-on-boot machines, we recommend that you disable this option.

   For Linux VMs, this checkbox is disabled.

9. On the **Storage** page, select the storage repository you want to use during conversion. This storage repository is where the VMs and the virtual disks that you are creating are stored permanently.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This tab indicates the proportion of available storage that the virtual disks of the converted VMs consume.

10. On the **Networking** page, for each VMware network listed, select the XenServer network to map it to. You can also select whether to preserve virtual MAC addresses. Click **Next**.
11. If you are converting Windows VMs, enable the **Install XenServer VM Tools for Windows after conversion** checkbox on the **XenServer VM Tools** page. This allows the Conversion Manager to automatically install XenServer VM Tools on your Windows VMs. (This page only appears for Windows VM conversions.)

    Installing XenServer VM Tools for Windows on each Windows VM is essential for a fully supported configuration. These tools enhance I/O performance, improving disk and network efficiency while supporting key VM features such as clean shutdowns, reboots, suspensions, and live migrations. While VMs can operate without these tools, their performance might be limited. If you enable automatic installation, choose a source:

    - **Use the existing XenServer VM Tools version** - If you have previously downloaded and uploaded XenServer VM Tools for Windows, you can select that version. The version you uploaded is displayed for your reference.
    - **Download and upload the latest version of XenServer VM Tools for Windows** - If internet access is available, XenCenter automatically connects to the XenServer website to download and upload the latest version of the tools to the Conversion Manager.
    - **Select a tools file from disk** - When you need a specific version or lack internet connectivity, you can manually upload the tools file from a local disk.

    Click **Next**.
12. On the **Finish** page, review the options you configured for the conversion process. You can click **Previous** to change these options.

    (Optional) Select **Start the converted VMs automatically after conversion** to power on each VM as soon as its conversion completes successfully. This option requires Conversion Manager 2026.1.0 or later and is disabled by default.

    NOTE:

    If a conversion job fails or does not complete, the converted VM does not start automatically, even when this option is enabled.

    To proceed with the configuration shown, click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The conversion process begins, during which the Conversion Manager automatically uninstalls VMware Tools on your Windows or Linux VMs. When the conversion completes, the converted VMs start automatically if you selected the auto-start option. Otherwise, start your VMs manually from XenCenter by right-clicking the VM and selecting **Start**.

After the VMs boot, XenServer VM Tools install automatically to ensure compatibility. To finalize the installation, manually restart the VM once more.

The **Conversion Manager** window displays conversions in progress and completed conversions.

Post-conversion tasks

After converting your VMs, complete the following tasks on Windows and Linux VMs:

Reactivate the Windows License on Windows VMs

On Windows VMs, depending on your Microsoft licensing model, you might have to reactivate the VM's Windows license. This reactivation happens because the Windows operating system perceives the conversion as a hardware change.

Reboot your Windows VMs

For Windows VMs, if you chose to have the Conversion Manager automatically install XenServer VM Tools, the tools are installed after the initial boot. To finalize the installation, manually restart the VM once more.

Other conversion tasks

The **Manage Conversions** window enables you to perform other tasks related to converting VMs. These tasks include clearing jobs, saving a summary of jobs, retrying jobs, canceling jobs, and displaying the log file.

To clear all jobs:

1. Select **Clear All**.
2. When prompted to confirm this action, click **Yes** to continue.

To save a summary of jobs:

1. Click **Export All**.
2. Specify where to save the CSV file.
3. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To retry a job:

1. Select the job from the list.
2. Click **Retry**.

> **NOTE:**
>
> The **Retry** option is only enabled for failed or canceled jobs.

To cancel a job:

1. Select the job from the list.
2. Click **Cancel**.

> **NOTE:**
>
> Cancel jobs is only enabled for queued or running jobs.

To save the conversion log file for a single job:

1. Select the job from the list.
2. From the logs menu, Click **Fetch Selected Log**.
3. Specify where to save the log file.

To save the conversion log file for all jobs:

1. From the logs menu, Click **Fetch All Logs**.
2. Specify where to save the log file.

To display conversion details:

1. Select the job from the list.

   The information is displayed in the **Details** panel.

Troubleshoot Conversion Manager

This section provides information about troubleshooting the conversion process and converted VMs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Problems starting a converted VM

In general, conversion runs smoothly and Conversion Manager virtual appliance converts VMs without any issues. However, in some rare cases, you might receive errors when attempting to open converted VMs. The following sections provide some guidance on resolving errors and other issues.

Blue screen with Windows STOP code 0x0000007B

This stop code indicates that Conversion Manager virtual appliance was unable to configure a Windows device that is critical to boot in XenServer® for the first time. Save the logs and send them to Support for further guidance.

Windows product activation

Depending on your licensing model, an error message on system activation might appear when you attempt to start a Windows VM.

Lost network settings in a Windows VM

If you import a Windows VM from an ESXi server to XenServer, the IPv4/IPv6 network settings can be lost. To retain the network settings, reconfigure the IPv4/IPv6 settings after completing the conversion.

Unable to start VMware SCSI disk

If a VMware VM boots from a SCSI disk but also has IDE hard disks configured, the VM might not boot when you convert it to XenServer. This issue occurs because the migration process assigns the IDE hard disks lower device numbers than SCSI disks. However, XenServer boots from the hard disk assigned to device 0. To resolve this issue, rearrange the virtual disk position in XenCenter® so that the VM reboots from the virtual disk that contains the operating system.

To change the position of the virtual disk containing the operating system:

1. In the XenCenter **Resources** pane, select the powered off guest VM.
2. Select the **Storage** tab.
3. From the **Virtual Disks** list, select the virtual disk containing the operating system and then click **Properties**.
4. In the virtual disk's **Properties** dialog, click the ***vm_name*** tab to display device options.
5. From the **Device Position** list, select **0** and Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Problems during conversion

If you experience problems or errors when converting VMs, try exporting the VMware VM as an OVF package. If you cannot export the VMware VM as an OVF package, Conversion Manager cannot convert this VM. Use the error messages you receive when attempting to export the VM as an OVF package to troubleshoot and fix the issues with your VMware VM. For example, you might have to configure a network or a storage controller before the VM can be exported as an OVF package or converted. For more information about troubleshooting your VMware ESXi/vCenter VMs, see the VMware documentation.

If you see any errors when converting Linux VMs, remove the converted VM, restart the Conversion Manager virtual appliance and retry.

Logs of failed conversions are stored in the Conversion Manager virtual appliance and can be retrieved by clicking **Fetch All Logs** on the **Conversion Manager** window. When you contact Support to raise any issues, we recommend that you provide the conversion log file and, additionally, a full server status report for troubleshooting. For more information, see Creating a Server Status Report.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitoring System Performance

Monitor system performance with XenCenter®

The **Performance** tab in XenCenter provides real time monitoring of performance statistics across resource pools. This tab also provides graphical trending of virtual and physical machine performance.

- You can view up to 12 months of performance data and zoom in to take a closer look at activity spikes. To learn more, see Viewing performance data.
- By default, graphs showing CPU, memory, network I/O, and disk I/O are displayed on the tab. However, you can add more performance data and change the appearance of the graphs. To learn more, see Configuring performance graphs
- Performance alerts can be generated when the following resources go over a specified threshold on a managed server, virtual machine, or storage repository:
  - CPU
  - Memory usage
  - Network
  - Storage throughput
  - VM disk activity

  For more information, see Configuring performance alerts.

NOTE:

Full performance data is only available for virtual machines with XenServer® VM Tools installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitor system performance with NRPE

NOTE:

The NRPE feature is available for XenServer Premium or Trial Edition customers. For more information about XenServer licensing, see Licensing. To upgrade, or to get a XenServer license, visit the XenServer website.

The **NRPE Configuration** tab on the **Properties** dialog allows you to configure NRPE for your XenServer hosts and pools, allowing you to use any third-party monitoring tool that supports the Nagios Remote Plugin Executor (NRPE) to monitor resources consumed by your hosts/pools and dom0 - the control domain of your host. For information on how to configure NRPE, see Monitoring host and dom0 resources with NRPE.

Monitor system performance with SNMP

NOTE:

The SNMP feature is available for XenServer Premium or Trial Edition customers. For more information about XenServer licensing, see Licensing. To upgrade, or to get a XenServer license, visit the XenServer website.

The **SNMP** tab on the **Properties** dialog allows you to configure SNMP for your XenServer hosts and pools, allowing you to use any third-party monitoring tool that supports the Simple Network Management Protocol (SNMP) to monitor resources consumed by your hosts/pools and dom0 - the control domain of your host. For information on how to configure SNMP, see Monitoring host and dom0 resources with SNMP.

Related documentation

XenServer Current Release

- Monitor host and dom0 resources with NRPE
- Monitor host and dom0 resources with SNMP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Viewing Performance Data

The **Performance** tab shows performance data for the selected server or virtual machine in graph form.

For servers you can view:

- CPU, memory, and network I/O usage data.
- You can add graphs showing extra resource usage data, if necessary. For example, you can include the Control Domain Load. This load is the average (Linux `loadavg`) of the number of processes queued inside the control domain over the last 5 minutes.
- Lifecycle events for all the VMs hosted on the server are shown in the **VM Lifecycle Events** pane.

For VMs, graphs showing CPU, memory, network I/O, and disk usage data are shown by default.

At the bottom of the tab, the summary graph gives a quick overview of what is happening on the machine. This graph also allows you to adjust the time frame that is shown in the other graphs. The time frame can be changed either to show data from a longer or shorter period, or to show data from an earlier period.

To include other types of performance data on the tab or to change the appearance of the graphs, see Configuring performance graphs.

To view data from a longer or shorter time period

By default, data from the last 10 minutes is displayed. To view data from a longer or shorter time period, do one of the following:

- To view available performance data for the last hour, 24 hours, week, month, or year, click **Zoom**. Select **1 Hour**, **1 Day**, **1 Week**, **1 Month**, or **1 Year**.
- To resize the time period that is displayed in the graphs, in the summary graph, point to the vertical split bar at the edge of the sample area. When the pointer changes to a double-headed arrow, drag the vertical split bar right or left.

  For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

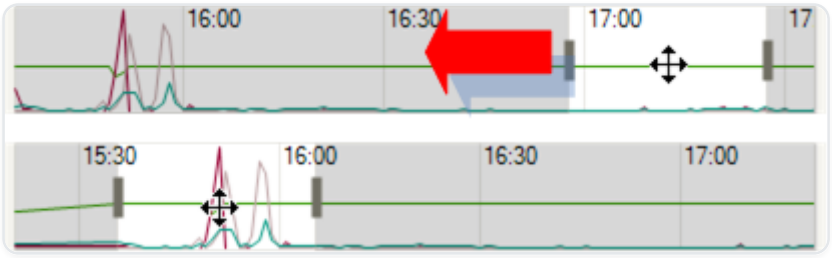


To view data from a different time period

To move the time frame for data displayed in the graphs, point to any graph. When the pointer changes to a move cursor, drag the graph or the sample area in the summary graph to the left or right.



For example:



To view VM lifecycle event data on a server

To view lifecycle events for the VMs hosted on a server, use the **VM Lifecycle Events** list.

- Each event has a tooltip with the full message for that lifecycle event ("Virtual Machine 'Sierra' has been started").
- You can use the cursor keys to navigate the items in the list.
- Double clicking or pressing **Enter** zooms the graphs to the point when the selected lifecycle event occurred.
- Selecting (single click or highlight with cursor keys) one of the events causes the lifecycle event on the graph itself to be highlighted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring Performance Graphs

To add a graph

1. On the **Performance** tab, select **Actions** and then **New Graph**. The **New Graph** dialog box is displayed.
2. Enter a name for the graph in the **Name** field.
3. From the list of datasources, check the check boxes for the datasources you want to include in the graph.
4. Click **Save**.

To edit a graph

1. Navigate to the **Performance** tab and select the graph that you would like to edit.
2. Select **Actions** and then **Edit Graph**.
3. On the graph details window, make the necessary changes and click **OK**.

To delete a graph

1. Select the graph to remove from the list of graphs displayed on the **Performance** tab.
2. Select **Actions** and then **Delete Graph**.
3. Click **Yes** to confirm the deletion.

To reorder a graph

1. Navigate to the **Performance** tab and select the graph that you would like to reorder.
2. Select the **Move Up** or **Move Down** tab to move the graph from its current location.

To change datasource color in graphs

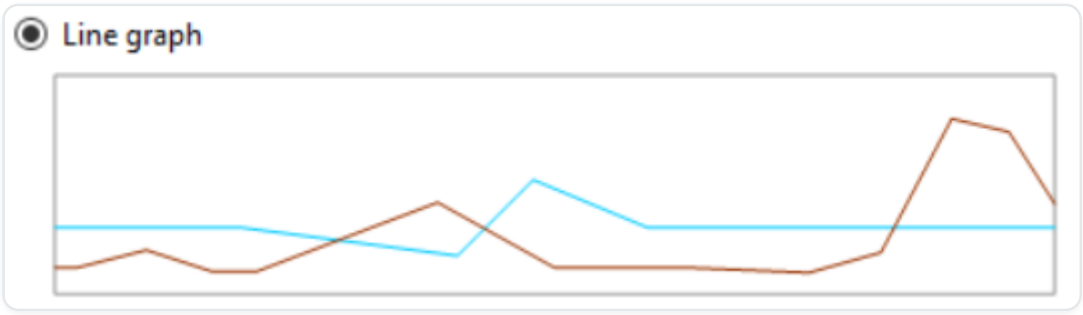
1. Navigate to the **Performance** tab.
2. Double-click on the graph for which you want to change the color of the datasource. The graph details dialog box is displayed.
3. Check the colored check box located against the required datasource and choose a new color from the color picker.
4. Click **OK** to confirm.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

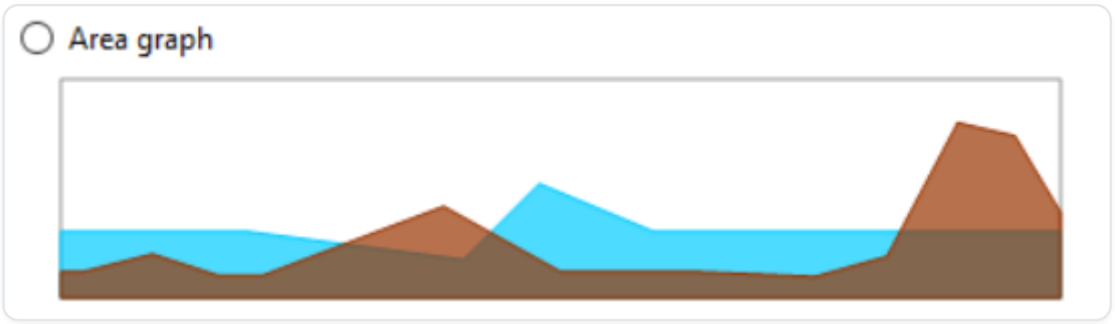
To Change the graph type

Data on the performance graphs can be displayed as lines or as areas:

Line Graph:



Area Graph:



To change the graph type:

1. On the **Tools** menu, select **Options** and then select the **Graphs** tab.
2. To view performance data as a line graph, choose the **Line graph** radio button.
3. To view performance data as an area graph, choose the **Area graph** radio button.
4. Click **OK** to save your changes.

NUMA optimization in XenCenter

Overview

XenCenter shows NUMA optimization status for virtual machines (VMs) on XenServer 9 hosts. Use XenCenter to verify placement and to visualize NUMA-related metrics after you enable them.

Where to view NUMA status

- VM **General** tab: Shows whether the VM is NUMA-optimized.
- VM **Performance** tab: Shows per-VM RRD data sources for NUMA and scheduling after you enable them.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Indicators

- `NUMA nodes = 1`: The VM is optimized and uses a single NUMA node.
- `NUMA nodes > 1`: The VM memory is spread across multiple NUMA nodes. The VM is not optimized.

Enable metrics

Per-VM NUMA-related metrics are disabled by default. To enable them:

1. Select the VM in the **Resources** pane.
2. On the **Performance** tab, select **Actions** > **New graph...**
3. Click **Show data sources** > **Disabled** to include disabled data sources in the list.
4. From the list of data sources select the check boxes of the data sources you want to enable such as "NUMA nodes", "vCPUs runnable any" and so on.
5. Click **Enable** to enable the recording of the selected metrics on the server.
6. Click **Save** to create the new graph with the selected datasources.

Guidance and considerations

Performance gains from NUMA optimization depend on:

- Workload and application profile in the VM.
- Benchmark or metric used to measure latency and throughput.
- CPU architecture and generation.

If your use case requires strict single-node placement and the VM cannot fit on one NUMA node, resize the VM memory to fit within a single node or adjust host memory allocation to make a single-node placement possible.

Monitoring host and dom0 resources with NRPE

NOTE:

The NRPE feature is available for XenServer Premium or Trial Edition customers. For more information about XenServer licensing, see Licensing. To upgrade, or to get a XenServer license, visit the XenServer website.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Users with the Pool Admin role can use any third-party monitoring tool that supports the Nagios Remote Plugin Executor (NRPE) to monitor resources consumed by your XenServer® host and dom0 - the control domain of your host.

You can use the following check plugins to monitor host and dom0 resources:

METRIC	NRPE CHECK NAME	DESCRIPTION	DEFAULT WARNING THRESHOLD	DEFAULT CRITICAL THRESHOLD	PERFORMANCE DATA RETURNED
Host CPU Load	check_host_load	Gets and checks the current load per physical CPU of the host, where load refers to the number of vCPU(s) in a running or runnable state.	3	4	Current system load of the CPU of the host (calculated by taking the average load of the physical CPU of the host).
Host CPU Usage (%)	check_host_cpu	Gets and checks the current average overall CPU usage of the host.	80%	90%	The percentage of host CPU that is currently free and the percentage that is in use.
Host Memory Usage (%)	check_host_memory	Gets and checks the current memory usage of the host.	80%	90%	The percentage of host memory that is currently free and the percentage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIC	NRPE CHECK NAME	DESCRIPTION	DEFAULT WARNING THRESHOLD	DEFAULT CRITICAL THRESHOLD	PERFORMANCE DATA RETURNED
					that is in use.
Host vGPU Usage (%)	check_vgpu	Gets and checks all the current running Nvidia vGPU usage of the host.	80%	90%	The percentage of running vGPU that is currently free and the percentage that is in use.
Host vGPU Memory Usage (%)	check_vgpu_memory	Gets and checks all the current running Nvidia vGPU memory usage (including the shared memory and graphic memory) of the host.	80%	90%	The percentage of running vGPU memory (including the shared memory and graphic memory) that is currently free and the percentage that is in use.
Dom0 CPU Load	check_load	Gets and checks the current system load average per CPU of dom0, where load refers to the	2.7,2.6,2.5	3.2,3.1,3	Host CPU load data calculated by taking the average of the last 1, 5, and 15 minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIC	NRPE CHECK NAME	DESCRIPTION	DEFAULT WARNING THRESHOLD	DEFAULT CRITICAL THRESHOLD	PERFORMANCE DATA RETURNED
		number of processes in a running or runnable state.			
Dom0 CPU Usage (%)	check_cpu	Gets and checks the current average overall CPU usage of dom0.	80%	90%	The average overall CPU usage of dom0 as a percentage.
Dom0 Memory Usage (%)	check_memory	Gets and checks the current memory usage of dom0.	80%	90%	The percentage of dom0 memory that is currently free and the percentage that is in use.
Dom0 Free Swap (%)	check_swap	Gets and checks the current swap usage of dom0.	20%	10%	The percentage of MB on dom0 that is currently free.
Dom0 Root Partition Free Space (%)	check_disk_root	Gets and checks the current root partition usage of dom0.	20%	10%	The percentage of MB on the dom0 root partition that is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIC	NRPE CHECK NAME	DESCRIPTION	DEFAULT WARNING THRESHOLD	DEFAULT CRITICAL THRESHOLD	PERFORMANCE DATA RETURNED
					currently free.
Dom0 Log Partition Free Space (%)	check_disk_log	Gets and checks the current log partition usage of dom0.	20%	10%	The percentage of MB on the dom0 log partition that is currently free.
Toolstack Status	check_xapi	Gets and checks the status of the XenServer management toolstack (also known as XAPI).			XAPI elapsed uptime in seconds.
Multipath Status	check_multipath	Gets and checks the status of the storage paths.			The status of the storage paths. `OK` indicates that all paths are active, `WARNING` indicates that some paths have failed but more than one path is active, `CRITICAL` indicates

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIC	NRPE CHECK NAME	DESCRIPTION	DEFAULT WARNING THRESHOLD	DEFAULT CRITICAL THRESHOLD	PERFORMANCE DATA RETURNED
					that there is only one path active or that all paths have failed, `UNKNOWN` indicates that host multipathing is disabled and that the status of the paths cannot be fetched.

NRPE is an on-premises service that runs in dom0 and listens on TCP port (default) 5666 for check execution requests from a monitoring tool. After a request arrives, NRPE parses it, finds the corresponding check command including the parameter's details from the configuration file, and then runs it. The result of the check is sent to the monitoring tool, which stores the results of past checks and provides a graph showing the historical performance data.

Prerequisites

To be able to use NRPE to monitor host and dom0 resources, the monitoring tool you are using must meet the following prerequisites:

- The monitoring tool must be compatible with NRPE version 4.1.0.
- To allow communication between NRPE and the monitoring tool, the monitoring tool must support TLS 1.2 with ciphers `ECDHE-RSA-AES256-GCM-SHA384` and `ECDHE-RSA-AES128-GCM-SHA256`, and the EC curve is `secp384r1`.

Constraints

- You can configure NRPE settings for an entire pool or for a standalone host that is not part of a pool. Currently, you cannot configure NRPE settings for an individual host in a pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you add a host to a pool that already has NRPE enabled and configured on it, XenCenter® does not automatically apply the pool's NRPE settings to the new host. You must reconfigure NRPE settings on the pool after adding the new host or configure the new host with same NRPE settings before adding it to the pool.

  NOTE:

  When reconfiguring NRPE settings on a pool after adding a new host, ensure the host is up and running.

- If a host is removed from a pool with NRPE enabled and configured on it, XenCenter does not alter the NRPE settings on the host or the pool.

Configure NRPE by using XenCenter

You can configure NRPE by using XenCenter or the xe CLI. For more information on how to configure NRPE by using the xe CLI, see Configure NRPE by using the xe CLI.

To configure NRPE for a standalone host or for an entire pool, go to the **NRPE Configuration** tab on the **Properties** dialog for your host/pool and follow these steps:

NOTE:

When configuring NRPE for a pool, the **NRPE Configuration** tab displays the default NRPE configuration values for the entire pool.

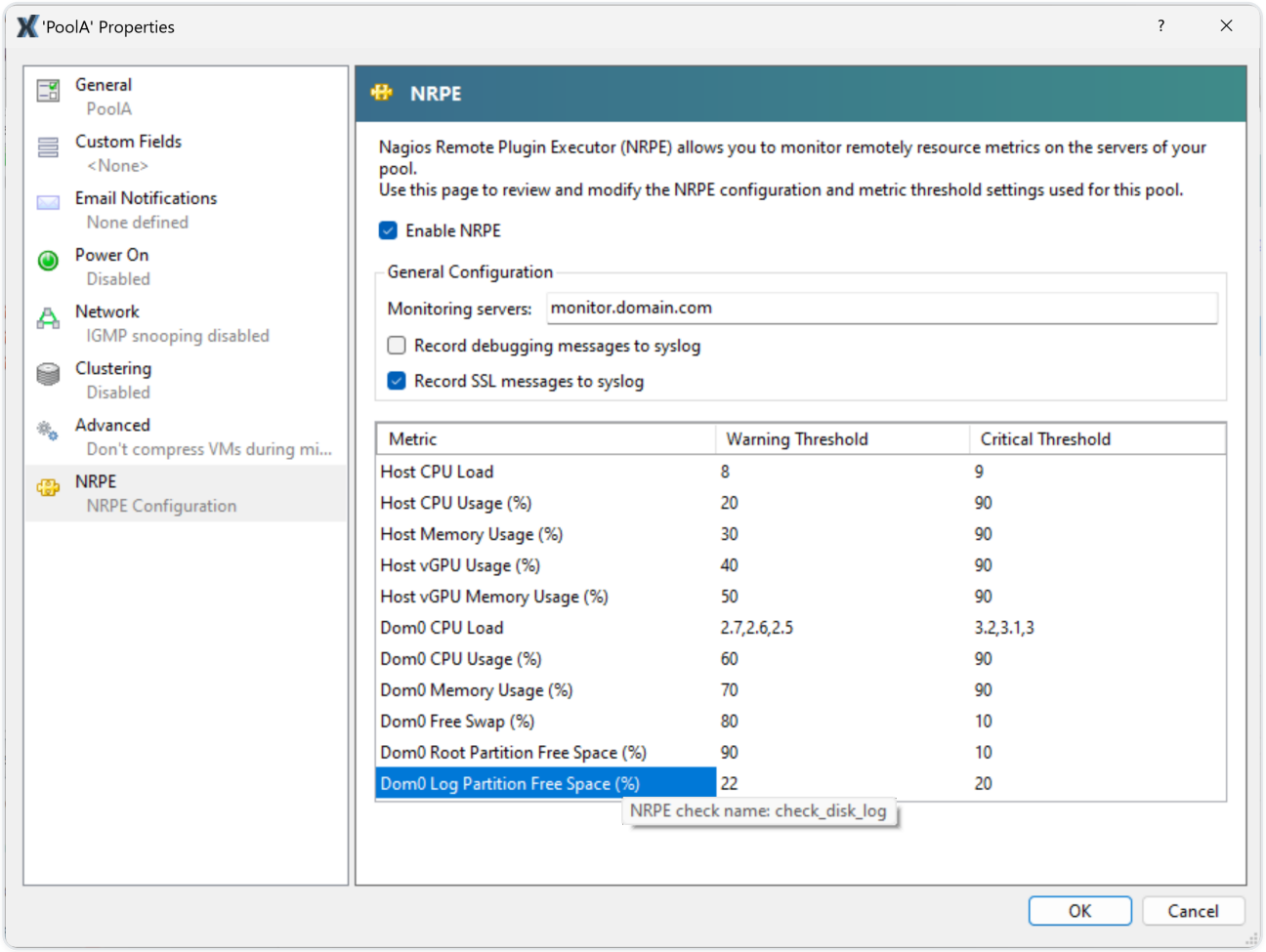
1. In the **Infrastructure** view, choose the host/pool that you want to configure NRPE settings for.
2. In the **General** tab, click **Properties**.
3. In the **Properties** dialog, select the **NRPE** tab.
4. Select the **Enable NRPE** check box.
5. To add more monitoring servers that are allowed to talk to the NRPE daemon, specify the hosts as a comma-delimited list of IP addresses or host names. They can be specified in the following formats:

   - IP address (only supports IPv4)
   - Classless Inter-Domain Routing (CIDR) (format: `xxx.xxx.xxx.xxx/n`, for example, `192.168.1.0/24`)
   - Host name

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. To enable debug logging, select the **Record debugging messages to syslog** check box.
7. To enable SSL logging, select the **Record SSL message to syslog** check box.
8. (Optional) Adjust the warning and critical thresholds by modifying the values in the warning and critical thresholds table.

   For some check plugins, you can set warning and critical threshold values so that if the value returned by a check plugin exceeds the threshold values, an alert is generated. The warning threshold indicates a potential issue and the critical threshold indicates a more serious issue that requires immediate attention. Although default values are set for the warning and critical thresholds, you can adjust the threshold values.
9. Click **OK** to apply any configuration changes to your host/pool.



Related documentation

XenServer Current Release

- Monitor host and dom0 resources with NRPE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitoring host and dom0 resources with SNMP

NOTE:

The SNMP feature is available for XenServer Premium or Trial Edition customers. For more information about XenServer licensing, see Licensing. To upgrade, or to get a XenServer license, visit the XenServer website.

With the Pool Admin role, you can use SNMP to remotely monitor resources consumed by your XenServer® host and dom0 - the control domain of your host. An SNMP manager, also known as a network management system (NMS), sends query requests to an SNMP agent running on a XenServer host. The SNMP agent replies to these query requests by sending data collected on various metrics back to the NMS. The data that can be collected is defined by object identifiers (OIDs) in a text file called a management information base (MIB). An OID represents a specific piece of measurable information about a network device, such as CPU or memory usage.

You can also configure traps, which are agent-initiated messages that alert the NMS that a specific event has occurred in XenServer. Both query requests and traps can be used to monitor the status of your XenServer pools. These are defined as metric and trap objects and are identified by OIDs in a MIB file `XENSERVER-MIB.txt`, available to download from the XenServer Downloads page. The following tables provide information about these metric and trap objects.

Metric objects

You can request a specific piece of information about your XenServer hosts by using the metrics listed in the following table. These metrics are used by the SNMP manager when sending query requests to an SNMP agent and so you can view this data in your NMS.

You can view the returned data from these metric objects from your NMS or from the xe CLI. To query the metric objects from the xe CLI, run `host-data-source-query` or `vm-data-source-query` and provide the RRDD data source as a value for the `data-source` parameter. For example:

```
xe host-data-source-query data-source=cpu_avg host=<host UUID>
```

NOTE:

By default, the NMS sends OID query requests to SNMP agents using port 161.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OBJECT IDENTIFIER (OID)	RRDD DATA SOURCE	RETURNED DATA	TYPE
1.3.6.1.4.1.60953.1.1.1.1	`memory`	Dom0 total memory in MB	Unsigned32
1.3.6.1.4.1.60953.1.1.1.2	`memory_internal_free`	Dom0 free memory in MB	Unsigned32
1.3.6.1.4.1.60953.1.1.1.3	`cpu_usage`	Dom0 CPU usage as a percentage	Float
1.3.6.1.4.1.60953.1.1.1.4	`memory_total_kib`	Host total memory in MB	Unsigned32
1.3.6.1.4.1.60953.1.1.1.5	`memory_free_kib`	Host free memory in MB	Unsigned32
1.3.6.1.4.1.60953.1.1.1.6	`cpu_avg`	Host CPU usage as a percentage	Float
1.3.6.1.4.1.60953.1.1.1.7	(see note 1)	pCPUs number	Unsigned32
1.3.6.1.4.1.60953.1.1.1.8	`running_vcpus`	Running vCPUs number	Unsigned32
1.3.6.1.4.1.60953.1.1.1.9	`running_domains`	Running VMs number	Unsigned32

NOTES:

1. The name of a pCPU is in the format `cpu` followed by a number. To query the number of pCPUs from the xe CLI, run the following command:

   ```
   xe host-data-source-list host=<host UUID> | grep -E 'cpu[0-9]+$'
   ```

   This returns a list of the CPU metrics that match the regular expression `cpu[0-9]+`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Traps

Traps are alerts sent by the SNMP agent to notify the SNMP manager when certain events occur, allowing you to monitor your XenServer hosts and identify issues early. You can configure your SNMP settings to generate a trap when a limit is reached (for example, if the host CPU usage is too high). When a trap is generated, it is sent to your NMS and the following fields are returned as part of the trap object.

NOTE:

By default, the SNMP agent on the pool coordinator host sends traps to the NMS using UDP port 162.

OBJECT IDENTIFIER (OID)	FIELD NAME	TYPE	DESCRIPTION
1.3.6.1.4.1.60953.1.1 0.1.1	`operation`	String	Can be one of the following values: `add` or `del`. `operation` is `add` if a trap is generated by XenServer and sent to your NMS (an alert is also created in XenCenter) or `del` if an alert is destroyed (for example, if you dismiss an alert).
1.3.6.1.4.1.60953.1.1 0.1.2	`ref`	String	The reference for the trap object.
1.3.6.1.4.1.60953.1.1 0.1.3	`uuid`	String	The UUID of the trap object.
1.3.6.1.4.1.60953.1.1 0.1.4	`name`	String	The name of the trap object.
1.3.6.1.4.1.60953.1.1 0.1.5	`priority`	Integer	The severity of the trap. Can be one of the following values:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OBJECT IDENTIFIER (OID)	FIELD NAME	TYPE	DESCRIPTION
			`1`: Critical, `2`: Major, `3`: Warning, `4`: Minor, `5`: Information, `others`: Unknown.
1.3.6.1.4.1.60953.1.10.1.6	`class`	String	The category of the trap generated. Can be one of the following values: `VM`, `Host`, `SR`, `Pool`, `VMPP`, `VMSS`, `PVS_proxy`, `VDI`, or `Certificate`.
1.3.6.1.4.1.60953.1.10.1.7	`obj-uuid`	String	The xapi object UUID of the various classes of the field `class`.
1.3.6.1.4.1.60953.1.10.1.8	`timestamp`	String	The time at which the trap is generated.
1.3.6.1.4.1.60953.1.10.1.9	`body`	String	Detailed information about the field `name`.

Prerequisites

- All hosts in a pool must be running the same XenServer version and this version must contain the SNMP plugin.

> **NOTE:**
>
> If you cannot see the **SNMP** tab in XenCenter®, it might be because the host or a member of the pool is not running a version of XenServer that supports SNMP. Update the host or pool to the latest version of XenServer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The NMS you are using must support SNMPv2c or SNMPv3.
- Your NMS and XenServer must be network-connected.

Constraints

- You can configure SNMP settings for an entire pool or for a standalone host that is not part of a pool. Currently, you cannot configure SNMP settings for an individual host in a pool.
- If you add a host to a pool that already has SNMP enabled and configured on it, XenCenter does not automatically apply the pool's SNMP settings to the new host. You must reconfigure SNMP settings on the pool after adding the new host or configure the new host with the same SNMP settings before adding it to the pool.

  NOTE:

  When reconfiguring SNMP settings on a pool after adding a new host, ensure the host is up and running and not in maintenance mode.

- If a host is removed from a pool with SNMP enabled and configured on it, XenCenter does not alter the SNMP settings on the host or the pool.
- Before performing a rolling pool upgrade or applying updates to your XenServer hosts and pools, back up the following configuration files if you manually modified them before and need them:
  - `/etc/snmp/snmpd.xs.conf`
  - `/etc/sysconfig/snmp`
  - `/var/lib/net-snmp/snmpd.conf`
- When the SNMP agent is offline, traps cannot be generated. For example, if the SNMP agent is restarted or the pool coordinator is rebooted or re-designated.

Configure SNMP by using XenCenter

You can configure SNMP for a standalone host or for an entire pool by using XenCenter or the xe CLI. For more information on how to configure SNMP by using the xe CLI, see Configure SNMP by using the xe CLI.

1. Download the `XENSERVER-MIB.txt` file from the XenServer Downloads page and import it into your preferred NMS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. In XenCenter, in the **Infrastructure** view, choose the host/pool that you want to configure SNMP settings for.
3. In the **General** tab, click **Properties**.
4. In the **Properties** dialog, select the **SNMP** tab.

   NOTE:

   When configuring SNMP for a pool, the **SNMP** tab displays the default SNMP configuration values for the entire pool. If you cannot see the **SNMP** tab in XenCenter, might be because the host or a member of the pool is not running a version of XenServer that supports SNMP. Update the host or pool to the latest version of XenServer.

5. Select the **Enable SNMP** check box to enable SNMP.
6. (Optional) Select the **Support SNMPv3** check box to enable XenServer to use SNMPv3 in addition to SNMPv2c. By default, XenServer uses SNMPv2c.
7. (Optional) To enable debug logging, select the **Record debugging messages to syslog** check box.
8. Click **OK** to apply configuration changes to your host or pool.
9. Configure your NMS by referring to your NMS documentation. Make sure that you specify the XenServer SNMP agent address (this is the IP address of the XenServer host or pool that you are monitoring).
10. (Optional) To configure a trap receiver and begin receiving alerts for when a specific event has occurred in XenServer:

    - In your NMS, configure a trap receiver by referring to your NMS documentation.
    - On the **SNMP** tab, click **Add Trap Receiver** and specify the **NMS Address**, **NMS Port**, and the parameters of the SNMP version of the NMS supported.
    - To test the configuration, click **Send Test Trap** to send a test trap to your NMS.
    - To delete a trap receiver, click **Delete Trap Receiver**.
    - Click **OK** to apply your configuration changes.

Related documentation

XenServer Current Release

- Monitor host and dom0 resources with SNMP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring Performance Alerts

Performance alerts can be generated when CPU, memory usage, network, storage throughput, or VM disk activity exceeds a specified threshold on a server, VM, or storage repository (SR). By default, the alert repeat interval is set to 60 minutes, and it can be modified if necessary.

Performance alerts appear in the **Alerts** view (accessed by clicking the **Notifications** button on the left hand pane). You can have performance alerts emailed to you. You can also enable an SNMP trap to be sent to your SNMP manager, also known as a network management system (NMS). For more information, see XenCenter Alerts.

You can configure performance alerts for servers, VMs, or SRs. To configure performance alerts:

1. Select the server, VM, or SR in the **Resources** pane. Select the **General** tab and then click **Properties**.
2. Select the **Alerts** tab. The following table summarizes which alerts are available for servers, VMs, or SRs:

ALERT NAME	SERVER	VM	SR	DESCRIPTION
Generate CPU usage alerts	X	X		Set the CPU usage and time threshold that trigger the alert.
Generate control domain CPU usage alerts	X			Set the control domain CPU usage and time threshold that trigger the alert.
Generate memory usage alerts	X			Set the memory usage and time threshold that trigger the alert.
Generate control domain	X			Set the control domain

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ALERT NAME	SERVER	VM	SR	DESCRIPTION
memory usage alerts				memory usage and time threshold that trigger the alert.
Generate control domain free memory alerts	X			Set the control domain free memory and time threshold that trigger the alert.
Generate disk usage alerts		X		Set the disk usage and time threshold trigger the alert.
Generate storage throughput alerts			X	Set the storage throughput and time threshold that trigger the alert. Note: Physical Block Devices (PBD) represent the interface between a specific XenServer server and an attached SR. When the total read/write SR throughput activity on a PBD exceeds the threshold you have specified,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ALERT NAME	SERVER	VM	SR	DESCRIPTION
				alerts are generated on the server connected to the PBD. Unlike other XenServer server alerts, this alert must be configured on the SR.
Generate network usage alerts	X	X		Set the network usage and time threshold that trigger the alert.

To change the alert repeat interval, enter the number of minutes in the **Alert repeat interval** box. After an alert threshold is reached and an alert generated, another alert is not generated until after the alert repeat interval has elapsed.

3. Click **OK** to save your changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Updates and Upgrades

XenCenter can automatically check for new XenCenter updates at regular intervals and notify you when a new product version is available. It is recommended that you install all published updates.

Update your version of XenCenter®

The most up-to-date version of XenCenter is supplied on the XenServer product downloads page. Use this file to update your XenCenter installation. For more information, see Update XenCenter.

Upgrade your hosts

To upgrade your hosts, use the **Rolling Pool Upgrade** wizard. You can use this wizard to upgrade multiple servers in a pool with minimal service interruption for running VMs. VMs are automatically migrated onto other available servers as the upgrade is applied to each server in turn. The wizard can also be used to upgrade standalone servers. See Upgrade your hosts.

Update XenServer® hosts

XenServer introduces a faster, more efficient release process designed to deliver updates faster than ever. New features, bug fixes, and performance improvements are frequently pushed to the content delivery network (CDN) as available updates for your XenServer hosts and pools. Each set of updates is cumulative, meaning they include the latest features and fixes along with all prior updates, ensuring your environment remains optimized with minimal effort.

Updates can be applied to your XenServer hosts and pools through the following methods:

- **Updates from the CDN**: Requires internet access to automatically download and apply updates from the CDN.
- **Offline Updates**: Designed for air-gapped environments, allowing you to manually download and apply updates without internet access.
- **Updates from an existing pool**: This method enables you to bring a standalone host or a pool up to the same level of updates as another pool that is at a higher level of updates. It is recommended for joining a newly installed host to a pool that is not at the latest level of updates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For advanced automation, you can also use the XenServer PowerShell module to script the upload and application of update bundles. For more information, see Update your XenServer hosts by using the XenServer PowerShell module.

To configure and apply updates for your XenServer hosts and pools, see Update your hosts.

Related documentation

XenServer Current Release

- Update your XenServer hosts
- Upgrade from Citrix Hypervisor 8.2 Cumulative Update 1

Upgrade your hosts

You can use the **Rolling Pool Upgrade** wizard to upgrade XenServer® standalone servers or a pool of servers to a newer version.

The Rolling Pool Upgrade wizard guides you through the upgrade procedure and organizes the upgrade path automatically. The Rolling Pool Upgrade wizard allows you to upgrade multiple servers and pools simultaneously. Each of the servers in the pool is upgraded in turn, starting with the pool coordinator. Before starting an upgrade, the wizard conducts pre-checks to ensure that certain pool-wide features, such as high availability and WLB, are temporarily disabled. The wizard also checks that each host in the pool is prepared for upgrade. Only one server is offline at a time, and any running VMs are automatically migrated off each server before the upgrade is installed on that server.

NOTE:

Rolling Pool Upgrade is available for licensed XenServer customers. For more information, see About XenServer Licensing.

The wizard can operate in manual or automatic mode:

- In manual mode, you must manually run the XenServer installer on each server in turn and follow the on-screen instructions on the serial console of the server. When the upgrade begins, XenCenter® prompts you to insert XenServer installation media or specify a PXE boot server for each server that you upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In automatic mode, the wizard uses network installation files on an HTTP, NFS, or FTP server to upgrade each server in turn. This mode does not require you to insert install media, manually reboot, or step through the installer on each server.

  If you perform a rolling pool upgrade in this manner, unpack the XenServer installation media onto your HTTP, NFS, or FTP server before starting the upgrade. You can do this by mounting the ISO and copying its contents to the network location. For more information, see Host your installation media on NFS, FTP, or HTTP.

Important: Before you upgrade

Upgrading a pool of servers requires careful planning. As you plan your upgrade, it is important to be aware of the following:

- Ensure your XenCenter client is up to date.
- If you are using XenServer to host Citrix Virtual Apps and Desktops workloads, there might be specific behaviors and requirements to consider that can optimize your XenServer upgrade process. For more information, see Upgrade scenarios for Citrix Virtual Apps and Desktops.
- XenServer is now an entitlement of the Citrix for Private Cloud, Citrix Universal Hybrid Multi-Cloud, Citrix Universal MSP, and Citrix Platform License subscriptions. Read more. For information about getting a license, see the XenServer website.
- VMs can only be migrated from a server that runs an older version of XenServer to one that runs the same version or higher. You cannot migrate VMs from an upgraded server to one running an older version of XenServer. Ensure to allow for space on your servers accordingly.
- We strongly advise against running a mixed-mode pool (one with multiple versions of XenServer coexisting) for longer than necessary. In this case, the pool operates in a degraded state during upgrade.
- Ensure that all hosts in your pool are synchronized to the correct date and time (for example, by using NTP).
- Do not attempt to perform any key control operations during the upgrade process. Though VMs continue to function as normal, VM actions other than migrate might not be available (for example, shut down, copy, and export). In particular, it is not safe to perform storage-related operations such as adding, removing, or resizing virtual disks.
- The wizard upgrades the pool coordinator first. Do not place the pool coordinator into maintenance mode using XenCenter before performing the upgrade as this action causes a new pool coordinator to be designated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Take a backup of the state of your existing pool using the `pool-dump-database` xe CLI command. For more information, see Command line interface. Backups allow you to revert a partially complete rolling upgrade back to its original state without losing any VM data. As it is not possible to migrate a VM from an upgraded server to a server running an older version, you might have to shut down VMs to revert the rolling upgrade for any reason.
- Ensure that your servers are not over-provisioned - that is, they have sufficient memory to carry out the upgrade. It is best to suspend any VMs that are not critical during the upgrade process.
- While the **Rolling Pool Upgrade** wizard checks that the following actions have been taken, you might choose to perform them before you begin the upgrade:
  - Empty the CD/DVD drives of the VMs in the pool. For details and instructions, see Upgrade.
  - Disable high availability.
  - Disable WLB

To upgrade XenServer using the Rolling Pool Upgrade wizard

1. Open the Rolling Pool Upgrade wizard: on the **Tools** menu, select **Rolling Pool Upgrade**.
2. Read the Before You Start information, and then select **Next** to continue.
3. Select the pool or standalone servers that you would like to upgrade and then select **Next**.
4. Choose the **Upgrade Mode**.
   - You can select **Automatic Mode** for an automated upgrade from network installation files on an HTTP, NFS, or FTP server. Unpack the XenServer installation media onto your HTTP, NFS, or FTP server before starting the upgrade. For more information, see Host your installation media on NFS, FTP, or HTTP.

     If you choose the **Automatic Mode**, specify the location of the network installation files, user name, and password before continuing to the next step.
   - You can select **Manual Mode** for a manual upgrade from either an ISO or a server using PXE boot. For more information about using PXE boot, see Configure your TFTP and DHCP servers.

     If you choose the **Manual Mode**, run the XenServer installer on each server in turn and follow the on-screen instructions on the serial console of the server. When the upgrade begins, XenCenter prompts you to insert XenServer installation media or specify a PXE boot server for each server that you upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. On the **Upgrade Options** page, choose whether you want XenCenter to automatically download and install the minimal set of updates after upgrading the servers to a newer version. The apply updates option is selected by default. However, you must have an internet connection to download and install the updates.

   In addition, to allow XenCenter to install a previously downloaded update or a supplemental pack after upgrading the servers, select **Install an update or supplemental pack from disk**. Select **Browse** to choose the file. Selecting a file incompatible with the upgraded version of XenServer can cause the installation to fail.

6. After choosing the Upgrade Options, select **Run Pre-checks**.

   NOTE:

   A new pre-check identifies hosts with drivers that have multiple variants. If multiple variants are found, XenCenter displays a warning for the host.

   Select **Select variant** to open a dialog that lists driver variants for the host that are applicable to the current hardware. You can change the variant by choosing a different option from the drop-down list. The new variant becomes active after the rolling pool upgrade completes and the host reboots.

7. Follow the on-screen recommendations to resolve any upgrade pre-checks that have failed. To allow XenCenter to automatically resolve all failed pre-checks, select **Resolve All**.

8. When the pre-checks have been resolved, select **Start Upgrade** to begin the upgrade.

When the upgrade begins, the wizard guides you through any actions you need to take to upgrade each server. Follow the instructions until you have upgraded and updated all servers in the pool.

NOTE:

If the upgrade process fails for any reason, the Rolling Pool Upgrade wizard halts the process. This halt allows you to fix the issue and resume the upgrade process by clicking the **Retry** button.

The Rolling Pool Upgrade wizard prints a summary when the upgrade is complete. Select **Finish** to close the wizard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- Upgrade from Citrix Hypervisor 8.2 Cumulative Update 1

Update your XenServer® hosts

With XenServer, new features and bug fixes are frequently pushed to the content delivery network (CDN) as available updates for your XenServer hosts and pools, allowing you to benefit from a more efficient release process that delivers new content to you at a faster cadence than was previously possible.

To ensure that you are always on the latest and greatest update, there is no picking and choosing - when you apply updates to your pool, it is updated to the latest, fully tested state. Configure your pool to automatically synchronize with an update channel. This action downloads all available updates to the pool coordinator. You can then apply all of the downloaded updates by using XenCenter. We expect you to consume all outstanding updates within six months of their release to remain in support.

NOTE:

Applying updates is only assured to work when the previous state of the pool is less than six months old. If you haven't applied updates for more than six months, updating to the latest update level is not tested and is not assured.

Complete the following steps to update your XenServer pools:

1. Install the latest version of XenCenter.
2. Install or upgrade to XenServer 9.
3. Configure updates for your pool.

   You can configure updates for a pool or standalone host from the following locations:

   - An update channel on the content delivery network (CDN). This method is recommended for internet-connected pools.
   - An offline update from a downloaded bundle This alternative method is intended for use when internet connectivity to your XenServer hosts is unavailable or restricted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- An existing pool. This method enables you to bring a standalone host or a pool up to the same level of updates as another pool that is at a higher level of updates. It is recommended for joining a newly installed host to a pool that is not at the latest level of updates.

4. View available updates for your pool.
5. Understand the guidance categories and update tasks.
6. Apply updates to your pool.
7. Complete any pending update tasks.

Configure updates for your pool

Updates from the CDN

Prerequisites

- Ensure that your XenServer® hosts have internet access and can connect to the required update domains.
- If your hosts are behind a firewall, allow access to subdomains of `ops.xenserver.com`. For more information, see Connectivity requirements.

NOTE:

Applying updates is only assured to work when the previous state of the pool is less than six months old. If you haven't applied updates for more than six months, updating to the latest update level is not tested and is not assured.

Follow these steps to configure your hosts for applying updates from the CDN:

1. In XenCenter®, on the **Tools** menu, select **Configure Updates**. Alternatively, go to the **Updates** section under your pool's **General** tab and select **Configure Updates** or right-click on your pool and select **Updates** > **Configure Updates**. The **Configure Server Updates** window opens.
2. On the **XenServer 8.4** tab, select the pools or hosts that you want to configure.
3. Under **Update Channel**, specify how soon you want to access updates. Your pool or host can be subscribed to one of the following update channels:

   - **Early Access**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Normal**

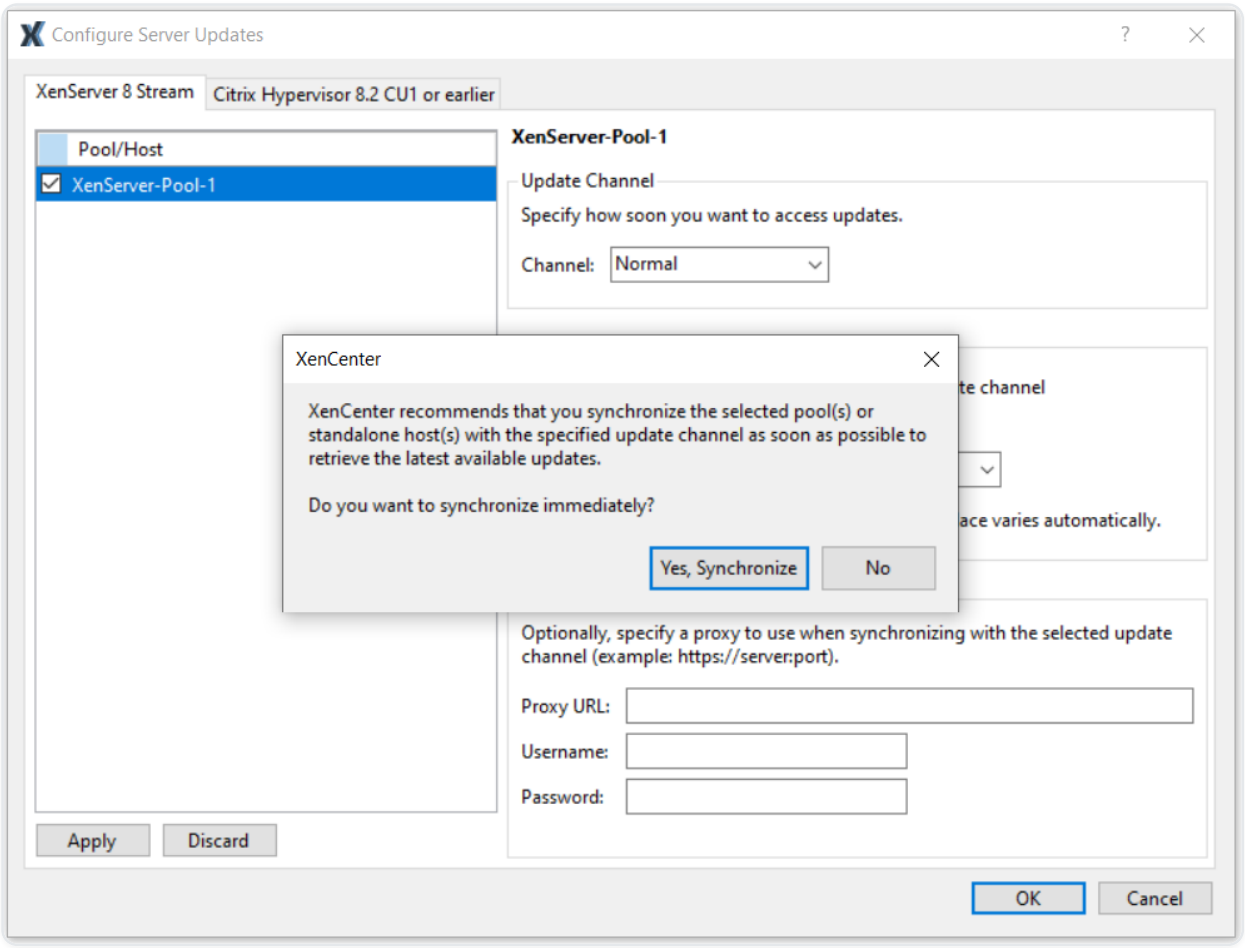
4. Under **Synchronization Schedule**, select how often you want your XenServer pool to synchronize with the update channel. This can be daily, or weekly on a certain day of the week.

   NOTE:

   - After synchronizing, apply the updates to your pool as soon as possible to benefit from the latest updates.
   - If you designate a new pool coordinator after synchronizing but before applying updates to the hosts in the pool, you must synchronize again with the new pool coordinator before you can update the pool.
   - Do not synchronize your XenServer pool while the pool is in the process of being updated.

5. (Optional) Under **Proxy Server**, specify a proxy to use when synchronizing with the update channel. This proxy server is used for communication between the host and the public CDN.
6. Click **Apply** to apply the configuration changes to your XenServer pool and then repeat the above steps to configure updates for the rest of your XenServer pools.
7. If you are happy with the configuration changes to your pools, click **OK** to save your changes and close the **Configure Server Updates** window. When you first set up your host or pool with an update channel (or if you later change your host or pool to synchronize with a different update channel), you are prompted to synchronize your host or pool with the update channel immediately. In the dialog box that opens, select **Yes, Synchronize** if you want to synchronize your host or pool with the update channel immediately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Alternatively, you can choose to synchronize your host or pool with the update channel at a later date. To synchronize your host or pool later, go to the **Updates** section under your pool's **General** tab and select **Synchronize Now** or right-click on your pool and select **Updates** > **Synchronize with update channel**.

8. As soon as your pool synchronizes with the update channel, apply the downloaded updates to your pool by using the **Install Updates** wizard. For more information, see Apply updates to your pool.

After configuring your XenServer pool or host, you can find the following information in XenCenter, in the **Updates** section under the **General** tab of your pool or host:

- The update channel you are subscribed to
- The last time your pool synchronized with the update channel
- The checksum of that synchronization
- The checksum of the last update you applied

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Offline Updates

Prerequisites

- Your host must be installed with the ISO published on October 7, 2024, or later.
- You must use XenCenter version 2024.4.0 or later to apply update bundles.

Follow these steps to configure Offline Updates:

1. Download the latest update bundle from the following page using your dedicated internet-connected machine: Download XenServer update bundles.
2. Transfer the update bundle to a location accessible from XenCenter.
3. In XenCenter, on the **Tools** menu, select **Configure Updates**. Alternatively, go to the **Updates** section under your pool's **General** tab and select **Configure Updates** or right-click on your pool and select **Updates** > **Configure Updates**. The **Configure Server Updates** window opens.
4. On the **XenServer 8.4** tab, select the pools or hosts that you want to configure.
5. Under **Update Channel**, select **Offline** to configure your host or pool to use the **Offline** update channel. Click **OK**.
6. You are prompted to upload an update bundle to your pool immediately.

   To upload an update bundle immediately, click **Yes** and in the window that opens, navigate to the location of the downloaded update bundle `.xsbundle` file on your computer and select it. Click **Next**.

   Alternatively, you can choose to upload an update bundle at a later date. To upload an update bundle later, go to the **Updates** section under your pool's **General** tab and select **Upload bundle** or right-click on your pool and select **Updates** > **Upload bundle**. The **Select update bundle file** window opens and you can select your `.xsbundle` file. You can also upload an update bundle using the **Install Updates** wizard. For more information, see Apply updates to your pool.
7. Review available updates for your pool and check if there are any update tasks required before or after applying updates. For more information, see View available updates for your pool.
8. Apply the updates to your pool by using the **Install Updates** wizard. For more information, see Apply updates to your pool.

After configuring your XenServer pool or host, you can find the following information in XenCenter, in the **Updates** section under the **General** tab of your pool or host:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The update channel your XenServer pool or host is configured to use
- The last time you uploaded an update bundle
- The checksum of that update bundle
- The checksum of the last update you applied

Update from a remote pool

This method enables you to update a pool or standalone host to the same level of updates as another pool (referred to as the "remote pool"). A remote-pool update synchronizes the host or pool with the remote pool and updates from update files held on the remote pool coordinator. Use this process to more easily join a new host to an existing pool by matching that pool's update level.

For a remote pool to be used as an update channel by a pool or standalone host, it must meet the following prerequisites:

- The remote pool must be at a more recent level of updates than the standalone host.
- The remote pool must have the latest synchronized updates applied to it.
- The pool coordinator has not changed since the remote pool was last updated.

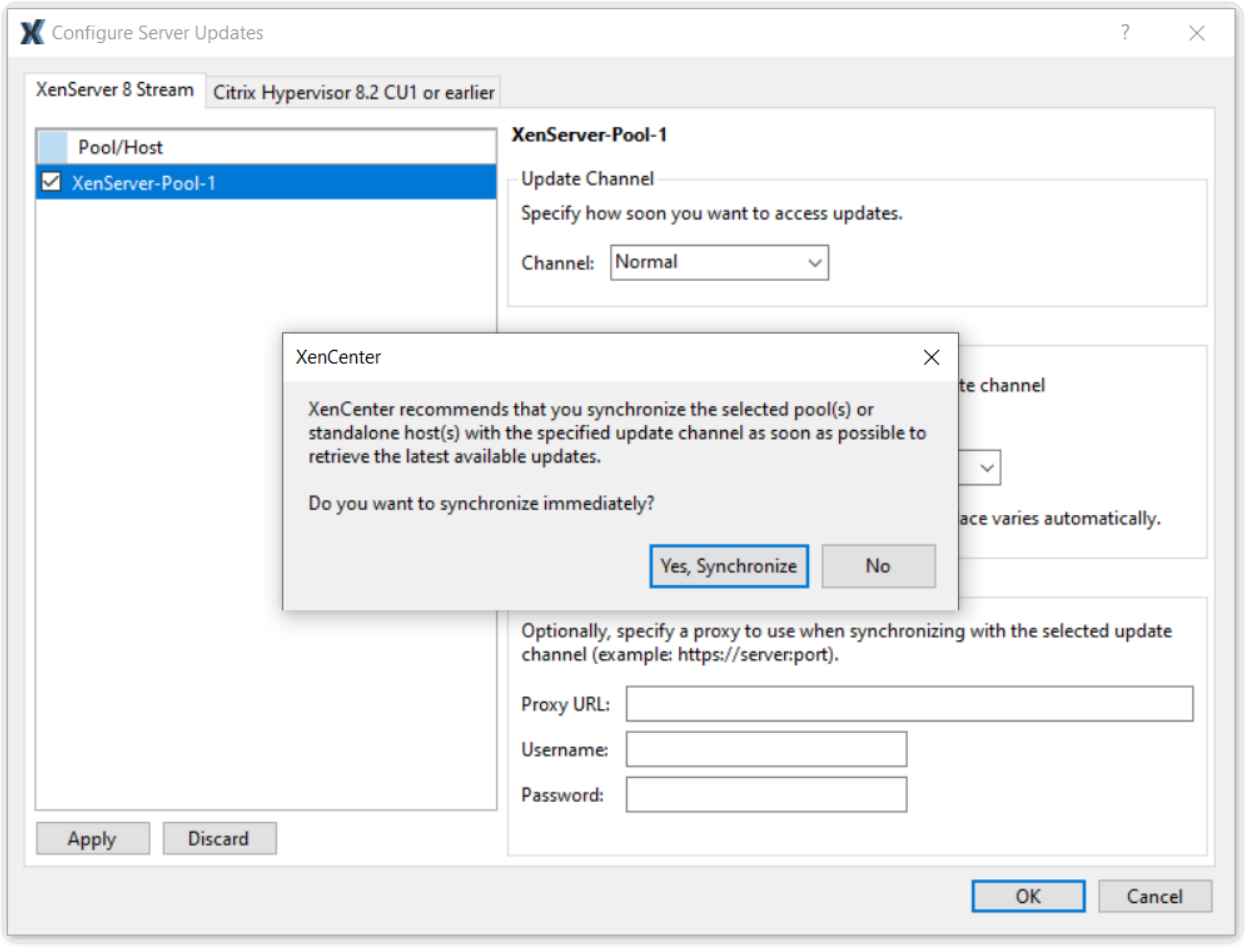
Configure a remote pool as an update channel

Follow these steps to configure your host or pool to use another pool as an updates channel:

1. In XenCenter, on the **Tools** menu, select **Configure Updates**. Alternatively, go to the **Updates** section under your pool's **General** tab and select **Configure Updates** or right-click on your pool and select **Updates** > **Configure Updates**. The **Configure Server Updates** window opens.
2. On the **XenServer 8.4** tab, select the pools or hosts that you want to configure.
3. Under **Update Channel**, select the remote pool you want to synchronize with from the section **Channels on other pools or standalone servers**. Click **OK**.
4. Click **Apply** to apply the configuration changes to your XenServer pool and then repeat the above steps to configure updates for the rest of your XenServer pools.
5. If you are happy with the configuration changes to your pools, click **OK** to save your changes and close the **Configure Server Updates** window. When you first set up your host or pool with an update channel (or if you later change your host or pool to synchronize with a different update channel), you are prompted to synchronize your host or pool with the update channel immediately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. In the dialog box that opens, select **Yes, Synchronize** if you want to synchronize your host or pool with the update channel immediately.



   Alternatively, you can choose to synchronize your host or pool with the update channel at a later date. To synchronize your host or pool later, go to the **Updates** section under your pool's **General** tab and select **Synchronize Now** or right-click on your pool and select **Updates** > **Synchronize with update channel**.

7. As soon as your pool synchronizes with the update channel, apply the downloaded updates to your pool by using the **Install Updates** wizard. For more information, see Apply updates to your pool.

After configuring your XenServer pool or host, you can find the following information in XenCenter, in the **Updates** section under the **General** tab of your pool or host:

- The update channel you are subscribed to
- The last time your pool synchronized with the update channel
- The checksum of that synchronization
- The checksum of the last update you applied

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View available updates for your pool

XenCenter issues notifications about available updates for your hosts and pools under the **Updates** tabs in the **Notifications** view. The **Updates** tabs are split into XenServer 8.4 updates and Citrix Hypervisor updates.



The XenServer 8.4 **Updates** tab refreshes in the following scenarios:

- For hosts and pools subscribed to the **Early Access** or **Normal** update channel, the tab refreshes based on the synchronization schedule you've set (either daily or weekly on a specific day).

  Alternatively, you can fetch the latest available updates for your hosts and pools by manually synchronizing with the **Early Access** or **Normal** update channels.
- For hosts and pools configured for Offline Updates, the tab refreshes each time you upload an update bundle to the host or pool.

  Alternatively, you can fetch the latest available updates for your hosts and pools by uploading the latest update bundle to your host or pool.

To view the latest updates available for pools configured to apply updates from the CDN, synchronize your XenServer pool with the update channel. You can do this in XenCenter® from the following places:

- In the **By Server** view of the **Updates** tab, you can choose to **Synchronize All** to synchronize all pools managed by XenCenter or **Synchronize Selected** to synchronize the selected pools.
- Alternatively, go to the **Updates** section under your pool's **General** tab and select **Synchronize Now** or right-click on your pool and select **Updates** > **Synchronize with update channel**.

To view the latest available updates for pools configured for Offline Updates, upload the latest update bundle to your pool. You can do this in XenCenter from the following places:

- In the **By Server** view of the **Updates** tab, you can choose to **Upload Bundle to All** to upload a bundle to all pools managed by XenCenter that use the **Offline** channel or **Upload Bundle to Selected** to upload a bundle to the selected pools.
- Alternatively, go to the **Updates** section under your pool's **General** tab and select **Upload bundle** or right-click on your pool and select **Updates** > **Upload bundle**.

You can then review all updates available for your XenServer 8.4 pools. The types of updates are:

- **Security fixes**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Bug fixes**
- **Improvements**
- **New features**
- **Preview features**
- **Foundational changes**

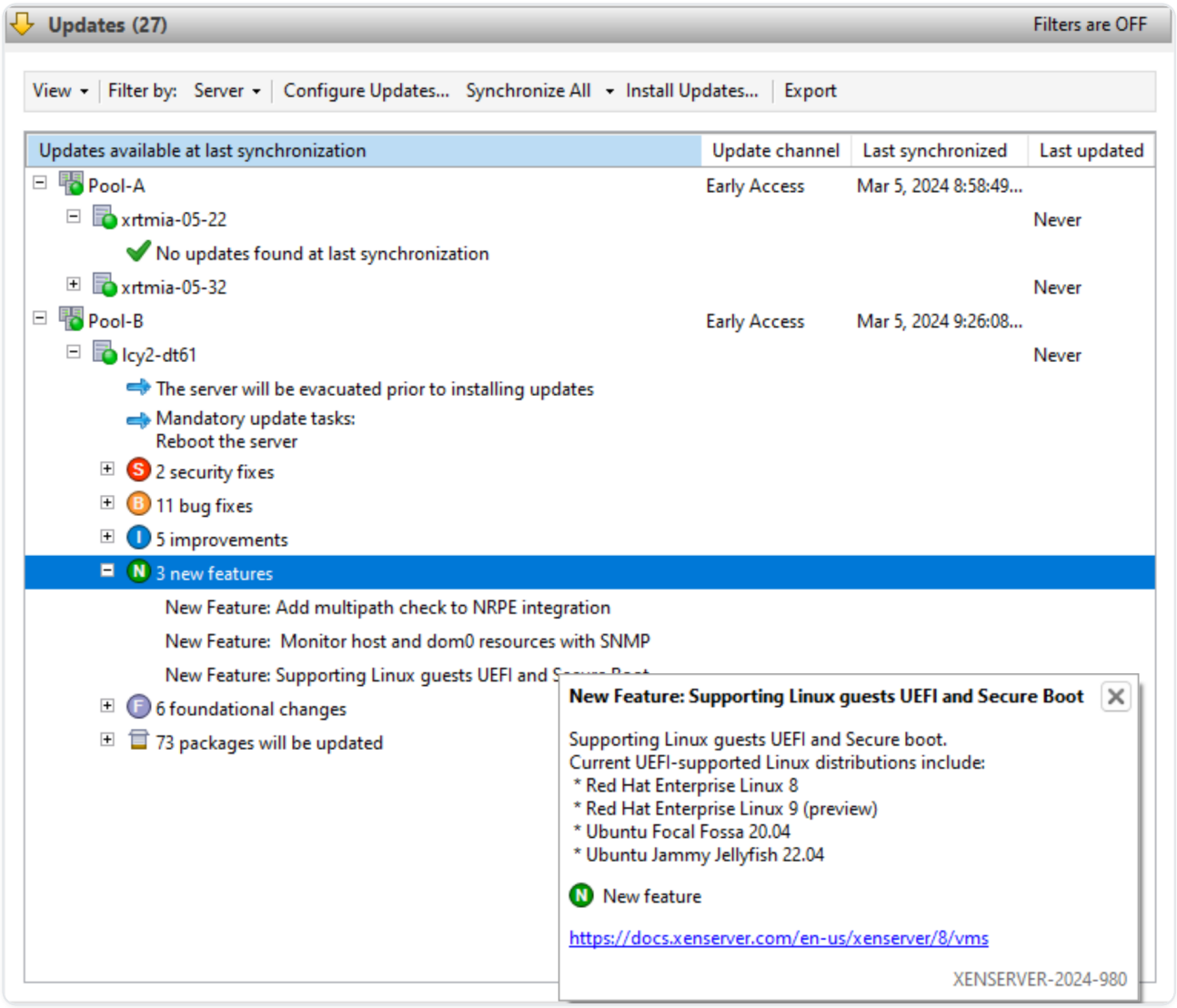
> **NOTE:**
>
> Foundational changes are non-customer visible groundwork changes to maintain and improve the product.

In the main panel, use the **View** option to choose whether the updates are displayed **By Server** or **By Update**.

By server

Updates are grouped by host and type of update.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can filter the update information by server. Select an update and hover over it to view detailed information about the update.

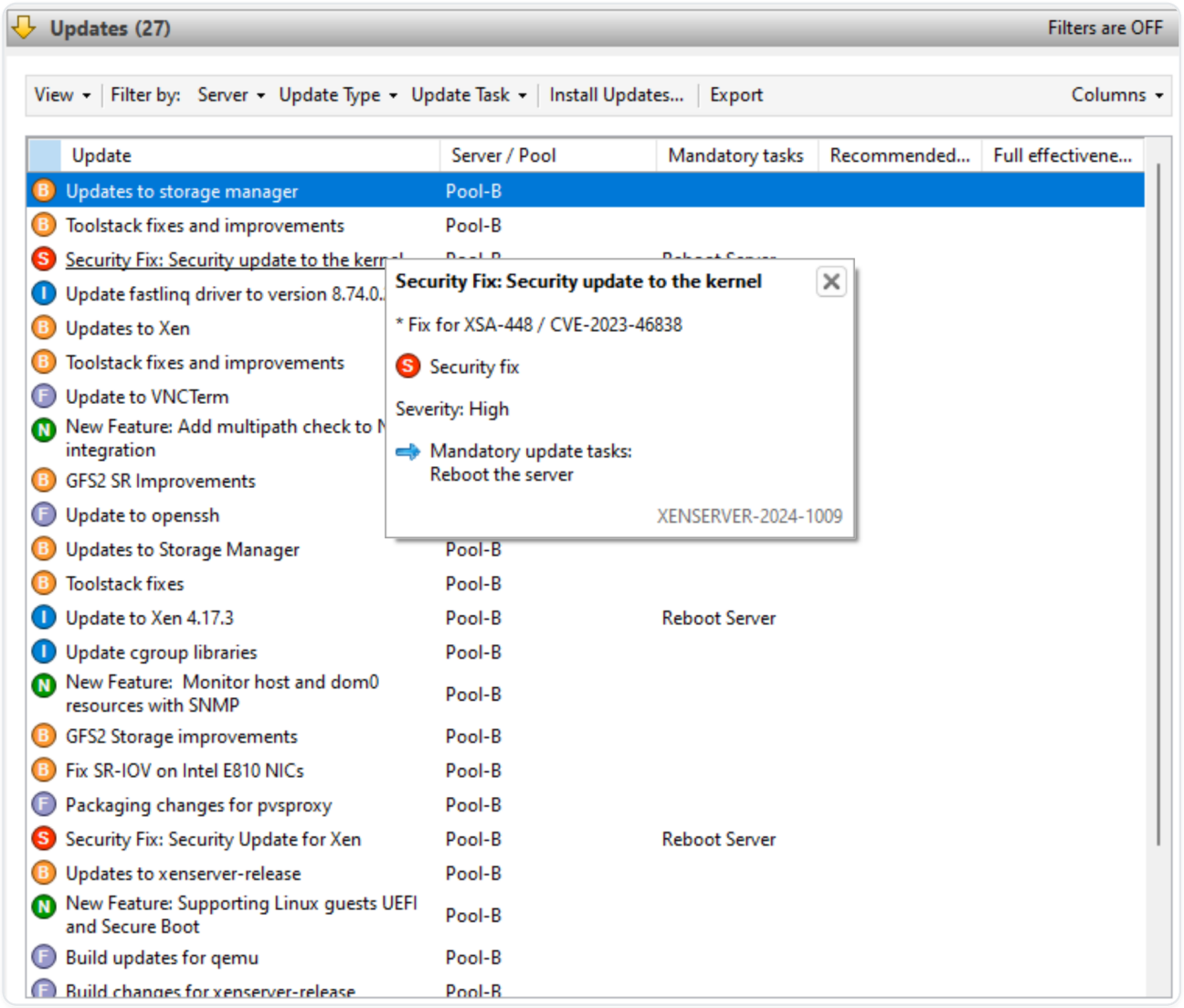
To view this information about your available updates offline, select **Export All** to export the information as a `.md` file. The contents of the `.md` file are grouped by pool and then host. For each host, the file lists the following information:

- Any update tasks for this host or its VMs. For more information about mandatory, recommended, and full effectiveness tasks, see Understand the guidance categories and update tasks.
- Whether these updates contain live patches that can be applied to this server
- Updates grouped by update type
  - The update name
  - A description of the update
- A list of the RPMs to be updated on the host

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By update

All updates are listed chronologically in order of release.



You can filter the update information by the server it can be applied to, by the update type, and by any update tasks that apply to it. Select an update and hover over it to view detailed information about the update.

To view this information about your available updates offline, select **Export All** to export the information as a `.csv` file. The `.csv` file contains the following information:

- The update type
- The update name
- The servers that this update can be applied to
- Whether the update includes a live patch that can be applied to the servers
- The mandatory, recommended, and full effectiveness tasks

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about mandatory, recommended, and full effectiveness tasks, see Understand the guidance categories and update tasks.

- To apply the updates to your hosts or pools, select **Install Updates** to open the **Install Updates** wizard. For more information, see the following section Apply updates to your pool.

Understand the guidance categories and update tasks

Some tasks (such as evacuating or rebooting your hosts) might be required before and after applying updates to your pool. Sometimes, there are no update tasks required.

Guidance categories

XenServer® tries to minimize the disruption to your VMs that these update tasks might cause by categorizing the tasks into **Mandatory**, **Recommended**, **Full-effectiveness**, and **Live patch**. These categorizations enable you to judge whether an update task that might cause downtime or minor disruption for your hosts or VMs is necessary for your environment and risk profile.

Updates can have tasks listed in more than one of these categories. For example, an update might require that you restart the host to get the full-effectiveness of the update, but recommend restarting the toolstack to get most of the benefit of the update with less potential disruption to the pool.

During the update process, you can choose to carry out one of the following three levels of tasks:

1. Mandatory
2. Mandatory + Recommended
3. Mandatory + Recommended + Full-effectiveness

Mandatory

Mandatory tasks *must* be performed after an update otherwise the system might fail at runtime. These actions are required to enable critical fixes and ensure that your environment is secure and stable. When you apply updates, XenCenter® performs these tasks. You cannot opt out of mandatory tasks.

Recommended

Recommended tasks are the tasks that we recommend you perform to get the benefit of the majority of features and fixes delivered in the updates. When you apply updates, these tasks are selected by default in XenCenter, but you can opt out of performing them. If you choose not to perform these tasks now, they are listed in the pending tasks for the applicable pool, host, or VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Why perform the recommended tasks:

- These tasks are the ones that ensure a secure, stable XenServer environment.

Why opt out of the recommended tasks:

- After reviewing the detailed information for the updates, you judge that the risk of not fully applying these updates now is acceptable.
- The recommended tasks cause unwanted disruption to your VMs now.

Full-effectiveness

Full effectiveness tasks are required to get the benefit of the related update. The updates that have full-effectiveness tasks associated with them are usually relevant only to users on certain hardware or using specific features.

Review the update information to understand whether these tasks are required for your environment. When you apply updates, these tasks are not selected by default in XenCenter, but you can choose to perform them during the update if you believe the update applies to your environment or configuration. If you choose not to perform these tasks now, they are listed in the pending tasks for the applicable pool, host, or VM.

Why perform the full-effectiveness tasks:

- The updates that have full-effectiveness tasks are relevant to your hardware, environment, or configuration.

Why remain opted out of the full-effectiveness tasks:

- The updates that have full-effectiveness guidance are not relevant to your hardware, environment, or configuration.
- The full-effectiveness tasks cause unwanted disruption to your VMs now.
- You do not need the benefits of these updates right now.

If the full-effectiveness tasks apply to your environment, but you have opted to defer them, plan to complete these tasks during a suitable maintenance window to maintain the stability of your environment.

Live patches

Updates to certain components can include a live patch. A live patch enables updates to be applied to core components without requiring a host reboot.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Whether a live patch can be applied to your hosts depends on the version of the component that was installed when the hosts were last rebooted. If an update can be applied as a live patch to your hosts, the live patch guidance replaces the recommended guidance.

EXAMPLE:

You have two pools. Pool A is updated to a recent level. Pool B has not been updated for some time. We release a new update that has the recommended update task "Restart host" and the live patch update task "Restart toolstack".

In pool A, the live patch can be applied to these more up-to-date hosts. XenCenter recommended guidance shows "Restart toolstack". The less disruptive task from the live patch guidance overrides the recommended guidance.
In pool B, the live patch cannot be applied to the hosts as they are at an older level. XenCenter recommended guidance shows "Restart host". The recommended guidance remains applicable. The live patch guidance is irrelevant in this case.
Sometimes only some of the fixes in an update are enabled when the update is applied as a live patch. In this situation, you might still see a recommended reboot for an update even though the live patch applies. Review the update details to understand whether you need all fixes in the update or just those fixes enabled by the live patch. You can then use this information to choose whether to perform the tasks. For more information, see View available updates for your pool.

Update tasks

Applying updates might require you to complete one or more tasks, either before or after the updates are applied. These tasks can appear in any guidance category.

Update tasks for your host

Tasks required *before* applying updates:

- **Evacuate server**: All VMs must be migrated off the XenServer host or shutdown before applying the update. To complete this task, XenCenter migrates any VMs off the host. While this task is in progress, the XenServer pool is operating at reduced capacity as one host is temporarily unavailable to run VMs. This task is sometimes carried out as part of the 'Reboot host' task.

Tasks required *after* applying updates:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Reboot server**: The XenServer host must be restarted. Any VMs are migrated off the host and the host is restarted. While this task is in progress, the XenServer pool is operating at reduced capacity as one host is temporarily unavailable to run VMs.
- **Restart toolstack**: The toolstack on the host must be restarted. If performed on the pool coordinator, the connection to the pool is temporarily lost. Restarting on other hosts has no visible effect on the pool's state.

Update tasks for your VM

Some updates provide new features for your VMs. These updates might require the following tasks on your VMs:

- **Reboot VM**: The VM must be restarted. In XenCenter, the VM displays a red stop icon (square on red) while restarting. Once the task is complete, the green play icon appears, indicating the VM is running. During the reboot, the VM is unavailable to end users.
- **Restart device model**: The device model for VMs on the updated host must be restarted. In XenCenter, the VM shows a yellow play triangle while the device model restarts. Once complete, the green play icon appears. During this time, you cannot stop, start, or migrate the VM. The end user of the VM might experience a brief pause and resume in their session. To support this task on a Windows VM, the VM must have XenServer VM Tools for Windows installed.

Apply updates to your pool

The update installation mechanism in XenCenter® applies the updates to your hosts and pools using the **Install Updates** wizard. During the process, XenCenter automatically works out the least impactful action required after applying all available updates. The **Install Updates** wizard automatically performs these steps:

1. If required, it migrates VMs off each host.
2. If required, it places the host in Maintenance mode.
3. It applies the updates.
4. If required, it runs any necessary update tasks such as rebooting the host, restarting the toolstack, or rebooting the VMs.
5. It migrates the VMs back to the updated host.

Any actions that are taken at the pre-check stage to enable the updates to be applied, such as turning off high availability, are reverted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Before you start

Before you apply an update to your servers, pay careful attention to the following:

- Back up all your servers
- If the set of updates includes updates to a driver, ensure that the new version of the driver is compatible with your hardware and firmware. For more information, see the Hardware Compatibility List (HCL) and your hardware vendor documentation.
- Ensure that High Availability (HA) is not enabled on any pool where you intend to apply updates.
- Ensure that you are logged in to XenCenter® as a Pool Administrator or Pool Operator, or using a local root account.

Install updates

Updates from the CDN

The following section provides step-by-step instructions on applying updates to your internet-connected pools using the **Install Updates** wizard:

1. From the XenCenter® menu, select **Tools** and then **Install Updates**.

2. In the **Install Updates** wizard, select **XenServer 8.4** and review the information on the **Before You Start** page. Click **Next** to continue.
3. Select **Apply updates**. Click **Next** to continue.
4. Select the XenServer® pools or hosts that you want to update. Click **Next** to progress to the next wizard page.
5. After updates are applied, some tasks, such as rebooting your hosts, might be required. On the **Update Mode** page, select the level of update tasks that you want XenCenter to automatically carry out after applying updates to your pool.

   Tasks are categorized as **Mandatory**, **Recommended**, or **Full Effectiveness** under **Tasks**. If there are no update tasks required, the page displays a note saying **No action required**.

   By default, XenCenter chooses the recommended level of update tasks. However, mandatory tasks are always performed and cannot be deselected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To review these tasks in detail, minimize the wizard and go to the **Notifications** > **Updates** tab. For more information about the different types of update tasks and the guidance levels provided by XenCenter, see Understand the guidance categories and update tasks.

Click **Next** to progress to the next wizard page and begin pre-checks.

6. The wizard performs several pre-checks to verify that the updates can be applied on your host or pool. For example, you must have synchronized your host or pool with the update channel within the past week.

   Follow the on-screen recommendations to resolve any pre-checks that have failed. If you prefer XenCenter to automatically resolve all failed pre-checks, select **Resolve All**. When the pre-checks have been resolved, select **Next** to continue.

7. Click **Install updates** for XenCenter to begin installing updates for your host or pool.

8. The **Install Updates** wizard shows the progress of the update, displaying the major operations that XenCenter performs while updating each host in the pool.

   NOTES:

   - If the update process cannot complete for any reason, XenCenter halts the process. This halt allows you to fix the issue and resume the update process by clicking the **Retry** button.
   - If you select **Cancel** at this stage, the **Install Updates** wizard reverts any changes that you might have made to resolve failed pre-checks (such as pausing High Availability and Workload Balancing or suspending VMs).

   Click **Finish** to complete the updates and close the **Install Updates** wizard.

Offline Updates

The following section provides step-by-step instructions for applying updates to pools configured for offline updates using the **Install Updates** wizard:

1. From the XenCenter menu, select **Tools** and then **Install Updates**.

2. In the **Install Updates** wizard, select **XenServer 8.4** and review the information on the **Before You Start** page. Click **Next** to continue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. If you have previously uploaded an update bundle, select **Apply updates**. Otherwise, choose **Select an update bundle or supplemental pack from disk** and click **Browse** to navigate to the location of the downloaded update bundle `.xsbundle` file on your computer.

   NOTE:

   You can download the latest update bundle from the following page using your dedicated internet-connected machine: Download XenServer update bundles. You then transfer the update bundle to a location accessible from XenCenter.

   Click **Next** to continue.

4. Select the XenServer pools or hosts that you want to update. Click **Next**.

5. If you selected to upload an update bundle, the **Install Updates** wizard displays the progress of uploading the bundle to your pool or hosts on the **Upload** page. However, if you are applying a previously uploaded update bundle, this page is not displayed.

   NOTE:

   If you've just uploaded an update bundle that is older than the one currently applied to your pool, XenCenter displays that there are no available updates to apply and you cannot proceed further.

   Once the process is complete, click **Next** to continue.

6. After updates are applied, some tasks, such as rebooting your hosts, might be required. On the **Update Mode** page, select the level of update tasks that you want XenCenter to automatically carry out after applying updates to your pool.

   Tasks are categorized as **Mandatory**, **Recommended**, or **Full Effectiveness** under **Tasks**. If there are no update tasks required, the page displays a note saying **No action required**.

   By default, XenCenter chooses the recommended level of update tasks. However, mandatory tasks are always performed and cannot be deselected.

   To review these tasks in detail, minimize the wizard and go to the **Notifications** > **Updates** tab. For more information about the different types of update tasks and the guidance levels provided by XenCenter, see Understand the guidance categories and update tasks.

   Click **Next** to progress to the next wizard page and begin pre-checks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. The wizard performs several pre-checks to verify that the updates can be applied on your host or pool.

   Follow the on-screen recommendations to resolve any pre-checks that have failed. If you prefer XenCenter to automatically resolve all failed pre-checks, select **Resolve All**. When the pre-checks have been resolved, select **Next** to continue.

8. Click **Install updates** for XenCenter to begin installing the updates to your host or pool.
9. The **Install Updates** wizard shows the progress of applying the updates, displaying the major operations that XenCenter performs while updating each host in the pool.

   NOTES:

   - If the update process cannot complete for any reason, XenCenter halts the process. This halt allows you to fix the issue and resume the update process by clicking the **Retry** button.
   - If you select **Cancel** at this stage, the **Install Updates** wizard reverts any changes that you might have made to resolve failed pre-checks (such as pausing High Availability and Workload Balancing or suspending VMs).

   Click **Finish** to complete the updates and close the **Install Updates** wizard.

Complete any pending update tasks

After applying updates, complete any pending update tasks to ensure your hosts and VMs operate as expected.

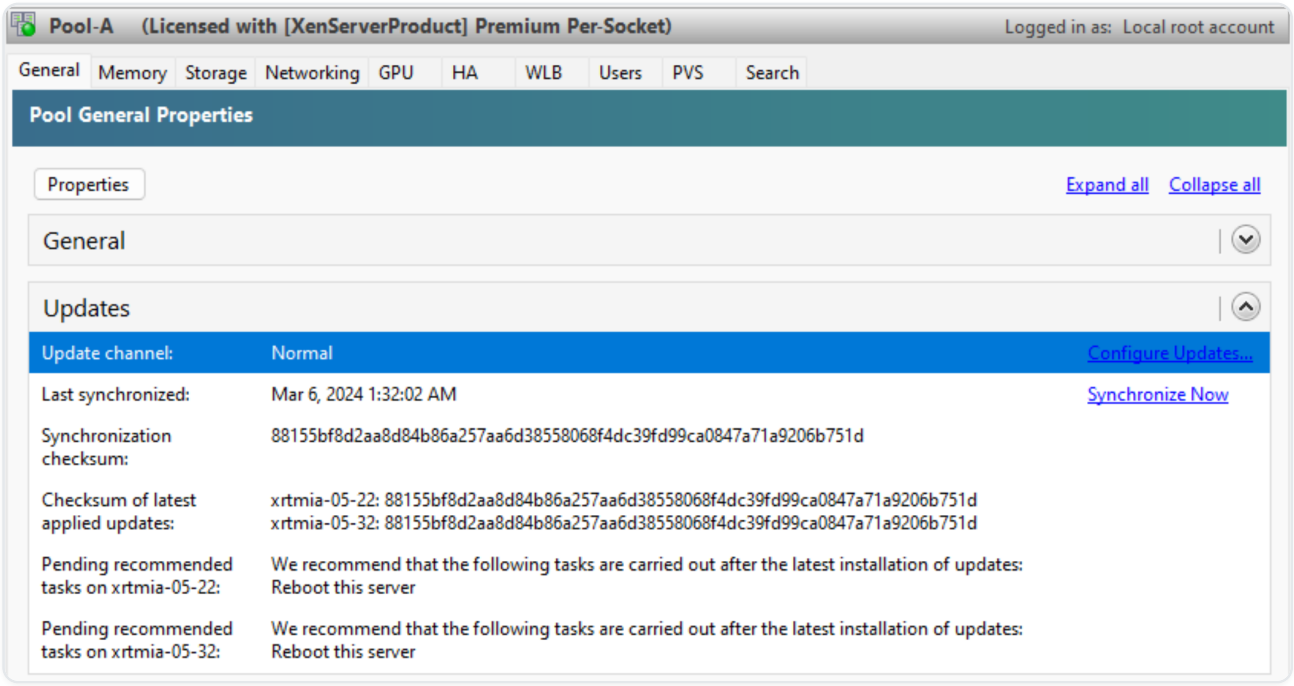
NOTE:

Before applying updates, you can review the required update tasks on the XenServer 8.4 **Updates** tab in the **Notifications** view. For more information, see View available updates for your pool.

If you skip any tasks during the update process, the pending tasks for each pool, host, or VM appear in the **Updates** section of the **General** tab for the pool, host, or VM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

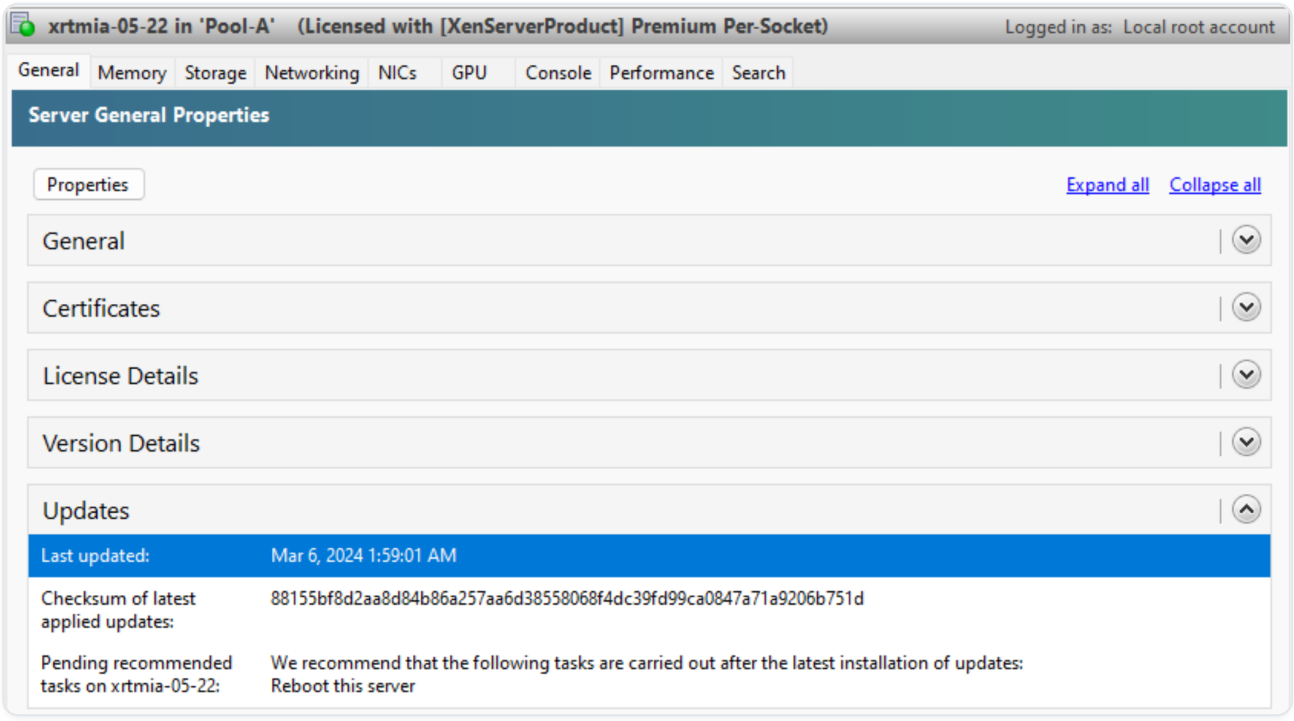
Pool pending tasks



This section shows the pending tasks for all hosts in the pool.

It also shows a checksum that indicates the level that the current pool coordinator has synchronized to and checksums for each host that indicate the level of the updates installed. These checksums can provide useful information if you need to contact Technical Support.

Host pending tasks

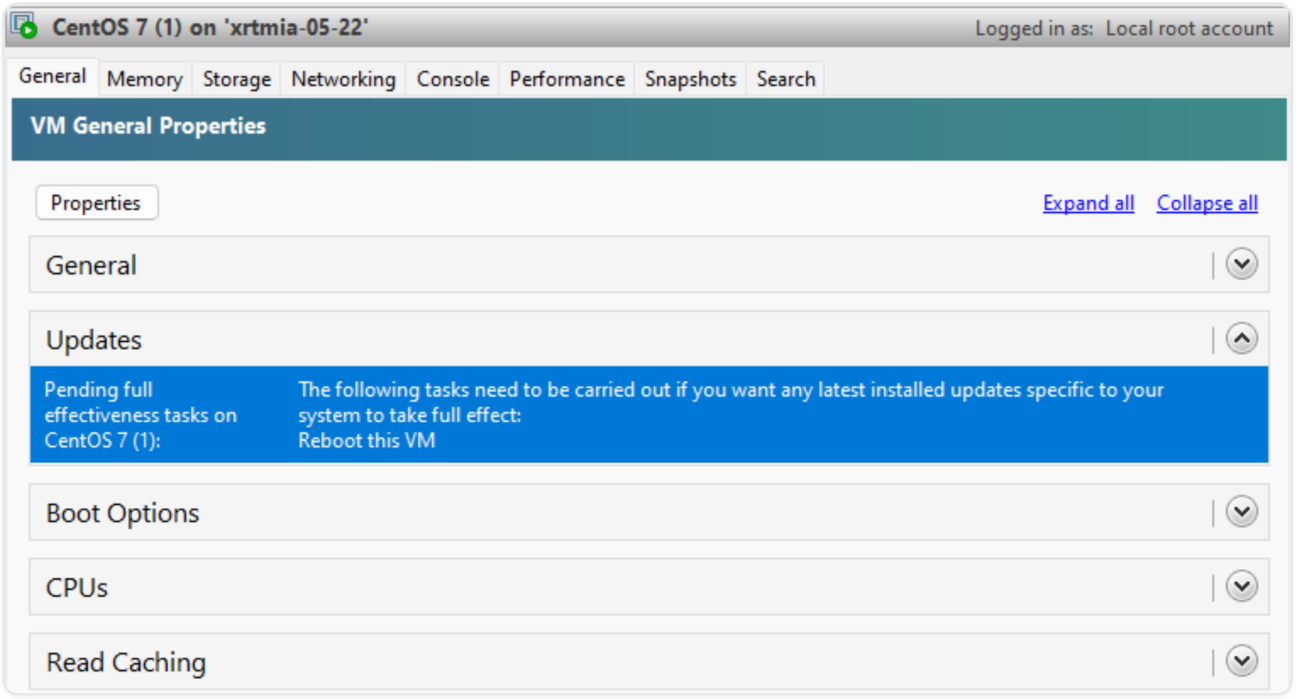


This section shows the pending tasks for the XenServer® host.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

It also shows a checksum that indicates the level of the updates installed. This checksum can provide useful information if you need to contact Technical Support.

VM pending tasks



This section shows the pending tasks for a VM.

Related documentation

XenServer Current Release

- Update your XenServer hosts

Live patches

XenServer® customers who deploy XenServer hosts might often need to reboot their servers after applying updates. This rebooting results in unwanted downtime for the servers while customers have to wait until the system is restarted. Reboots reduce the uptime of the servers and impact business. Live patching enables customers to install some Linux kernel and Xen hypervisor updates without having to reboot the servers. This feature reduces maintenance costs and downtime. Such updates consist of the following components:

- A live patch that is applied to the memory of the server
- An update that updates the files on disk

Live patching is enabled by default. For more information about enabling and disabling live patching, see Change Pool Properties.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When applying an update using the **Install Updates** wizard, the **Pre-checks** page displays information about the update tasks. Complete these tasks for the update to take effect. In addition, the wizard checks whether you must reboot the servers after applying the update and displays the result. This feature enables customers to know the update tasks well in advance and schedule the application of updates accordingly.

Live patching scenarios

Updates can be live patched across pools, servers, or on a standalone server. Some updates might need you to reboot the server, some need the XAPI toolstack to be restarted, and a few updates do not have any update tasks.

The following scenarios describe the behavior when a live patch is and is not available for an update:

- **Updates with live patch** Updates that update the Linux kernel and the Xen® hypervisor usually do not need a reboot after applying the update. However, in some rare cases, when the live patch cannot be applied, a reboot might be required.
- **Updates without live patch** No change in the behavior here. It works as usual.

NOTE:

If a server doesn't require a reboot or if the update contains live patches that can apply to the servers, XenCenter® displays **No action required** on the **Update Mode** page.

Update XenCenter®

When a new version of XenCenter is available, XenCenter displays the notification **XenCenter Update** in the menu bar.

Click this notification to choose one of the following actions:

- **Download and Install**: XenCenter downloads the update file, verifies its checksum, and launches the installer.

  By default, XenCenter launches automatically after the installation process has completed. You can change this behavior in the **XenCenter Setup** wizard.

  If you have events running in XenCenter, XenCenter alerts you of the status of these events. It prompts you to either abort the installation or to exit XenCenter and continue the installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **<version> Release Notes**: Open a browser window to view the release notes for the new version of XenCenter on the web.

You can prompt XenCenter to check for updates by going to **Help > Check For Updates**.

You choose whether to automatically check for updates by going to **Tools > Options** and then to the **Updates** panel, deselect **Check for new versions of XenCenter**.

You can configure a proxy server that XenCenter goes through to check for and download updates. For more information, see Proxy server.

NOTE:

To provide update notifications and automatic updates, XenCenter requires internet access. If your XenCenter is behind a firewall, ensure that it has access to `updates.ops.xenserver.com` through the firewall. For more information, see Connectivity requirements.

If you cannot allow your XenCenter access to the internet and want to instead update it manually, new versions of the XenCenter installer are periodically supplied on the XenServer product downloads page.

Update Notifications

Use XenCenter to enable the automatic and periodic checking of new updates for XenCenter and XenServer.

Enable XenCenter® notifications

Prerequisites

- Ensure that your XenCenter has internet access and can connect to the required update domains.
- If your XenCenter is behind a firewall, allow access to subdomains of `updates.ops.xenserver.com`. For more information, see Connectivity requirements.

When you launch XenCenter for the first time, you are asked if you want XenCenter to periodically check and prompt you when there's a new version of the application available for download.

You can also enable XenCenter notifications by following these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In XenCenter, on the **Tools** menu, select **Options**. The **Options** window opens.
2. Select the **XenCenter Updates** tab.
3. Select the **Check for new versions of XenCenter** check box to allow XenCenter to periodically check and notify you when a new XenCenter version is available.
4. Click **OK** to apply your changes and close the **Options** window.

Enable update notifications for your hosts

XenCenter issues notifications about available updates for your hosts and pools running XenServer under the **Updates** tabs in the **Notifications** view.

The **Updates** tab refreshes based on your update configuration:

- Updates from the CDN: The tab refreshes according to the synchronization schedule you've set (daily or weekly). You can also manually synchronize with the **Early Access** or **Normal** update channels to fetch the latest updates.
- Offline Updates: The tab refreshes each time you upload an update bundle to the host or pool. You can also manually upload the latest update bundle to your host or pool to fetch the latest updates.

The updates are grouped by host and type of update (security fixes, bug fixes, improvements, new features, preview features, or foundational changes). Use the **Configure Server Updates** dialog to configure update notifications for your XenServer hosts and pools:

1. In XenCenter, on the **Tools** menu, select **Configure Updates**. Alternatively, go to the **Updates** section under your pool's **General** tab and select **Configure Updates** or right-click on your pool and select **Updates** > **Configure Updates**. The **Configure Server Updates** window opens.
2. Select the pools or hosts that you want to configure.
3. Under **Update Channel**, specify how soon you want to access updates. Your pool or host can be configured to one of the following update channels:
    - **Early Access**
    - **Normal**
    - **Offline**
4. If you selected **Early Access** or **Normal**, select how often you want your XenServer pool to synchronize with the update channel under **Synchronization Schedule**. This can be daily, or weekly on a certain day of the week.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenCenter synchronizes your pool with the update repository and downloads any available updates to the pool coordinator. Then, apply the downloaded updates to your pool by using XenCenter.

> **NOTE:**
>
> After synchronizing, apply the updates to your pool as soon as possible to benefit from the latest updates.

5. (Optional) If you selected **Early Access** or **Normal**, specify a proxy to use when synchronizing with the update channel under **Proxy Server**. This proxy server is used for communication between the host and the content delivery network (CDN).
6. Click **Apply** to apply the configuration changes to your XenServer pool and then repeat the above steps to configure updates for the rest of your XenServer pools.

Install supplemental packs

Supplemental packs (including driver disks) are used to modify and extend the functionality of the XenServer host, by installing software into the control domain (dom0). Users can add supplemental packs either during the initial XenServer installation, or at any time afterwards. When you upgrade XenServer, previously applied supplemental packs are removed by upgrade and so they must be reapplied during or after the upgrade. Facilities also exist for OEM partners to add their supplemental packs to XenServer installation repositories to allow automated factory installations.

To install a supplemental pack using XenCenter®

1. Download the supplemental pack (`filename.iso`) to a known location on your computer.
2. From the XenCenter menu, select **Tools** and then **Install Updates**.
3. Read the information on the **Before You Start** page and then select **Next** to continue.
4. On the **Select Update** page, select **Browse** to add the supplemental pack and then click **Next** to continue.
5. On the **Select Servers** page, select the pool or host to apply the supplemental pack to. Click **Next**. This action uploads the supplemental pack to the default SR of the pool or the host.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> If the default SR in a pool is not a shared SR, or does not have enough space, XenCenter tries to upload the supplemental pack to another shared SR with sufficient space. If none of the shared SRs have sufficient space, the supplemental pack is uploaded to local storage on each host.

6. The **Upload** page displays the status of the upload. If there is not enough space on the SR, an error is displayed. Click **More Info** for details and take necessary action to free up the space required for the upload.
7. After the file is successfully uploaded, XenCenter performs pre-checks to determine whether the supplemental pack can be applied onto the selected servers.

   Follow the on-screen recommendations to resolve any update pre-checks that have failed. If you would like XenCenter to automatically resolve all failed pre-checks, click **Resolve All**.
8. Choose the **Update Mode**. Review the information displayed on the screen and select an appropriate mode. If you select **Cancel** at this stage, the **Install Updates** wizard reverts the changes and removes the supplemental pack from the SR.
9. Select **Install update** to proceed with the installation. The **Install Updates** wizard shows the progress of the update, displaying the major operations that XenCenter performs while updating each host in the pool.
10. When the supplemental pack installation is complete, click **Finish** to close the wizard. The newly installed supplemental pack is displayed in the **Updates** section on the **General** tab of the host or the pool.

Related documentation

XenServer Current Release

- Install the XenServer host
- Install supplemental packs

Install driver disks

Note: Driver disks are not published for XenServer 9. If you are running XenServer 9, use Driver multi-version instead.

You can install a driver disk using one of the following methods:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- By using XenCenter® (recommended)
- During a clean XenServer® installation
- By using the xe CLI

For information on how to install a driver disk during a clean XenServer installation, see Install the XenServer host. For information on how to install a driver disk by using the xe CLI, see Install driver disks.

After installing the driver, restart your server for the new version of the driver to take effect. As with any software update, we advise you to back up your data before installing a driver disk.

Install a driver disk by using XenCenter

Perform the following steps to install the driver disk by using XenCenter:

1. Download the driver disk to a known location on a computer that has XenCenter installed.

   You are not required to extract the contents of the zip file. XenCenter can install the driver from the zip file or the iso.
2. In XenCenter, go to **Tools** > **Install Updates**. The **Install Update** dialog opens.
3. On the **Select update** tab, choose **Select an update or supplemental pack from disk** and browse to the location of the zip file or iso.

   Click **Next**.
4. Complete the steps in the dialog to select your servers and install the driver disk.
5. To complete the installation, XenCenter can restart the server now. Alternatively, you can choose to restart manually at a time that is convenient for you.

   NOTE:

   The driver does not take effect until after the host is restarted.

Related documentation

XenServer 8.4

- Hardware drivers
- Install the XenServer host
- Install driver disks

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenCenter® Alerts

You can view different types of system alerts in XenCenter by clicking **Notifications** and then **Alerts**.

The **Alerts** view displays various types of alerts, for example:

- **Performance alerts**. Performance alerts can be generated when CPU, memory usage, network, storage throughput, or VM disk activity exceeds a specified threshold on a server, VM, or SR. For information on configuring performance alerts, see Configuring performance alerts.
- **HA (High Availability) status alerts**. Alerts can be generated for changes to a pool's high availability status, such as when a pool becomes over committed.
- **License expiry alerts**. Alerts are generated when the XenServer® license on your managed server approaches or reaches its expiry date. You also receive these alerts when your Trial Edition 90-day trial period expires.
- **End of life alerts**. Alerts are generated when the XenServer version on your managed server approaches or reaches its end of life. To ensure that updates to address any future functional and security-related issues can be applied, update your environment to a later supported release. Go to the **Updates** view to see what update or upgrade options are available.
- **Certificate alerts**. Alerts are generated when the certificate on a XenServer host approaches or reaches its expiry date. The first alert is generated 30 days before expiry. The severity of the alert increases 14 days and again 7 days before expiry.
- **Update channel alerts**. Alerts are generated if you have not configured an update channel for your XenServer pool or if the last time you synchronized your pool with the update channel was more than 90 days ago. After 180 days, the severity of the alert increases.
- **VM group alerts**. Alerts are generated if all the running VMs in an anti-affinity group reside on a single host. If this changes, the alert is cleared. This alert is not generated if only one of the VMs in the group is running or no VMs in the group are running.
- **GFS2 cluster alerts**. For pools with GFS2 clustering enabled, alerts are generated when a host in the pool joins, leaves, or fences. An alert is also generated if the cluster is close to losing quorum.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Working with alerts

XenCenter is equipped with powerful filtering capabilities. It enables you to filter alerts displayed on the **Alerts** tab. You can view alerts only from specific pools or servers, or only those alerts generated during a specific time period. For some alerts, it might be possible to quickly address the issue that caused the alert to be generated. The following sections list various options available in the **Alerts** view.

Filter by Severity

Filters alerts by their severity

By default, alerts of all severity levels are displayed on the **Alerts** tab. To view alerts of a particular severity, select **Filter by Severity** and then cancel the selection on other severity levels from the list. Select **Show All** to view all the alerts.

Filter by Location

Filters alerts by the source from which they originate

By default, alerts from all hosts connected to XenCenter are displayed. To stop displaying alerts from a specific host, select the list and cancel the selection on the host. Clicking again on the host toggles your selection.

Filter by Date

Filters alerts based on the time of occurrence

By default, all alerts for the current XenCenter session are displayed. Select the list and select a date range from the list. Alternatively, select **Custom** to define your own date range by specifying the start and end date/time. Select **Show All** to view all the alerts.

Refresh

If new alerts are generated when the **Alerts** tab is open, they might not appear in the list. Select **Refresh** to view an updated the list.

Export All

Exports alerts as a comma delimited (.csv) file for viewing and analysis in external applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dismiss All

Removes alerts from the view

To dismiss or remove all the alerts, select **Dismiss All**. To dismiss a specific set of alerts, select the required alerts from the list, and select **Dismiss Selected**.

Actions

Enables you to perform specific actions on the alerts displayed. The **Actions** list displays all actions available for the selected alert.

Select an alert from the list and then select the action relevant to the alert to address it. For example, select:

- **Alarm Settings** to manage alerts for your host's CPU, memory usage, network activity, and storage throughput. This action opens the **Host Properties** dialog box.
- **Copy** to copy information about the alert to the clipboard.
- **Dismiss** to dismiss the alert.
- **Go to Web Page** to open the update page in a web browser.
- **HA settings** to manage High Availability alerts. This action opens the **Configure HA** dialog box.
- **Help** to open the Help topic related to the alert.
- **License Manager** to manage your licenses. This action opens the **License Manager** dialog box.
- **View Log Files** to open the directory where logs are stored.
- **Install Certificates** to update the certificate on a server. This action opens the **Install Certificates** dialog.
- **Configure Updates** to configure server updates for your host or pool.
- **Synchronize Now** to synchronize your host or pool with its configured update channel.

Receiving alert notifications by email

You can configure XenCenter to email notifications when alerts are generated for any servers and VMs in a pool, or for a standalone server and its VMs. When you turn on the email notification feature, you receive an email notification when alerts with a priority of 3 or higher are generated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you generate your own alerts using the XenServer xe CLI, you can assign a priority for different types of alerts. For more information, see Command line interface.

To turn on email notifications

1. Select a pool or standalone server in the **Infrastructure** view.
2. Select the **General** tab and then **Properties**.
3. Select the **Email Notifications** tab in the **Properties** dialog box.
4. Select the **Send email alert notifications** check box and then type the delivery address details.

   NOTE:

   Enter the details of an SMTP server which does not require authentication. Emails sent through SMTP servers which require authentication are not delivered. For instructions on using authenticated SMTP servers to receive email notifications, see Monitor and manage.

5. Select **OK** to save your changes and close the dialog box.

Receiving alert notifications with SNMP

NOTE:

The SNMP feature is available for XenServer Premium or Trial Edition customers. For more information about XenServer licensing, see Licensing. To upgrade, or to get a XenServer license, visit the XenServer website.

With the Pool Admin role, you can use SNMP to remotely monitor resources consumed by your XenServer host and dom0 - the control domain of your host. You can also configure traps, which are messages that alert the network management system (NMS) that an error or failure has occurred in XenServer. For more information on how to configure an NMS trap receiver, see Monitoring host and dom0 resources with SNMP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

This section provides information about gathering diagnostics and logs that can help with troubleshooting issues.

- XenCenter Event Log
- Creating a Server Status Report
- Resolving SR Connectivity Problems

To find information about and resolutions for specific issues, search our Knowledge Center on the Citrix support site.

Related documentation

XenServer Current Release

- Troubleshooting

Using the XenCenter® Event Log

XenCenter maintains an event log which can be helpful with troubleshooting. You can view a summary of events in the current XenCenter session by clicking **Notifications** and then **Events**. A much more detailed, permanent record of XenCenter events is stored in a log file in your profile folder. You can use this record to troubleshoot any problems that might arise during the XenCenter session.

Viewing events in the current session

To view the events summary for your current XenCenter session, select **Notifications** and then **Events**.

Viewing the XenCenter event log file

A permanent XenCenter log file (syslog) is generated when you use XenCenter. This file includes a complete description of all operations and errors that occur when using XenCenter. It also contains informational logging of events that provide an audit trail of various actions that have occurred in XenCenter and on your managed resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The XenCenter log file is stored in `%appdata%\XenServer\XenCenter`.

The log output from XenCenter is invaluable when diagnosing problems in your XenServer® environment. To quickly locate the XenCenter log file, from the XenCenter menu, select **Help > View XenCenter Log Files**.

Working with events in the current session

XenCenter enables you to filter events in the current session and perform a specific action to address them. The following table lists the various options available in the **Events** view.

Filter by status

Filters events by their progress

By default, all events for the current XenCenter session are displayed. Select a specific status from the menu to toggle the selection.

Filter by server

Filters events by the source from which they originate

By default, events from all hosts connected to XenCenter are displayed. To stop displaying events from a specific host, select the menu and cancel the selection on the host. Clicking again on the host toggles the selection.

Filter by Date

Filters events based on the time of occurrence

By default, all events for the current XenCenter session are displayed. Select the menu and select a date range from the list. Alternatively, select **Custom** to define your own date range by specifying the start and end date/time.

Dismiss All

Removes events from the Events view

To dismiss or remove all the current events select **Dismiss All**. To dismiss a specific set of events, select the required events from the list, and select **Dismiss Selected**.

Actions

Enables you to perform specific actions on the events displayed

Select an event from the list and then select:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Dismiss** to dismiss the event
- **Go To** to navigate to the host from which the event originated. Selecting this action takes you to the **Infrastructure** view
- **Copy** to copy information about the event to the clipboard

Creating a Server Status Report

The **Server Status Report** wizard provides a convenient way to collect and package a comprehensive snapshot of a specific XenServer® installation for troubleshooting purposes. Options let you include or exclude a range of different configuration files and log files for selected servers.

The server status report gets packaged as a single zip file that can be stored or emailed. The size of the report you generate varies, depending on which items you choose to include. The zip file includes:

- A folder for each server, containing the report types you select in the wizard
- XenCenter® log files

By default, the files gathered for a server status report can be limited in size. If you need log files that are larger than the default, you can run the command `xenserver-status-report -u` in the XenServer server console.

To generate a server status report

On the **Tools** menu, select **Server Status Report** and follow the steps in the **Server Status Report** wizard:

1. **Select Servers**. Select the servers for which you want to collect report data. You can select a pool checkbox to select all the available servers in that pool.

   All available managed servers are listed. If a server is not listed, you might be able to add it to the list by clicking **Add New Server**.
2. **Select Report Contents**. Select the data to include in the report and then select **Next**.
3. **Report Destination**.

   a. Specify the file name for your server status report.

   b. Specify or browse to the folder to save the report in. The destination folder for your server status report must exist and be writable by XenCenter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Select **Next**.

4. **Compile Report**. This page shows the progress of the report compilation and reports any problems with the data collection. When the report compilation is complete, select **Finish** to save the report files to your specified folder and then close the wizard.

After collecting the server status report, you can upload it to Citrix Insight Services. This site can be used to understand the server or pool general health when not facing critical issues.

Related documentation

XenServer Current Release

- Troubleshooting

Resolving SR Connectivity Problems

For a storage repository to be available to a server, a connection must exist between the server and the SR. This connection is provided in software by a Physical Block Device (PBD). A PBD stores information that allows a given SR to be mapped to a server. A PBD must be attached or plugged in to the server for the SR to be available. If a PBD is unplugged for some reason, the SR is no longer available to the server and appears with a broken storage icon in the **Resources** pane.



You might be able to diagnose and resolve some common SR connection problems using the **Repair Storage Repository** tool. In the **Resources** pane, select the storage resource, right-click, and select **Repair Storage Repository** on the shortcut menu.

Alternatively, on the **Storage** menu, select **Repair Storage Repository**.

The available storage repositories are listed, and you can see their status.

- **Connected**. The connection between the SR and the server is working normally and the storage provided by the SR is available.
- **Unplugged**. The storage is unavailable because the PBD is unplugged.
- **Connection missing**. The storage is unavailable because the PBD cannot be found.

Select **Repair** to have XenCenter® attempt to repair the storage. Progress and results are displayed within the **Repair Storage Repository** dialog box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related documentation

XenServer Current Release

- Manage storage repositories

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Getting Help

There are several different places you can find the information you need about using XenServer and XenCenter®:

- **XenCenter product documentation**. Comprehensive reference documentation aimed at XenCenter users.
- **XenServer product documentation**. Comprehensive reference documentation aimed at XenServer administrators and developers.
- **Citrix Knowledge Center**. Browse or search for knowledge base articles and technical notes.
- **Citrix Tech Zone**. Citrix Tech Zone is home to technical, in-depth articles inspired and driven by technical communities and enthusiasts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

XenCenter® Document History

The following table describes important changes to the XenCenter product documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	DESCRIPTION
03 Aug 2026	New release: XenCenter 2026.4.1	This release includes enhancements and bug fixes. For more information, see What's new in XenCenter.
14 Jul 2026	New release: XenCenter 2026.4.0	This release includes security fixes. For more information, see the Security Bulletin.
25 Jun 2026	New release: XenCenter 2026.3.0	This release includes new features and bug fixes. For more information, see What's new in XenCenter.
01 Jun 2026	New release: XenCenter 2026.2.1	This release includes several improvements and bug fixes. For more information, see What's new in XenCenter.
29 Apr 2026	New release: XenCenter 2026.2.0	This release offers certificate validation for the License Server and a number of enhancements and bug fixes. For more information, see What's new in XenCenter.
09 Mar 2026	New release: XenCenter 2026.1.0	This release focuses on improved Active Directory lockout handling, providing the ability to limit VM/Host console sessions to 1 and general security and stability enhancements. For more

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	DESCRIPTION
		information, see What's new in XenCenter.
08 Dec 2025	New release: XenCenter 2025.5.0	XenCenter 2025.5.0 released. For more information, see What's new in XenCenter.
23 Oct 2025	New release: XenCenter 2025.4.0	XenCenter 2025.4.0 released. For more information, see What's new in XenCenter.
11 Aug 2025	New release: XenCenter 2025.3.0	This release includes the easier pool join feature. For more information, see What's new in XenCenter.
18 Jun 2025	New release: XenCenter 2025.2.1	XenCenter 2025.2.1 released. For more information, see What's new in XenCenter.
07 May 2025	New release: XenCenter 2025.2.0	XenCenter 2025.2.0 released. For more information, see What's new in XenCenter.
03 Mar 2025	New release: XenCenter 2025.1.0	XenCenter 2025.1.0 released. For more information, see What's new in XenCenter.
05 Dec 2024	New release: XenCenter 2024.4.0	XenCenter 2024.4.0 released. For more information, see What's new in XenCenter.
10 Oct 2024	New release: XenCenter 2024.3.1	XenCenter 2024.3.1 released. For more

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	DESCRIPTION
		information, see What's new in XenCenter.
25 Sep 2024	New feature: anti-affinity VM placement groups	The VM placement groups feature is now available in XenCenter. For more information, see Manage VM groups.
22 Aug 2024	New release: XenCenter 2024.3.0	XenCenter 2024.3.0 released. For more information, see What's new in XenCenter.
09 Jul 2024	New release: XenCenter 2024.2.1	XenCenter 2024.2.1 released. For more information, see What's new in XenCenter.
06 Jun 2024	New release: XenCenter 2024.2.0	This release includes the ability to import a VHDX or AVHDX disk image as a VM. For more information, see What's new in XenCenter.
26 Mar 2024	XenCenter 2024.1.0 is GA with XenServer 8.4	The latest version of XenCenter is now supported in production with XenServer 8.4. For more information, see What's new in XenCenter.
06 Mar 2024	New release of XenCenter	XenCenter 2024.1.0 released. This update includes changes to licensing, improved update guidance, and monitoring with SNMP. For more information, see XenCenter current release.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	DESCRIPTION
04 Dec 2023	New release of XenCenter	XenCenter 2023.4.0 (preview) released. For more information, see XenCenter current release.
05 Oct 2023	New release of XenCenter	XenCenter 2023.3.2 (preview) released. For more information, see XenCenter current release.
24 Aug 2023	Use XenCenter to apply frequent updates to XenServer	New features and bug fixes are frequently made available to you in XenCenter, allowing you to benefit from a more efficient release process that delivers new content to you at a faster cadence than was previously possible. For more information, see Update your XenServer hosts.
24 Aug 2023	XenCenter quick updates	XenCenter updates can be downloaded and applied from within the UI. For more information, see Updating XenCenter.
24 Aug 2023	PuTTY is no longer bundled with XenCenter	To launch an SSH console to a XenServer host by using XenCenter, you must install an external SSH console tool and ensure that XenCenter is configured to use it. For more information, see Configure XenCenter to use an external SSH console.
24 Aug 2023	New release of XenCenter	XenCenter 2023.3.1 (preview) released. For more information, see XenCenter current release.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.

© 1997–2026 Citrix Systems, Inc. All rights reserved.