Virtual Server Protection (VSP)
Version 11 Service Pack 11

Thursday, April 12, 2018
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Creating a Life Cycle Policy ............................................................................................................ 132

Plans .................................................................................................................................................. 134
Server Plans ...................................................................................................................................... 135
Creating a Server Plan ....................................................................................................................... 136
Modifying a Server Plan .................................................................................................................... 137
Snap Plans .......................................................................................................................................... 137
Creating a Snap Plan ......................................................................................................................... 138
Adding a Microsoft Hyper-V Hypervisor to an Array ....................................................................... 139
Adding a VMware Hypervisor to an Array ....................................................................................... 140
Adding a Server to an Array ............................................................................................................... 141
Editing the Backup Copy Schedule of a Snap Plan ........................................................................... 141
Editing the Security Section of a Snap Plan ...................................................................................... 142
Adding a Storage Array to the CommServe Database ...................................................................... 142
Storage Pool ..................................................................................................................................... 143

Monitoring ........................................................................................................................................ 144
Alerts ................................................................................................................................................ 144
Creating an Alert Definition ............................................................................................................... 144
Editing Alert Definitions .................................................................................................................... 145
Viewing Triggered Alerts ................................................................................................................... 145
Deleting Triggered Alerts .................................................................................................................. 145
Alert Information for Triggered Alerts .............................................................................................. 146
Viewing Events ................................................................................................................................. 146
Jobs .................................................................................................................................................... 147
Controlling Activities ....................................................................................................................... 147
Controlling Jobs ................................................................................................................................. 147
Viewing Jobs ..................................................................................................................................... 148

Copyright © 2018 Commvault Systems, Inc. All rights reserved.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Sending Log Files ................................................................. 148
Job Information ................................................................. 149

Storage Targets ..................................................................... 151
Configuring a Disk Library as a Storage Target ...................... 151
Adding a Mount Path ............................................................ 152
Configuring a Cloud Library as a Storage Target ...................... 153
Cloud Provider Information .................................................... 154
Configuring a Tape Library as a Storage Target ....................... 157
Exporting Media ................................................................. 158
Resetting a Library ............................................................. 158
Deconfiguring a Library ......................................................... 159
Validating a Drive ............................................................... 159
Cleaning a Drive ................................................................. 160
Unloading a Drive ............................................................... 160
Resetting a Drive ............................................................... 161
Reports for Tape Storage Targets ........................................... 161

User Security Settings ......................................................... 163
Updating Your Password ..................................................... 163
Users and User Groups ....................................................... 163
Creating a User ................................................................. 164
Managing Users ............................................................... 164
Creating a User Group ......................................................... 164
Managing User Groups ....................................................... 165
Managing User Group Membership ....................................... 165

Copyright © 2018 Commvault Systems, Inc. All rights reserved.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Adding Domains ................................................................. 166
Managing Roles ................................................................. 167
Adding Identity Servers ....................................................... 167
  Sample SAML IdP Metadata XML .................................... 169
  Sample SAML SP Metadata XML .................................... 169
Creating Certificates for SAML Integration ................................. 170
Identity Provider Use Cases ................................................ 173
Administering the Security Associations of a Server ..................... 180

System Settings ......................................................................... 181
Applying a License ............................................................... 181
Creating Global Exceptions ................................................... 181
Creating a Backup Window ..................................................... 182
Configuring an Email Server ............................................... 182
Configuring Private Metrics Reporting .................................... 183
  Uploading Data for Cloud Metrics Reporting ...................... 184
Configuring Cloud Metrics Reporting ..................................... 184
  Uploading Data for Cloud Metrics Reporting ...................... 185
Registering the Admin Console .............................................. 186

Commvault Enterprise Software ................................................ 186

Index ................................................................................. 191
Introduction to Virtual Server Protection (VSP)

Virtual Server Protection (VSP) can be deployed as an all-in-one data protection and recovery solution for virtual machines. The VSP package contains all components that are required to protect virtual machines in a compact configuration that can be used for evaluation and to provide ongoing protection.

Virtual Server Protection uses the Admin Console, a web-based interface that enables you to back up virtual machines running on VMware or Microsoft Hyper-V, restore data from virtual machines, and manage protection operations.

To get started quickly, you can perform simple configuration of virtual machine servers, storage, and virtual machine collections in a few minutes, then initiate protection operations immediately. You can use the Admin Console, dashboard to initiate backups and restores, provide summary information about virtual machine protection, and manage jobs, schedules, alerts, events, and users.

Support

To schedule a review session with a Systems Engineer to conduct a product overview, discuss best practices, design concepts, or general administration, or if you are having issues installing the software or are receiving error messages that require assistance, please submit a request to VM@commvault.com (Mailto:VM@commvault.com).

Key Features

- Includes all components required to protect virtual machines in a VMware vCenter or ESX server, or in cluster shared volume (CSV) storage attached to Hyper-V servers.
- Provides a Setup wizard to configure host connectivity, storage, and backups in a matter of minutes, and back up selected virtual machines immediately.
- Performs off-host backups for virtual machines to support continuity of operations and disaster recovery.
- Provides granular backup and recovery options.
- Enables scheduled backup and restore jobs; virtual machines are automatically protected without user intervention.
- Provides source-side or target-side deduplication to reduce backup storage requirements and network traffic.
- Includes advanced configuration and management options.
- Includes monitoring and reporting tools for intelligent VM data analytics.

Additional features for Microsoft Hyper-V:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Enables backups of Hyper-V nodes without requiring that an agent be installed in each node.
- Includes automatic cluster awareness with full integration of CSVs and Live Migration protection for VMs that migrate to a new node.
- Provides application-consistent protection to enable rapid recovery of applications running inside virtual machines.

Buying VSP or Extending Your VSP License

You can upgrade VSP to the full Commvault product. Contact your account team to obtain the appropriate license.

You can extend your VSP license by sending an email to Commvault Customer Support at prodreg@commvault.com. Include the IP address of the backup server. The IP address for the backup server is shown in the License Expiration Warning that is presented when you start the CommCell Console.

To transfer information from VSP to a production environment using different servers, see CommServe Hardware Refresh (https://documentation.commvault.com/commvault/v11/article?p=products/commserve/hardware_refresh_prereq.htm).

Installing the Virtual Server Protection Package

Use the Virtual Server Protection package to set up a CommCell environment for protecting virtual machines.

This package includes the following Commvault software: CommServe, Admin Console, Virtual Server Agent, MediaAgent, CommCell Console, Web Server, Web Console, and Workflow Engine.

Before You Begin

- Download the Virtual Server Protection installer from the Media Kits (https://store.commvault.com/webconsole/softwarestore/store.do#!/home/130) area of the Commvault Store.
- Verify that the computer where you plan to install the package satisfies the minimum requirements specified in System Requirements (on page 9).

Procedure

1. Start the Virtual Server Protection installer, select where to extract the installation files, and then click Extract.
2. On the welcome page, select the I Agree check box and proceed to the next page.

3. On the Choose the Installation Type page, click Install packages on this computer and proceed to the next page.

4. On the Installation Path page, change the default path if you want to install the software on a different location, and then proceed to the next page.

The installation starts.

5. Complete the steps in the installation wizard.

6. On the completion page, make a note of the Admin Console URL and then click Finish.

What to Do Next

Provide the Admin Console URL to backup administrators, database administrators, and other users that might need to access the console.

To get started with the Virtualization application, see Getting Started with Virtualization (on page 12).

System Requirements for Virtualization

Review the following requirements for the Virtual Server Protection (VSP) package.

General Package Requirements

The computer on which you plan to install the package must satisfy the following system requirements:

| Operating Systems | • Microsoft Windows Server 2016 x64 Editions  
|                   | • Microsoft Windows Server 2012 R2 x64 Editions  
|                   | • Microsoft Windows Server 2012 x64 Editions  
|                   | • Microsoft Windows Server 2008 x64 Editions  
| Hard Drive | 500 GB recommended. Depending upon the number of virtual machines that you are planning to backup, ensure that the backup server computer has sufficient free space to store all virtual machine data.  
| Memory | 16 GB RAM minimum required  
| Processor | All Windows-compatible processors supported  
| IIS | IIS must be enabled on the backup server.  

Supported Web Browsers for the Admin Console

You can run the Admin Console on the following browsers:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Apple Safari version 8.0 and later
- Google Chrome v40 and later
- Microsoft Edge
- Microsoft Internet Explorer (IE) v10 or later
- Mozilla Firefox v47.0 or later

Accessing the Admin Console

You can access the Admin Console by using the URL that your administrator provides.

CommCell administrators and Tenant administrators can also access the Admin Console from the My Applications page on their Web Console.

Procedure

1. Go to the Admin Console URL that your administrator provided.
   The URL has the following format: http://webhost/adminconsole.
2. Type your user name and password.
3. Optional: To remain logged on, select the Stay Logged In check box.
   If you do not select the Stay Logged In check box, you are automatically logged out after 30 minutes.
4. Click Login.

Result

The first time you log on, the software prompts you to configure core information by completing the Core Setup Wizard (on page 10).

What to Do Next

Refer to the documentation that corresponds to the solution that you want to use, for example, Virtualization (on page 11).

If you want to switch between solutions, from the navigation pane, click Solutions, and then select the solution that you want to use.

Completing the Core Setup Wizard

When you log on to the Admin Console for the first time, a setup wizard guides you through the core setup required by the applications available in the Admin Console. After you complete the core setup, you can complete the setup wizards specific to the applications you need.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

The core setup includes the following:

- Registering your product
- Configuring an email server
- Adding storage

Information you will need to complete the core setup wizard:

- An account on the Commvault Cloud website https://cloud.commvault.com
- The name and port number of your email server
- The location of the disk library where you want to store backed up data

What to Do Next

In an application tile, click **Complete setup** to start the setup wizard for a specific application. For example, to start the setup wizard for the Virtualization application, click **Complete setup** in the **Virtualization** tile. For a list of available applications, see Commvault Solutions for Data Protection and Recovery.

Virtualization

The Virtual Server Protection (VSP) package is a solution for virtual machine backup and recovery. The Virtualization application streamlines the process of backing up virtual machines, restoring virtual machine data, and monitoring protection operations.

To get started quickly, you can perform simple configuration of virtual machine hypervisors, storage, and virtual machine subclients in a few minutes, then run backups immediately. You can initiate backups and restores, get information about virtual machine protection, and manage jobs, schedules, alerts, events, and users.

If the Virtualization application is not displayed when you open the Admin Console, select **Solutions > Virtualization** from the navigation pane. This option is only available after you have completed the setup for Virtualization (on page 14).

Key Features

- Protect virtual machines for the following hypervisors:
  - Amazon
  - Google Cloud Platform
  - Microsoft Azure
  - Microsoft Azure Stack
  - Microsoft Hyper-V
  - Nutanix Acropolis Hypervisor (AHV)
  - OpenStack
  - Oracle Cloud Infrastructure Classic
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Oracle VM
- VMware (vCenter or ESX server)

- Quickly configure hypervisors, storage, and subclients (collections of virtual machines) to back up.
- Back up virtual machines immediately or by using a defined schedule. You can also back up individual VMs on demand.
- Restore full virtual machines, disks, and guest files with granular backup and recovery options.
- Use the dashboard view to monitor jobs, events, and alerts.

Getting Started with Virtualization

This topic describes the high-level steps that first-time users must follow to set up the Virtualization application in the Admin Console.

Step 1: Install the Virtual Server Protection package

To access the Virtualization application, the administrator must install the Virtual Server Protection package. For instructions, see Installing the Virtual Server Protection Package (on page 8).

Step 2: Log onto the Admin Console

Access the Admin Console (on page 10) using the URL that was provided by the administrator.

Step 3: Complete the Core Setup Wizard

Configure core information by completing the Core Setup Wizard (on page 10).

Step 4: Complete the Virtualization Application Wizard

Perform initial configurations to set up the Virtualization application by completing the Virtualization Setup (on page 14).

During the setup, you will add a hypervisor, configure storage, add virtual machines, and perform other important configurations.

Step 5: Perform Your First Backup and Restore

For instructions, see the following procedures:
1. Perform a backup (on page 85).
2. Restore full virtual machines or files and folders (on page 87).
Step 6: What to Do Next

After initial setup, you can perform the following tasks to customize your operations:

- Add additional hypervisors (on page 22).
- Add subclients (on page 37) for different virtual machines to match the desired service level agreement (SLA) for each group.
- Define rules to include (on page 40) or exclude (on page 45) virtual machines for subclients.
- Edit subclient options (on page 51) to modify backups.

Virtual Server Agent (VSA) Requirements

The VSA is installed on computers that can perform backup and restore operations for a specific hypervisor platform.

- For Amazon, the VSA is installed on a machine or an Amazon instance that can connect to ec2.amazonaws.com. For backups, the VSA must be installed on an Amazon instance in each region to be protected. Each VSA proxy can protect instances in the same region. For VM conversion and restores, the VSA can be installed on an Amazon instance or on an external machine.

- For Microsoft Azure, the VSA can be installed on one or more machines or Azure virtual machines. Any machine where the VSA is installed can act as a VSA proxy to perform backups and restores. For best results, deploy the VSA proxy on a virtual machine in the Azure cloud. A VSA proxy for Azure Classic must have an Azure management certificate installed. Deploying the VSA proxy on an Azure VM that is optimized for I/O intensive workloads will support faster backups. If the Azure subscription includes multiple regions, deploy at least one VSA proxy per region.

- For Microsoft Hyper-V support, the VSA is installed on a standalone Hyper-V server or on a node in the Hyper-V cluster. If the Virtual Server Agent is not installed on a Hyper-V node that is selected as a VSA proxy, the Virtual Server Agent and additional software must be pushed to that machine during Virtualization setup.

- For Nutanix Acropolis AHV support, the VSA is installed on a virtual machine in the Nutanix cluster.

- For OpenStack, the VSA is installed on an instance in the OpenStack data center.

- For Oracle Cloud Classic, the VSA is installed on an Oracle Cloud Classic instance.

- For Oracle VM, the VSA is installed on a virtual machine in the Oracle VM Manager environment.

- For VMware support, the VSA is installed on one or more physical computers or virtual machines.

When installing the Admin Console with an existing Commvault deployment, ensure that the following requirements are met:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- At least one machine must have the Virtual Server Agent installed.
- To add Hyper-V servers, the CommServe system must have the Virtual Server Agent installed.

Virtual Machine Support

In general, the VSA supports backup and recovery for guests running any of the operating systems supported by the hypervisor platform.

VMware

For VMware, the VSA has the following requirements for guest virtual machines:

| Virtual Machine Host | The following versions are supported for vSphere, vCenter, vCenter Server Appliance, and ESX/ESXi: 4.1 or later, 5.0.x, 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 5.5.6, 6.0, 6.0.1, 6.0.2, 6.0.3, 6.5  
For any ESXi servers, the VADP is not available in the free version of ESXi. The Essentials licensing level or higher is required. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine Hardware Version</td>
<td>4.0, 7.0, 8.0, 9.0, 10.0, 11.0, 13.0</td>
</tr>
<tr>
<td>Virtual Machine Operating Systems</td>
<td>All Guest Operating Systems supported by VADP</td>
</tr>
<tr>
<td>VMware Tools on Virtual Machines</td>
<td>Install the latest version of VMware Tools supported by the host on each virtual machine. At a minimum, the version of VMware tools on virtual machines must also be supported on the host; unsupported versions must be upgraded.</td>
</tr>
</tbody>
</table>

Using the Setup Wizard for the Virtualization Application

When you log on to the Admin Console for the first time, a setup wizard guides you through the core setup (on page 10) required by the applications available in the Admin Console. After you complete the core setup, complete the setup wizard specific to the Virtualization application.

Before You Begin

- Complete the Core Setup Wizard (on page 10).
- You will need the following information to complete the setup wizard for the Virtualization application:
  - The access point and credentials for at least one hypervisor.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- For Hyper-V, one or more nodes on which you will install the Virtual Server Agent (VSA) to create proxies for backup and restore operations.

To use Changed Block Tracking for Hyper-V 2012 R2, select all nodes in the Hyper-V cluster.

- At least one machine must have the VSA installed. If you installed the Virtual Server Protection package on a backup server, the VSA is included with that installation.

- To discover Hyper-V servers, the CommServe system must have the VSA installed. If you installed the Virtual Server Protection package on a backup server, the VSA is included with that installation.

- For the Nutanix Acropolis Hypervisor (AHV), a VSA proxy must be installed on a virtual machine in the Nutanix cluster. If you installed the Virtual Server Protection package on a VM in the Nutanix cluster, the VSA is included with that installation.

About This Task

At any point during the setup wizard, click Finish setup later to leave the wizard. If you leave the setup wizard before it is complete, it will appear the next time you log on.

Procedure

Perform the following steps to configure email, hypervisor, storage, and virtual machine information.

1. After you complete the core setup, in the Virtualization tile, click Complete setup.

2. On the Add server backup plan page, type a name for the plan, then provide information about storage, retention, and backup schedules. For more information, see Creating a Server Plan (on page 136).

3. Click Save.

   The Add hypervisor page appears. The options vary depending on the hypervisor type you select.

4. Provide the following information:

   b. Hypervisor name or Client name: Enter a descriptive name for the hypervisor.

   c. Enter host or account information:
      ▪ Amazon:

         Access key: Type the Access Key ID that is associated with your Amazon EC2 account.

         Secret key: Type the Secret Access Key that is associated with your Amazon EC2 account.

      ▪ Microsoft Azure Classic or Azure Resource Manager:

         Subscription ID: Enter the subscription ID for your Azure account.

      ▪ Microsoft Azure Classic:

         Thumbprint: Enter the thumbprint for the Azure management certificate.

      ▪ Microsoft Azure Resource Manager:

         Tenant ID: Enter the tenant ID associated with the Azure account.
Application ID: Enter the application ID associated with the tenant.

Application password: Enter the password for the application.

- Microsoft Hyper-V:
  
  **Hostname / IP address:** Provide a fully qualified hostname or IP address for the hypervisor.
  
  **Username** and **Password:** Enter the user credentials to provide administrative access to the hypervisor.

- Nutanix AHV:
  
  **Hostname / IP address:** Provide a fully qualified hostname or IP address for the hypervisor.
  
  **Username** and **Password:** Enter the user credentials to provide administrative access to the hypervisor.

- OpenStack:
  
  **Keystone Address:** Enter the fully qualified host name or IP address for the keystone node. If there are multiple endpoints for the keystone URL, use the public endpoint.
  
  **User name:** Enter the user name for the keystone node user with administrator privileges.
  
  **OpenStack Domain** (optional): If a domain is configured in the OpenStack environment, enter the domain for the keystone node user.
  
  **Password:** Enter the password for the user account.

- Oracle Cloud Classic:
  
  **End point:** Enter the fully qualified domain name (FQDN) for the endpoint that is used to access Oracle Cloud Classic.
  
  **Identity domain/username:** Enter the domain and user name required to access the endpoint.
  
  **Password:** Enter the password for the user account.

- Oracle VM:
  
  **Oracle VM Manager:** Enter the fully qualified host name or IP address for the Oracle VM Manager.
  
  **User name:** Enter the user name required to access Oracle VM Manager.
  
  **Password:** Enter the password for the user account.

- VMware:
  
  **Hostname / IP address:** Provide a fully qualified hostname or IP address for the hypervisor.
  
  **Username** and **Password:** Enter the user credentials to provide administrative access to the hypervisor.

  d. **Proxy** (Amazon, Azure, Nutanix AHV, OpenStack, Oracle Cloud Classic, or Oracle VM): Select a pre-installed proxy from the Proxy list:
     
     - Amazon: Select an Amazon instance in the region to be protected.
     - Azure: Select an Azure virtual machine in the region to be protected.
     - Nutanix AHV: Select a pre-installed proxy in the Nutanix cluster.
     - OpenStack: Select a previously deployed proxy that is an instance in the OpenStack data center.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Oracle Cloud Classic: Select a previously deployed proxy that is an Oracle Cloud Classic instance.
- Oracle VM: Select a previously deployed proxy that is a virtual machine hosted on an Oracle VM Server.

For VMware, the backup server is automatically selected as a default proxy.

e. For a Hyper-V server, click Discover nodes. When the Proxies field is populated, select one or more nodes on which to install the Virtual Server Agent.

**Note:** You can continue the setup process while the VSA is being installed on Hyper-V nodes, but you cannot perform backups until that installation is complete.

For more information, see Adding a Hypervisor (on page 22).

5. Click **Save**.

6. On the **Add subclient** page, type a descriptive name to identify the subclient, and then select virtual machines to be protected. For more information, see Adding a Subclient (on page 37).

7. Click **Save**.

8. To finish, choose one of the following options:
   - Click **Back up Now** to perform an immediate backup of the virtual machines in the subclient (without requiring confirmation).
     
     The **Job details** page appears and displays job status information.
   - Click **Do it later** to go to the hypervisor page without performing a backup.

**Note:** For Hyper-V, the **Back up Now** option might not be available immediately. You can go to the hypervisor page.

When VSA installation on proxies is complete, perform a backup (on page 85).

Using the Virtualization Dashboard to Manage Data Protection

The Virtualization Dashboard displays summary information about data protection for virtual machines. You can use the dashboard to understand the current status of operations and to go to detail pages.

1. From the navigation pane, click **Dashboard** to view the Virtualization Dashboard.

   The top row of the dashboard provides summary information for key items.

2. Click the text label under any of these items to view details:
   - **No of Hypervisors** (on page 32): Number of hypervisors hosting virtual machines.
   - **No of Protected VMs** (on page 129): Number of virtual machines that have been backed up.
   - **Critical Alerts** (on page 146): Critical alerts in the last 24 hours
   - **Critical Events** (on page 146): Critical events in the last 24 hours

3. In the second row, click in a graphic to get detailed information:
Configuration for Virtualization

The first time you log on, you are prompted to add a hypervisor, configure storage, and identify virtual machines to back up as described in Using the Virtualization Setup Wizard (on page 14).

To support ongoing operations, you can add hypervisors, subclients, storage, and users.

For VMware and Hyper-V subclients, you can enable IntelliSnap backups by creating a Snap plan (on page 138) and adding the Snap plan to a subclient. For more information, see Snap Plans (on page 137).

Security Configuration for Virtualization

The Admin Console has predefined user groups and roles that you can use to manage security for users, hypervisors, subclients, and virtual machines.

User Groups

By default, the Admin Console has the following user groups:

- Administrator
- Backup operator
- Restore operator
- View All

Roles

Roles define a set of permissions. By associating roles, user groups, and users with a particular hypervisor, you can control access to the hypervisor and grant permissions to perform actions. By default, the Admin Console has the following roles:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Administrator_Role
- Alert Creator
- Alert Owner
- All Users Laptops
- Backup operator_Role
- Client Admins
- Compliance
- End Users
- Master
- MSP Subscription: Only for MSP administrators managing a multi-tenant environment.
- Plan Creator Role
- Plan Subscription Role
- Restore operator_Role
- View

Virtualization Requirements

For hypervisors, subclients, or virtual machines, you can associate users or groups with roles to determine what actions users can perform. You can also assign users or groups as owners who have management permissions for those entities.

You can use predefined roles, modify predefined roles, or create new roles.

In general, the following permissions are required for general administrative users for virtualization:

- All Alert permissions
- The following Client permissions are required:
  - Agent Management
  - Agent Scheduling
  - Install Package/Update
  - Data Protection/Management Operations
  - Browse
  - In Place Recover
  - Out-of-Place Recover
  - In Place Full Machine Recovery
  - Out of Place Full Machine Recovery
  - Overwrite on restore
- The following Commcell permissions are required:
  - License Management
  - Install Client
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- The following Global permissions are required:
  - Administrative Management
  - Job Management
  - Alert Management
  - View
  - Change security settings
  - Events Organizer
- All Plan permissions
- All Schedule Policy permissions
- All Storage Management permissions
- All User Management permissions

Note: In a multi-tenant environment, you should also include all Workflow permissions for VSA administrators.

Security Configuration for End Users

The following permissions are required to backup VMs, browse VM data, and restore VMs or VM files. For detailed information about security, see User Security Settings (on page 163).

Client permissions:
- **Data Protection/Management Operations**: Perform backups for their own VMs.
- **Browse**: Browse virtual machine data.
- **In Place Recover**: Recover files and folders to the source VM.
- **Out-of-Place Recover**: Recover files and folders to a different location.
- **In Place Full Machine Recovery**: Recover a full VM to the original location (requires **Overwrite on Restore** permission).
- **Out of Place Full Machine Recovery**: Recover a full VM to a different location.
- **Overwrite on Restore**: Overwrite the original VM with the restored VM.

Configuring a Firewall for a VSA Proxy in the Cloud

For Amazon or Microsoft Azure, you can configure a firewall to communicate with a VSA proxy running in Amazon or Azure.
Before You Begin

- In the CommServe system for the Admin Console (the backup server), firewalls must be enabled in the Firewall Configuration tab of the CommCell Properties.

Procedure

1. From the navigation pane, click Servers.
2. Click the name of the Amazon or Azure server for which you are adding a gateway.
3. In the Proxy area, click Configure Proxy.
   
   The Add Proxy dialog box appears.
4. In the Host Name box, enter the public IP address for the VSA proxy.
5. In the Client Name box, enter a descriptive display name for the gateway.
6. Click Save.

   Adding a proxy creates a client for the VSA proxy, adds the client to the Firewall Topologies > Proxy Clients group in the CommCell Console, and pushes the firewall configuration to the CommServe system.

   You receive an email notification with the steps to install the proxy package on your client computer.

7. Go to the Virtualization section of the Commvault Store (https://store.commvault.com/webconsole/softwarestore/store.do#!/home), download the VSA Proxy Firewall package, and copy it to the VSA proxy machine.
8. Connect to the VSA proxy machine and log on.
9. Ensure that tunnel port 8403 is open on the VSA proxy machine for communications from the backup server.
10. Install the VSA Proxy Firewall package on the VSA proxy machine.

   The notification email includes the information to include when installing the proxy:
   
   - Client Name: Use the gateway client name that you entered when adding the proxy in the Admin Console.
   - Host Name: Use the host name that you entered when adding the proxy in the Admin Console.
   - CommServe Client Name: Use the client name of the CommServe system for the Admin Console. Enter the short name, not including the domain name.

11. After the install completes successfully, return to the Admin Console.
12. From the navigation pane, click Servers.
13. Click the name of the Amazon or Azure server for which you are adding a gateway.
15. Select the proxy that you created in this procedure.
16. Click OK.
Hypervisors

Hypervisors provide hosting for virtual machines. You can include hypervisors for different virtualization platforms in the same Admin Console implementation:

- Amazon: The hypervisor represents an Amazon Web Services (AWS) account.
- Google Cloud Platform: A hypervisor represents a Google Cloud service account.
- Microsoft Azure - Classic: A hypervisor represents an Azure subscription.
  - Microsoft Azure - Resource Manager: A hypervisor represents an application.
- Microsoft Azure Stack: A hypervisor represents an Azure subscription.
- Microsoft Hyper-V: A hypervisor represents a Hyper-V cluster, a Hyper-V server in a cluster, or a standalone Hyper-V server.
- Nutanix Acropolis AHV: A hypervisor represents a Nutanix cluster.
- OpenStack: A hypervisor represents a keystone node in an OpenStack deployment.
- Oracle Cloud Infrastructure Classic: A hypervisor represents an Oracle Cloud Infrastructure Classic endpoint.
- Oracle VM: A hypervisor represents an Oracle VM Manager.
- VMware: A hypervisor represents a vCenter or a standalone ESX server.

The main Hypervisors page shows all of the hypervisors in your environment. You can click on any hypervisor to get summary information, or click on a Jobs link in the Actions column to check the status of jobs for a hypervisor. Some users may only have access to specific hypervisors for which they are responsible.

For each hypervisor, you can define subclients (collections of virtual machines) that you want to manage separately. For example, you can put virtual machines in different subclients so that you can have different backup criteria or schedules for different classes of virtual machines.

Adding a Hypervisor

Add a hypervisor to support data protection operations for all virtual machines hosted or managed by the hypervisor.

The following hypervisors are supported:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Amazon
- Google Cloud Platform
- Microsoft Azure Classic or Azure Resource Manager
- Microsoft Azure Stack
- Microsoft Hyper-V
- Nutanix Acropolis Hypervisor (AHV)
- OpenStack
- Oracle Cloud Infrastructure Classic
- Oracle VM
- VMware

**Adding an Amazon Hypervisor**

Add an Amazon hypervisor to support data protection operations for all virtual machines hosted or managed by the hypervisor.

**Before You Begin**

The hypervisor represents an Amazon Web Services (AWS) account.

Be prepared to enter a key pair (Access Key and Secret Key) obtained from the Amazon EC2 website section on Security Credentials.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.  
   The **Hypervisors** page appears.
2. Click **Add hypervisor**.
3. For **Select type**, select **Amazon**.
4. For **Hypervisor name** or **Client name**, type a descriptive name for the hypervisor.
5. Enter host or account information:
   - **Access key**: Type the Access Key ID that is associated with your Amazon EC2 account.
   - **Secret key**: Type the Secret Access Key that is associated with your Amazon EC2 account.
6. From the **Proxy** list, select a previously deployed Amazon instance in the region to be protected.
7. Click **Save**.
Adding a Google Cloud Platform Hypervisor

Add a Google Cloud hypervisor to support data protection operations for all instances hosted or managed by the hypervisor.

Before You Begin

- Create a Google Cloud Platform service account and download a P12 private key.
  The user who creates the Google Cloud Platform service account must have the Owner role assigned.
- Make a note of the service account ID, project ID, P12 key file name, and P12 key password.
- Place the P12 private key in the base certificates folder for Google Cloud Platform: `<base folder>/certificates/external`
  If the `\Base\certificates\external` folder does not already exist, create the folder.
- There must be one Virtual Server Agent (VSA) proxy for each Google Cloud Platform service account.
  You can add more VSA proxies as needed.

Procedure

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   The Hypervisors page appears.
2. Click **Add hypervisor**.
3. For **Select type**, select the following:
   - Google Cloud Platform
4. For **Client name**, type a descriptive name for the hypervisor.
5. Enter the Google Cloud Platform **Project ID**.
6. Enter the Google Cloud Platform **Service Account ID**.
7. Enter the Google Cloud Platform **P12 Key File Name**.
   The P12 file should reside in the following location on the proxy computer: `<Base-folder>/certificates/external`
8. Enter the Google Cloud Platform **Private Keys Password**.
9. From the **Proxy** list, select a previously deployed proxy.
   The VSA proxy must be a Google Cloud Platform instance in the region to be protected.
10. Click **Save**.

Adding a Microsoft Azure Hypervisor

Add a Microsoft Azure hypervisor to support data protection operations for all virtual machines hosted or managed by the hypervisor.
**Before You Begin**

You will need the following information to add a hypervisor:

- For Azure Classic deployments, the hypervisor represents an Azure subscription.
  - Be prepared to enter an Azure subscription ID and thumbprint.
- For Azure Resource Manager deployments, the hypervisor represents an application.
  - Be prepared to enter a subscription ID, tenant ID, application ID, and application password.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**. The Hypervisors page appears.
2. Click **Add hypervisor**.
3. For **Select type**, select one of the following:
   - **Azure - Classic**
   - **Azure - Resource Manager**
4. For **Hypervisor name** or **Client name**, type a descriptive name for the hypervisor.
5. Enter host or account information:
   - **Subscription ID**: Enter the subscription ID for your Azure account.
   - **Thumbprint**: Enter the thumbprint for the Azure management certificate.
   - **Tenant ID**: Enter the tenant ID associated with the Azure account.
   - **Application ID**: Enter the application ID associated with the tenant.
   - **Application password**: Enter the password for the application.
6. From the **Proxy** list, select a previously deployed proxy
   - The VSA proxy must be an Azure virtual machine in the region to be protected.
7. Click **Save**.

**Adding a Microsoft Azure Stack Hypervisor**

Add a Microsoft Azure Stack hypervisor to support data protection operations for all virtual machines hosted or managed by the hypervisor.
Before You Begin

Be prepared to enter a subscription ID, tenant ID, application ID, and application password.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.
2. Click Add hypervisor.
3. For Select type, select the following:
   o Azure - Stack
4. For Hypervisor name or Client name, type a descriptive name for the hypervisor.
5. Enter host or account information:
   o Subscription ID: Enter the subscription ID for your Azure account.
   o Tenant ID: Enter the tenant ID associated with the Azure account.
   o Application ID: Enter the application ID associated with the tenant.
   o Application password: Enter the password for the application.
6. From the Proxy list, select a previously deployed proxy
   The VSA proxy must be an Azure virtual machine in the region to be protected.
7. Click Save.

Adding a Microsoft Hyper-V Hypervisor

Add a Microsoft Hyper-V hypervisor to support data protection operations for all virtual machines hosted or managed by the hypervisor.

Before You Begin

You will need the following information to add a hypervisor:

- The hypervisor can be a Hyper-V cluster, a Hyper-V server in a cluster, or a standalone Hyper-V server.

  Be prepared to enter credentials for the Hyper-V server or cluster. The user must belong to the local administrators group for Hyper-V Server 2008 R2 or the Hyper-V administrators group for Hyper-V Server 2012 and later. For a Hyper-V cluster, the user account must have full cluster permissions (Read and Full Control).
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Also identify one or more nodes on which you will install the VSA to create proxies for backup and restore operations.

Considerations

You can install the Commvault System Center plug-in to manage backups and recovery of Hyper-V virtual machines from within System Center.

For more information, see Installing and Launching the System Center Plug-In (on page 27).

Procedure

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
   The **Hypervisors** page appears.

2. Click **Add hypervisor**.

3. For **Select type**, select **Hyper-V**.

4. For **Hypervisor name** or **Client name**, type a descriptive name for the hypervisor.

5. Enter host or account information:
   
   - **Hostname / IP address**: Provide a fully qualified hostname or IP address for the hypervisor.
   - **Username** and **Password**: Enter the user credentials to provide administrative access to the hypervisor.

6. Click **Discover nodes**.

7. When the **Nodes** field is populated, select one or more nodes on which to install the Virtual Server Agent.
   
   For a Microsoft Hyper-V cluster, or to use Changed Block Tracking for Hyper-V 2012 R2, select all nodes in the Hyper-V cluster.

8. Click **Save**.

**Installing and Launching the System Center Plug-In**

You can install the Commvault System Center plug-in to manage backups and recovery of Hyper-V virtual machines from within System Center.

Download the Commvault System Center plug-in from the Admin Console, and follow the instructions provided with the download to install the plug-in.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Before You Begin

- The plug-in is supported only for Internet Explorer 10 or later.

Procedure

1. Log on to the Admin Console.
2. From the navigation pane, go to Administration > Operations > Plugins.
3. In the upper right corner of the Plugins page, click System center.
4. The Microsoft system center plugin page displays instructions you can use to install and enable the plug-in.
5. Click Download plugin package for virtual machine manager to download the plug-in package.
6. After the download completes, copy the zip file for the package to a folder that is accessible from the Virtual Machine Manager.
7. Open the System Center Virtual Machine Manager Console.
8. The Connect to Server dialog box appears.
9. Log on to Virtual Machine Manager with administrator credentials.
10. The Virtual Machine Manager Console appears.
11. In the navigation pane, click Settings.
12. In the ribbon, click Import Console Add-in.
13. The Import Add-in wizard guides you through the installation.
14. Follow the steps in the wizard to install the zip file that contains the Commvault plug-in.
15. After the installation is complete, you can access the Admin Console from Virtual Machine Manager by clicking VMs and Servers and then clicking Admin Console in the ribbon, or by right-clicking a virtual machine and selecting VM Info.

Adding a Nutanix AHV Hypervisor

Add a Nutanix AHV hypervisor to support data protection operations for all virtual machines hosted or managed by the hypervisor.

Before You Begin

You will need the following information to add a hypervisor:

- The hypervisor is the Nutanix cluster, identified by the cluster name or the virtual IP address for the cluster.
  
  Be prepared to enter Prism administrator user credentials.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- A VSA proxy must be installed on a virtual machine in the Nutanix cluster. If you have installed the Virtual Server Protection package on a VM in the Nutanix cluster, the VSA is included with that installation.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors.**
   The **Hypervisors** page appears.
2. Click **Add hypervisor.**
3. For **Select type**, select **Nutanix Acropolis.**
4. For **Hypervisor name** or **Client name**, type a descriptive name for the hypervisor.
5. Enter host or account information:
   - **Hostname / IP address**: Provide a fully qualified hostname or IP address for the hypervisor.
   - **Username** and **Password**: Enter the user credentials to provide administrative access to the hypervisor.
6. From the **Proxy** list, select a previously deployed proxy in the Nutanix cluster.
7. Click **Save.**

**Adding an OpenStack Hypervisor**

Add an OpenStack hypervisor to support data protection operations for all instances or images hosted or managed by the hypervisor.

**Before You Begin**

You will need the following information to add a hypervisor:

- Install the Virtual Server Agent (VSA) on at least one instance (proxy) in the OpenStack data center. You can install the VSA on other instances to create additional VSA proxies for the data center.
- At least one VSA proxy is needed for each region.
- Identify the keystone address for the OpenStack node and obtain administrator user credentials. If there are multiple endpoints for the keystone URL, use the public endpoint.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors.**
   The **Hypervisors** page appears.
2. Click **Add hypervisor.**
   The **Add hypervisor** page appears.
3. For **Select type**, select **OpenStack.**
4. For **Keystone Address**, enter the fully qualified host name or IP address for the keystone node.

   **Note:** If the endpoint uses a port other than 5000 or if the endpoint listening on port 5000 is not configured to authenticate the user, enter the full keystone endpoint URL. The endpoint URL must be able to authenticate the user logon credentials, and can be the public or admin URL.

5. For **Hypervisor name**, type a descriptive name for the hypervisor.

6. Enter host or account information:
   - **User name**: Enter the user name for the keystone node user with administrator privileges.
   - **OpenStack Domain** (optional): If a domain is configured in the OpenStack environment, enter the domain for the keystone node user.
   - **Password**: Enter the password for the user account.

7. From the **Proxy** list, select a previously deployed proxy that is an instance in the OpenStack data center.

8. Click **Save**.

---

**Adding an Oracle Cloud Infrastructure Classic Hypervisor**

Add an Oracle Cloud Infrastructure Classic hypervisor to support data protection operations for all instances hosted or managed by the hypervisor.

**Before You Begin**

You will need the following information to add a hypervisor:

- Install the Virtual Server Agent (VSA) on at least one Oracle Cloud Infrastructure Classic instance. You can install the VSA on other machines to create additional VSA proxies.
- At least one VSA proxy is needed.
- Identify the endpoint that can be used to access Oracle Cloud Infrastructure Classic.
- Obtain administrator user credentials.
  - Non-administrators can perform backups and restores for local or Oracle Cloud Infrastructure Classic libraries if they have the following Oracle Cloud Infrastructure Classic permissions:
    - Compute: Compute Operations
    - Storage: Storage Read Write Group

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**. The **Hypervisors** page appears.
2. Click **Add hypervisor**. The **Add hypervisor** page appears.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

3. For **Select type**, select **Oracle Cloud Classic**.

4. For **Endpoint**, enter the fully qualified domain name (FQDN) for the endpoint that is used to access Oracle Cloud Classic.

5. For **Hypervisor name**, type a descriptive name for the hypervisor.

6. Enter host or account information:
   - **Identity domain/username**: Enter the domain and user name required to access the endpoint.
   - **Password**: Enter the password for the user account.

7. From the **Proxy** list, select a previously deployed proxy that is an Oracle Cloud Classic instance.

8. Click **Save**.

---

**Adding an Oracle VM Hypervisor**

Add an Oracle VM hypervisor to support data protection operations for all virtual machines hosted or managed by the Oracle VM Manager deployment.

**Before You Begin**

You will need the following information to add a hypervisor:

- Install the Virtual Server Agent (VSA) on at least one virtual machine hosted on an Oracle VM Server that is part of the Oracle VM deployment. You can install the VSA on other virtual machines to create additional VSA proxies.
- At least one VSA proxy is needed.
- Identify the IP address for the Oracle VM Manager node.
- Obtain administrator user credentials.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   The **Hypervisors** page appears.

2. Click **Add hypervisor**.
   The **Add hypervisor** page appears.

3. For **Select type**, select **Oracle VM**.

4. Provide the following information:
   - **Oracle VM Manager**: Enter the fully qualified host name or IP address for the Oracle VM Manager.
   - **Hypervisor name**: Type a descriptive name for the hypervisor.
   - **User name**: Enter the user name required to access Oracle VM Manager.
   - **Password**: Enter the password for the user account.
   - **Proxy**: Select a previously deployed proxy that is a virtual machine hosted on an Oracle VM Server.
5. Click **Save**.

**Adding a VMware Hypervisor**

Add a VMware hypervisor to support data protection operations for all virtual machines hosted or managed by the hypervisor.

**Before You Begin**

The hypervisor can be a vCenter or a standalone ESX server.

Be prepared to enter a vCenter user account with permissions sufficient to access the vCenter, ESX servers, datastores, and virtual machines, as well as volumes, files, and folders within virtual machines. The account must be able to perform discovery, backup, and restore operations.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**. The **Hypervisors** page appears.
2. Click **Add hypervisor**.
3. For **Select type**, select **VMware**.
4. For **Hypervisor name** or **Client name**, type a descriptive name for the hypervisor.
5. Enter host or account information:
   - **Hostname / IP address**: Provide a fully qualified hostname or IP address for the hypervisor.
   - **Username and Password**: Enter the user credentials to provide administrative access to the hypervisor.
6. When adding an additional hypervisor to an existing configuration, select a previously deployed proxy from the **Proxy** list.
7. Click **Save**.

**Viewing Hypervisor and Subclient Details**

When you log on or click **Hypervisors** in the navigation pane, the list of configured hypervisors is displayed. You can use the **Hypervisors** page to add or view hypervisor information, to access subclients, or to check job status.

**Hypervisors Page**

From the main **Hypervisors** page, you can perform the following actions:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Click **Send logs** to collect log information for a support case.
- Click **Add hypervisor** to configure a new hypervisor.
- Click an entry in the **Name** column to view hypervisor details.

- Under the **Actions** column, click the action button in the row for the hypervisor and select one of the following options:
  - Click **Jobs** to view all jobs.
  - Click **Delete** to delete the hypervisor (confirmation is required for this action).
  - Click **Send logs** to collect log information for a support case.

**Hypervisor Detail Page**

When you select a specific hypervisor, you can view details for the hypervisor:

- **VM status**: The number of virtual machines that are protected (backed up), not protected, backed up with errors, or all VMs. You can click on a bar in the graph to view reports (on page 61).
- **Activity control**: Whether Data management (backups) and Data recovery are enabled for the hypervisor.
- **Options**: Special configuration for the hypervisor. Options are not available for all hypervisors, and the available options are different for each hypervisor type.
- **Alerts**: What alerts are enabled.
- **Proxy**: What Virtual Server Agent proxies are available to perform backup and restore operations for the hypervisor.
- **Security**: Security associations and virtual machine owners.
- **Subclients**: What subclients are configured.

From the hypervisor details page, you can perform the following actions:

- Click **Jobs** at the top right to view all jobs for the hypervisor.
- Click **Edit hypervisor details** at the top right to change the host name, user name, or password.
- Click **Delete** at the top right to delete this hypervisor entry. You are then asked to confirm this action. Deleting a hypervisor also deletes all backups for the hypervisor.
- Click a bar in the **VM status** area to display information about virtual machines on the hypervisor.
- Click **ON** or **OFF** for **Data management** or **Data recovery** to toggle those settings.
- Click **Edit** in the **Settings** area to update the configuration for the hypervisor.
- Click an alert to view the alert definition, including the list of users who receive the alert.
- In the **Proxy** area, click **Reorder** to change the sequence that is used to select proxies for jobs, or click **Edit** to enable or disable proxies for use with this hypervisor.
- In the **Security** area, click **Edit** to assign roles to users or user groups or to add owners for virtual machines.

In the **Subclients** area you can perform the following actions:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Click **Add subclient** to create a new group of virtual machines to back up.
- Click a subclient name to view or modify subclient settings.
- Click **Restore** to recover data from the subclient on the same row. The **Restore** button is only displayed if a successful backup has been performed for a subclient.

- Under the **Actions** column for the **Subclients** area, you can click the action button in the row for the subclient and select one of the following options:
  - Click **Delete** to remove a subclient. You are then asked to confirm this action. Deleting a subclient also deletes all backups for the subclient. You cannot delete a default subclient.
  - Click **Jobs** to view job information for the subclient on the same row.
  - Click **Back up now** to perform an immediate backup of the virtual machines in the subclient.

**Subclient Detail Page**

When you select a subclient from the hypervisor details page, you can view details for the subclient:

- Display showing the number of virtual machines for the subclient that are protected, unprotected, backed up with errors, or all VMs. You can click on a bar in the graph to view VMs for the subclient (on page 61).
- A summary of backup information.
- Whether backup jobs are currently running.
- The content that is defined for the subclient (virtual machines to be backed up).
- Security information.
- Storage information.
- Options for default backup settings, including changed block tracking (CBT), number of readers, and application or crash consistent backups.
- Scheduled backup jobs.
- Proxy information.
- Alerts enabled for the subclient. You can click on an alert to view the alert definition, including the list of users who receive the alert.

From the subclient details page, you can perform the following actions:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Click **Restore** in the top right area of the page to restore virtual machine data.
- Click a bar in the **VM status** area to display information about virtual machines on the hypervisor.
- In the **Summary** area, you can toggle **Data management** on or off to enable or disable backups and restores.
- In the **Backup** area, click **Jobs** to view jobs, or **Back up now** to perform a backup for the subclient.
- In the **Content** area, click **Manage** to add virtual machines to a subclient or change existing content selections.
- Under the **Content** area, click **Show filters** to view filters that are defined to exclude virtual machines from backups.
- In the **Security** area, click **Edit** to change user security settings or VM ownership.
- In the **Storage target** area, click **Edit** to change the storage library name or the retention period for backup data.
- In the **Options** area, click **Edit** to change backup options.
- In the **Schedules** area, click **Add schedule** or **Manage** to add or modify a scheduled backup.
- In the **Proxy** area, click **Reorder** to change the sequence that is used to select proxies for jobs, or click **Edit** to enable or disable proxies for use with this hypervisor.
- In the **Alerts** area, click an alert entry to view the alert definition.

**Editing Hypervisor Information**

You can change settings for a hypervisor by editing the hypervisor details.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   The **Hypervisors** page appears.
2. Click the name of the hypervisor.
   The hypervisor details page appears.
3. In the top right corner of the page, click **Edit hypervisor details**.
   The **Edit hypervisor details** dialog box appears.
4. To point to a different hypervisor, edit the information for the hypervisor access point and credentials:
   - **Hyper-V, Nutanix AHV, or VMware**:
     - **Hostname / IP address**: Provide a fully qualified hostname or IP address for the hypervisor.
     - **Username** and **Password**: Enter the user credentials to provide administrative access to the hypervisor.
   - **Amazon**:
     - **Access key**: Type the Access Key ID that is associated with your Amazon EC2 account.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Secret key**: Type the Secret Access Key that is associated with your Amazon EC2 account.
  - Azure Classic or Azure Resource Manager:
    - **Subscription ID**: Enter the subscription ID for your Azure account.
  - Azure Classic:
    - **Thumbprint**: Enter the thumbprint for the Azure management certificate.
  - Azure Resource Manager:
    - **Tenant ID**: Enter the tenant ID associated with the Azure account.
    - **Application ID**: Enter the application ID associated with the tenant.
    - **Application password**: Enter the password for the application.
  - OpenStack:
    - **Keystone Address**: Enter the fully qualified host name or IP address for the keystone node.
  - Oracle Cloud Classic:
    - **End point**: Enter the URL for the endpoint that is used to access Oracle Cloud Classic.
  - Oracle VM:
    - **Oracle VM Manager**: Enter the fully qualified host name or IP address for the Oracle VM Manager.
    - **Username**: Enter the user name required to access Oracle VM Manager.
    - **Password**: Enter the password for the user account.

5. Click **Save**.

**Editing Hypervisor Options**

You can change the configuration for a hypervisor by editing the hypervisor options.

**Before You Begin**

- To configure access to vCloud Director for VMware, obtain the vCloud host name and user credentials.
- To select a MediaAgent to recover UNIX file system data, a file recovery enabler for Linux must be deployed in your environment.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**. The **Hypervisors** page appears.
2. Click the name of the hypervisor. The hypervisor details page appears.
3. In the **Settings** area, click **Edit**.
   - For Google Cloud Platform, you can set the following options:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Client Name**: Enter a descriptive name for the Google Cloud service account.
- **Service Account ID**: Enter the service account ID.
- **Project ID**: Enter the project ID.
- **P12 key filename**: Enter the file name for the P12 private key.
- **Private Keys password**: Enter the password for the private key.
  
  o For VMware, you can set the following options:
    - **vCloud host name**: To enable backups and restores for vCloud Director, enter the vCloud host name.
    - **Username**: Enter the username for the vCloud account. Do not include the domain name.
    - **Password**: Enter the password for the vCloud account, then re-enter the same password in the Confirm password box.
  
  o For Amazon, Azure, Hyper-V, OpenStack, Oracle Cloud Infrastructure Classic, Oracle VM, and VMware, you can set the following option:
    - **File recovery enabler for Linux**: Select a MediaAgent that has been configured to recover UNIX file system data.

4. Click **Save**.

Subclients (VM Groups)

Subclients are sets of virtual machines that can be included in backup or restore operations. Each hypervisor contains at least one default subclient, which provides protection for any virtual machines that are not included in another subclient.

You can add additional subclients for a hypervisor as needed. For example, you can put virtual machines in different subclients so that you can have different backup criteria or schedules for different classes of virtual machines.

Subclients for a hypervisor are displayed on the details page for the hypervisor. You can select a subclient to view summary information, get status, and perform backups and restores.

When you select **Solutions > Virtualization > VM groups** from the navigation pane, you can view the complete set of subclients defined for all hypervisors.

Adding a Subclient

Add a subclient to identify a specific set of virtual machines to back up or restore.
Before You Begin

- Define a server plan (on page 136) that specifies the storage, retention, and backup schedule to be used for the subclient.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. Click Add subclient.
   The Add subclient dialog box appears.
4. Provide the following information:
   - **Name**: Type a descriptive name for the subclient.
   - **Browse and select VMs (or instances)**: Expand the tree below this field to select hosts, specific VMs, or VM storage locations for the subclient. Click Select all to quickly select all objects or Clear all to remove all current selections.
     
     You can select one of the following options from the grouping list to control the browse display:
     
     - **Amazon**:
       - **By instance type**: Select an instance of a particular type within a region.
       - **By region**: Select an instance within a region.
       - **By zone**: Select an instance within a zone and region.
       - **VMs**: Select this option to browse and select specific VMs.
     - **Google Cloud Platform**:
       - **By region**: Select an instance within a region.
     - **Microsoft Azure Classic**:
       - **Regions**: Select an Azure region to include all VMs in that region.
       - **Resource group**: Select a resource group for Azure Resource Manager.
       - **Storage Accounts**: Select a storage account to include all VMs that reside in the storage account.
       - **Tags**: Select a tag to include all VMs associated with the selection.
       - **VMs**: Select this option to browse and select specific VMs.
     - **Microsoft Azure Resource Manager**:
       - **Resource group**: Select a resource group for Azure Resource Manager.
       - **VMs**: Select this option to browse and select specific VMs.
     - **Microsoft Azure Stack**: 

Resource group: Select a resource group for Azure Stack.

VMs: Select this option to browse and select specific VMs.

- Microsoft Hyper-V:

  Group by host: Select this option to view hosts and the VMs running on each host. Select a host entry to protect all VMs on the host, or expand the tree to select specific VMs.

  Virtual machines are shown directly under the host.

  Storage: Select this option to view storage containing virtual machine data. Select the storage entry to protect all VMs on the storage, or expand the tree to select specific VMs.

  VMs: Select this option to browse and select specific VMs.

- Nutanix AHV:

  Container: Select a storage container or specific virtual machines.

  Data protection: Select a host, protection domain, or specific virtual machines.

  VMs: Select this option to browse and select specific VMs.

- OpenStack:

  Projects: Select a project, region, instance, or image.

  Admin: Select images or instances.

- Oracle Cloud Infrastructure Classic:

  Instances: Select instances to be backed up.

- Oracle VM:

  Servers and VMs: Select server pools, VM pools, servers, or virtual machines.

  Repositories: Select storage repositories.

- VMware:

  Group by datastore: Select this option to view datastores containing virtual machine data.

  The top level of the browse shows all accessible hosts at the top level, with datastores under hosts and virtual machines under each datastore. Select a datastore entry to protect all VMs on the storage, or expand the tree to select specific VMs.

  Group by host: Select this option to view hosts and the VMs running on each host. Select a host entry to protect all VMs on the host, or expand the tree to select specific VMs.

  The top level of the browse shows all accessible vCenters at the top level, ESX servers under vCenters, and virtual machines under each ESX server.

  VMs: Select this option to browse and select specific VMs.

You can also define rules (on page 40) to discover virtual machines or instances automatically.

- Plan: Select a plan that specifies the storage, retention, and backup schedule to be used for the subclient.

Note: For VMware and Hyper-V subclients, you can enable IntelliSnap backups by creating a Snap plan (on page 138) and adding the Snap plan to a subclient. For more information, see Snap Plans (on page 137).
5. Click **Save** to save the subclient.

Subclients are created with default settings for backup options. To change default settings, see Editing Subclient Options (on page 51).

## Managing Subclient Content

For an existing subclient, you can add virtual machines or modify the content selections.

### Procedure

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
The **Hypervisors** page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   
The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.
3. Click the name of an existing subclient.
4. Click **Manage** in the **Content** area.
   
The **Content** tab of the **Subclient content** page shows the currently selected content to be backed up (hosts, specific VMs, or source virtual machine storage).
5. To remove a virtual machine, click ![Remove](image) in the **Actions** column of the row for the VM and select **Remove**.
6. To add subclient content, click **Add virtual machines**.
   
The **Add virtual machines** page appears.
7. Select a browse method for the **Browse and select VMs** list, and then expand the tree below the list to select hosts, specific VMs, or VM storage locations for the subclient, or to clear previous selections.

   You can select one of the following options from the list to control the browse display:
   
   - **Amazon**:
     - **By instance type**: Select an instance of a particular type within a region.
     - **By region**: Select an instance within a region.
     - **By zone**: Select an instance within a zone and region.
     - **VMs**: Select this option to browse and select specific VMs.
   
   - **Microsoft Azure Classic**:
     - **Cloud services**: Select cloud services for Azure Classic.
     - **Regions**: Select an Azure region to include all VMs in that region.
     - **Storage Accounts**: Select a storage account to include all VMs that reside in the storage account.
     - **VMs**: Select this option to browse and select specific VMs.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Microsoft Azure Resource Manager:
  - **Regions**: Select an Azure region to include all VMs in that region.
  - **Resource group**: Select a resource group for Azure Resource Manager.
  - **Storage Accounts**: Select a storage account to include all VMs that reside in the storage account.
  - **Tags**: Select a tag to include all VMs associated with the selection.
  - **VMs**: Select this option to include browse and select specific VMs.

- Microsoft Hyper-V:
  - **Group by host**: Select this option to view hosts and the VMs running on each host. Select a host entry to protect all VMs on the host, or expand the tree to select specific VMs.
  - Virtual machines are shown directly under the host.
  - **Storage**: Select this option to view storage containing virtual machine data. Select the storage entry to protect all VMs on the storage, or expand the tree to select specific VMs.
  - **VMs**: Select this option to browse and select specific VMs.

- Nutanix AHV:
  - **Container**: Select a storage container or specific virtual machines.
  - **Data protection**: Select a host, protection domain, or specific virtual machines.
  - **VMs**: Select this option to browse and select specific VMs.

- OpenStack:
  - **Projects**: Select a project, region, instance, or image.
  - **Admin**: Select images or instances.

- Oracle Cloud Classic:
  - **Instances**: Select instances to be backed up.

- Oracle VM:
  - **Servers and VMs**: Select server pools, VM pools, servers, or virtual machines.
  - **Repositories**: Select storage repositories.

- VMware:
  - **Group by datastore**: Select this option to view datastores containing virtual machine data. The top level of the browse shows all accessible hosts at the top level, with datastores under hosts and virtual machines under each datastore. Select a datastore entry to protect all VMs on the storage, or expand the tree to select specific VMs.
  - **Group by host**: Select this option to view hosts and the VMs running on each host. Select a host entry to protect all VMs on the host, or expand the tree to select specific VMs.
  - The top level of the browse shows all accessible vCenters at the top level, ESX servers under vCenters, and virtual machines under each ESX server.
  - **VMs**: Select this option to browse and select specific VMs.

8. Click **OK** after selecting VMs or other objects.

9. To discover virtual machines automatically:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

a. Click **Add rule**.

b. From the **Select rule for** list, choose one of the following:

- Amazon:
  
  **Guest DNS hostname**: In the **Name** box, type a hostname or a pattern to identify a hostname or domain (for example, *myhost.mycompany.com* to identify a specific host or *.mycompany.com* to identify all hosts on that domain).

  **Guest OS**: In the **Name** box, type the exact name of the operating system or a pattern to identify an operating system group (for example, *Microsoft* to identify any virtual machine that has a version of the Windows operating system).

  **Instance name/pattern**: In the **Name** box, type the display name of the instance or a pattern using wildcards (for example, *Test* to identify instances for which the instance name begins with "Test").

  **Instance state**: Select **Running** or **Stopped**.

  **Zone**: In the **Name** box, type the name of the zone or a pattern using wildcards (for example, *us-east* to identify zones for which the zone name begins with "us-east"). When you add a zone, all instances in the zone are included in backups.

- Microsoft Azure Classic:

  **Cloud services**: In the **Name** box, type a cloud service name or a pattern to identify a cloud service.

  **Power state**: From the **Name** list, select the power on status of virtual machines to be included in the subclient content. You can select **On** to identify VMs that are powered on, **Off** to identify VMs that are powered off, or **Other** to identify VMs with a different power on status, such as Suspended.

  **Region**: Select a region to include all VMs in that region.

  **Virtual machine name/pattern**: In the **Name** box, type the display name of the virtual machine or a pattern using wildcards (for example, *Test* to identify VMs for which the VM name begins with "Test").

- Microsoft Azure Resource Manager:

  **Power state**: From the **Name** list, select the power on status of virtual machines to be included in the subclient content. You can select **On** to identify VMs that are powered on, **Off** to identify VMs that are powered off, or **Other** to identify VMs with a different power on status, such as Suspended.

  **Region**: Select a region to include all VMs in that region.

  **Resource group**: In the **Name** box, type a resource group name or a pattern to identify a resource group.

  **Storage Account**: Select a storage account to include all VMs that reside in the storage account.

  **Virtual machine name/pattern**: In the **Name** box, type the display name of the virtual machine or a pattern using wildcards (for example, *Test* to identify VMs for which the VM name begins with "Test").

- Microsoft Hyper-V:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

**Guest DNS hostname:** In the Name box, type a hostname or a pattern to identify a hostname or domain (for example, `myhost.mycompany.com` to identify a specific host or `*mycompany.com` to identify all hosts on that domain).

**Guest OS:** In the Name box, type the exact name of the operating system or a pattern to identify an operating system group (for example, `Microsoft*` to identify any virtual machine that has a version of the Windows operating system).

**Host:** In the Name box, type the host name, the IP address of the host, or a host name pattern using wildcards. When you add a host, all virtual machines on the host are included in the backup.

**Notes:** In the Name box, type a pattern to identify virtual machines based on notes text contained in annotations for the VM summary (for example, `Test*` to identify VMs with a note that begins with "Test").

**Power state:** From the Name list, select the power on status of virtual machines to be included in the subclient content. You can select **On** to identify VMs that are powered on, **Off** to identify VMs that are powered off, or **Other** to identify VMs with a different power on status, such as Suspended.

**Virtual machine name/pattern:** In the Name box, type the display name of the virtual machine or a pattern using wildcards (for example, `Test*` to identify VMs for which the VM name begins with "Test").

- **Nutanix AHV:**

  **Power state:** From the Name list, select the power on status of virtual machines to be included in the subclient content. You can select **On** to identify VMs that are powered on, **Off** to identify VMs that are powered off, or **Other** to identify VMs with a different power on status, such as Suspended.

  **Virtual machine name/pattern:** In the Name box, type the display name of the virtual machine or a pattern using wildcards (for example, `Test*` to identify VMs for which the VM name begins with "Test").

- **OpenStack:**

  **Instance name/pattern:** In the Name box, type the display name of the instance or a pattern using wildcards (for example, `Test*` to identify instances for which the instance name begins with "Test").

  **Power state:** From the Name list, select the power on status of instances to be included in the subclient content. You can select **On** to identify instances that are powered on, **Off** to identify instances that are powered off, or **Other** to identify instances with a different power on status, such as Suspended.

- **Oracle Cloud Classic:**

  **Instance name/pattern:** In the Name box, type the display name of the instance or a pattern using wildcards (for example, `Test*` to identify instances for which the instance name begins with "Test").

  **User:** Enter a name or pattern to identify a user, or browse to select a user.

- **Oracle VM:**

  **Repository:** In the Name box, type the name of a repository.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Virtual machine name/pattern: In the Name box, type the display name of the virtual machine or a pattern using wildcards (for example, Test* to identify VMs for which the VM name begins with "Test").

Server: In the Name box, type the name of a server.

Server folder: In the Name box, type the name of a server folder.

Server pool: In the Name box, type the name of a server pool.

Server pool folder: In the Name box, type the name of a server pool folder.

Virtual machine folder: In the Name box, type the name of a virtual machine folder.

- VMware:
  Datastore: In the Name box, type a datastore name or pattern.

Guest DNS hostname: In the Name box, type a hostname or a pattern to identify a hostname or domain (for example, myhost.mycompany.com to identify a specific host or *mycompany.com to identify all hosts on that domain).

Guest OS: In the Name box, type the exact name of the operating system or a pattern to identify an operating system group (for example, Microsoft* to identify any virtual machine that has a version of the Windows operating system).

Host: In the Name box, type the host name, the IP address of the host, or a host name pattern using wildcards. When you add a host, all virtual machines on the host are included in the backup.

Notes: In the Name box, type a pattern to identify virtual machines based on notes text contained in annotations for the VM summary (for example, Test* to identify VMs with a note that begins with "Test").

Power state: From the Name list, select the power on status of virtual machines to be included in the subclient content. You can select On to identify VMs that are powered on, Off to identify VMs that are powered off, or Other to identify VMs with a different power on status, such as Suspended.

Template: From the Name list, select True to include templates or False to not include templates.

Virtual machine name/pattern: In the Name box, type the display name of the virtual machine or a pattern using wildcards (for example, Test* to identify VMs for which the VM name begins with "Test").

c. From the Which matches with list, select Equals, Contains, Starts with, or Ends with.

d. In the Name box, provide a value as required for the type of rule.

e. Click OK.

10. To edit a rule, click in the Actions column of the row for the VM and select Edit rule.

11. Click Preview to see a list of the virtual machines that will be backed up and the hosts for the VMs.

12. Click OK to save the changes to subclient content.
Creating VM (Instance) Filters

From the Subclient content dialog box, you can create filters to exclude virtual machines (or instances) from backups.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   
   The Hypervisors page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.

3. Click the name of an existing subclient.

4. Click Manage in the Content area.
   
   The Subclient content dialog box appears.

   The Filters tab shows content to be excluded from backups.

5. On the Filters tab, to remove a filter, click in the Actions column of the row for the filter and select Remove.

6. To add filters by browsing, click Add virtual machines.

7. In the Add virtual machines page, select a browse method for the Browse and select VMs list, and then expand the tree below the list to select hosts, specific VMs, or VM storage locations for the subclient, or to clear previous selections.

   You can select one of the following options from the list to control the browse display:

   o Amazon:
     
     ▪ By instance type: Select an instance of a particular type within a region.
     ▪ By region: Select an instance within a region.
     ▪ By zone: Select an instance within a zone and region.
     ▪ VMs: Select this option to browse and select specific VMs.

   o Microsoft Azure Classic:
     
     ▪ Cloud services: Select cloud services for Azure Classic.
     ▪ Regions: Select an Azure region to include all VMs in that region.
     ▪ Storage Accounts: Select a storage account to include all VMs that reside in the storage account.
     ▪ VMs: Select this option to browse and select specific VMs.

   o Microsoft Azure Resource Manager:
     
     ▪ Regions: Select an Azure region to include all VMs in that region.
     ▪ Resource group: Select a resource group for Azure Resource Manager.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Storage Accounts**: Select a storage account to include all VMs that reside in the storage account.
- **Tags**: Select a tag to include all VMs associated with the selection.
- **VMs**: Select this option to browse and select specific VMs.
  
  - Microsoft Hyper-V:
    - **Group by host**: Select this option to view hosts and the VMs running on each host. Select a host entry to protect all VMs on the host, or expand the tree to select specific VMs.
    - Virtual machines are shown directly under the host.
    - **Storage**: Select this option to view storage containing virtual machine data. Select the storage entry to protect all VMs on the storage, or expand the tree to select specific VMs.
    - **VMs**: Select this option to browse and select specific VMs.
  
  - Nutanix AHV:
    - **Container**: Select a storage container or specific virtual machines.
    - **Data protection**: Select a host, protection domain, or specific virtual machines.
    - **VMs**: Select this option to browse and select specific VMs.
  
  - OpenStack:
    - **Projects**: Select a project, region, instance, or image.
    - **Admin**: Select images or instances.
  
  - Oracle Cloud Classic:
    - **Instances**: Select instances to be backed up.
  
  - Oracle VM:
    - **Servers and VMs**: Select server pools, VM pools, servers, or virtual machines.
    - **Repositories**: Select storage repositories.
  
  - VMware:
    - **Group by datastore**: Select this option to view datastores containing virtual machine data. The top level of the browse shows all accessible hosts at the top level, with datastores under hosts and virtual machines under each datastore. Select a datastore entry to protect all VMs on the storage, or expand the tree to select specific VMs.
    - **Group by host**: Select this option to view hosts and the VMs running on each host. Select a host entry to protect all VMs on the host, or expand the tree to select specific VMs.
    - The top level of the browse shows all accessible vCenters at the top level, ESX servers under vCenters, and virtual machines under each ESX server.
    - **VMs**: Select this option to browse and select specific VMs.

8. Click **OK** after selecting VMs or other objects.
9. To exclude virtual machines based on different criteria:
   a. Click **Add filter rule** and then provide information for the rule:
   b. From the **Select rule for** list, choose one of the following:
      - Amazon:
Guest DNS hostname: In the Name box, type a hostname or a pattern to identify a hostname or domain (for example, myhost.mycompany.com to identify a specific host or *mycompany.com to identify all hosts on that domain).

Guest OS: In the Name box, type the exact name of the operating system or a pattern to identify an operating system group (for example, Microsoft* to identify any virtual machine that has a version of the Windows operating system).

Instance name/pattern: In the Name box, type the display name of the instance or a pattern using wildcards (for example, Test* to identify instances for which the instance name begins with "Test").

Instance state: Select Running or Stopped.

Zone: In the Name box, type the name of the zone or a pattern using wildcards (for example, us-east* to identify zones for which the zone name begins with "us-east"). When you add a zone, all instances in the zone are excluded from backups.

- Microsoft Azure Classic:
  Cloud services: In the Name box, type a cloud service name or a pattern to identify a cloud service.
  Power state: From the Name list, select the power on status of virtual machines to be excluded from backups. You can select On to identify VMs that are powered on, Off to identify VMs that are powered off, or Other to identify VMs with a different power on status, such as Suspended.
  Region: Select a region to exclude all VMs in that region.
  Virtual machine name/pattern: In the Name box, type the display name of the virtual machine or a pattern using wildcards (for example, Test* to identify VMs for which the VM name begins with "Test").

- Microsoft Azure Resource Manager:
  Power state: From the Name list, select the power on status of virtual machines to be excluded from backups. You can select On to identify VMs that are powered on, Off to identify VMs that are powered off, or Other to identify VMs with a different power on status, such as Suspended.
  Region: Select a region to exclude all VMs in that region.
  Resource group: In the Name box, type a resource group name or a pattern to identify a resource group.
  Storage Account: Select a storage account to exclude all VMs that reside in the storage account.
  Virtual machine name/pattern: In the Name box, type the display name of the virtual machine or a pattern using wildcards (for example, Test* to identify VMs for which the VM name begins with "Test").

- Microsoft Hyper-V:
  Guest DNS hostname: In the Name box, type a hostname or a pattern to identify a hostname or domain (for example, myhost.mycompany.com to identify a specific host or *mycompany.com to identify all hosts on that domain).
Guest OS: In the Name box, type the exact name of the operating system or a pattern to identify an operating system group (for example, Microsoft* to identify any virtual machine that has a version of the Windows operating system).

Host: In the Name box, type the host name, the IP address of the host, or a host name pattern using wildcards. When you add a host, all virtual machines on the host are excluded from the backup.

Notes: In the Name box, type a pattern to identify virtual machines based on notes text contained in annotations for the VM summary (for example, Test* to identify VMs with a note that begins with "Test").

Power state: From the Name list, select the power on status of virtual machines to be excluded from backups. You can select On to identify VMs that are powered on, Off to identify VMs that are powered off, or Other to identify VMs with a different power on status, such as Suspended.

Virtual machine name/pattern: In the Name box, type the display name of the virtual machine or a pattern using wildcards (for example, Test* to identify VMs for which the VM name begins with "Test").

- Nutanix AHV:

  Power state: From the Name list, select the power on status of virtual machines to be excluded from backups. You can select On to identify VMs that are powered on, Off to identify VMs that are powered off, or Other to identify VMs with a different power on status, such as Suspended.

  Virtual machine name/pattern: In the Name box, type the display name of the virtual machine or a pattern using wildcards (for example, Test* to identify VMs for which the VM name begins with "Test").

- OpenStack:

  Instance name/pattern: In the Name box, type the display name of the instance or a pattern using wildcards (for example, Test* to identify instances for which the instance name begins with "Test").

  Power state: From the Name list, select the power on status of instances to be excluded from backups. You can select On to identify instances that are powered on, Off to identify instances that are powered off, or Other to identify instances with a different power on status, such as Suspended.

- Oracle Cloud Classic:

  Instance name/pattern: In the Name box, type the display name of the instance or a pattern using wildcards (for example, Test* to identify instances for which the instance name begins with "Test").

  User: Enter a name or pattern to identify a user, or browse to select a user.

- Oracle VM:

  Repository: In the Name box, type the name of a repository.

  Virtual machine name/pattern: In the Name box, type the display name of the virtual machine or a pattern using wildcards (for example, Test* to identify VMs for which the VM name begins with "Test").

  Server: In the Name box, type the name of a server.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Server folder: In the Name box, type the name of a server folder.
Server pool: In the Name box, type the name of a server pool.
Server pool folder: In the Name box, type the name of a server pool folder.
Virtual machine folder: In the Name box, type the name of a virtual machine folder.

- VMware:
  Datastore: In the Name box, type a datastore name or pattern.
  Guest DNS hostname: In the Name box, type a hostname or a pattern to identify a hostname or domain (for example, myhost.mycompany.com to identify a specific host or *mycompany.com to identify all hosts on that domain).
  Guest OS: In the Name box, type the exact name of the operating system or a pattern to identify an operating system group (for example, Microsoft* to identify any virtual machine that has a version of the Windows operating system).
  Host: In the Name box, type the host name, the IP address of the host, or a host name pattern using wildcards. When you add a host, all virtual machines on the host are excluded from the backup.
  Notes: In the Name box, type a pattern to identify virtual machines based on notes text contained in annotations for the VM summary (for example, Test* to identify VMs with a note that begins with "Test").
  Power state: From the Name list, select the power on status of virtual machines to be excluded from backups. You can select On to identify VMs that are powered on, Off to identify VMs that are powered off, or Other to identify VMs with a different power on status, such as Suspended.
  Template: From the Name list, select True to exclude templates or False to not exclude templates.

- Virtual machine name/pattern: In the Name box, type the display name of the virtual machine or a pattern using wildcards (for example, Test* to identify VMs for which the VM name begins with "Test").

c. From the Which matches with list, choose Equals, Contains, Starts with, or Ends with.
d. In the Name box, provide a value as required for the type of rule.
e. Click OK.

10. To edit a rule, click in the Actions column of the row for the VM and select Edit rule.
11. Click OK to save the changes to subclient content.

Creating Disk (Volume) Filters

From the Subclient content dialog box, you can create disk filters to exclude virtual machine disks from backups.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Procedure

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   The Hypervisors page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.

3. Click the name of an existing subclient.

4. Click Manage in the Content area.
   The Subclient content dialog box appears.
   The Disk Filters tab shows disks to be excluded from backups.

5. On the Disk Filters tab, to remove a filter, click in the Actions column of the row for the filter and select Remove.

6. To exclude virtual machine disks, click Add disk filter.

7. In the Add disk filter dialog box, provide information for the rule:
   a. From the Disk filter type list, choose one of the following:

      **Amazon**:
      - **Volume device name/pattern**: In the Volume device name/pattern box, enter the device name of the volume or a pattern using wildcards (for example, /**/xdv* to identify volume devices in any folder for which the volume device name begins with "xdv").
      - **Volume name/pattern**: In the Volume name/pattern box, enter the display name of the volume or a pattern using wildcards (for example, Data* to identify volumes for which the volume name begins with "Data").
      - **Volume type**: To filter the operating system volume, select root (the only value).

      **Note**: You cannot back up the root volume for an instance that is launched from AWS Marketplace.

      **Microsoft Azure**:
      - **Blob URI/pattern**: In the Blob URI/pattern box, type the URI for an Azure blob or a pattern with wildcards to identify blob storage objects.
      - **Disk name/pattern**: In the Disk name/pattern box, enter the name of the disk or a pattern using the '*' wildcard to represent a string of characters (for example, disk12.vhd or disk*.vhd).
      - **Disk type**: To filter the operating system volume, select OS Disk (the only value).

      **Microsoft Hyper-V**:
      - **Virtual device node**: Select this option to filter a specific device node.
        Select a disk controller from the Controller list, and type an integer for the controller channel in the Location box.
      - **Virtual disk name/pattern**: Type a pattern for the names of disks to filter.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

For example, you can filter disks using patterns such as VMName.vhd or VMName.vhdx.

Nutanix AHV:

- **Container**: In the Container box, type the container name.
- **Disk address**: Choose pci, scsi, or ide from the Disk address list, and then type the number in the Disk number box.

OpenStack:

- **Volume name/pattern**: In the Volume name/pattern box, enter the display name of the volume or a pattern using wildcards (for example, Data* to identify volumes for which the volume name begins with "Data").
- **Volume type**: To filter the operating system volume, select root (the only value).

Oracle VM:

- **Disk slot number**: To exclude disks based on the slot number, select this option and then enter the beginning and end slot numbers to be excluded.
- **Repositories**: To exclude all VM disks from specified repositories, select this option and then select from the Repositories list.

VMware:

- **Datastore**: Select a datastore to filter all disks on the datastore.
- **Hard disk label**: Select this option to filter disks based on number labels. Specify the range by typing values in the Hard Disk Number From and Hard Disk Number To boxes.
- **Virtual device node**: Select this option to filter a specific device node. Select the node from the Virtual Device Node list.
- **VMDK name/pattern**: Type a pattern for the names of disks to filter. For example, you can filter disks with patterns such as VMName.vmdk, *VMName.vmdk, /**/folder/VM*.vmdk, or [Datastore]*/VM*.vmdk.

b. Click OK.

8. To edit a rule, click edit in the Actions column of the row for the filter and select Edit rule.
9. Click OK to save the changes to subclient content.

**Subclient Options**

For an existing subclient, you can modify options that affect backups.

The options vary depending on the type of hypervisor.

**Editing Subclient Options for Amazon**

For an existing subclient, you can modify options that affect backups.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.

3. Click the name of a subclient.
   The subclient details page appears.
   The Settings area shows settings that are used to back up the virtual machines in the subclient.

4. In the Settings area, click Edit.

5. In the Edit options dialog box, provide the following information:
   - No. of readers: Set the number of readers to control how many parallel read operations can be launched during backups.

6. Click Save.

Editing Subclient Options for Azure

For an existing subclient, you can modify options that affect backups.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.

3. Click the name of a subclient.
   The subclient details page appears.
   The Settings area shows settings that are used to back up the virtual machines in the subclient.

4. In the Settings area, click Edit.

5. In the Edit options dialog box, provide the following information:
   - Use changed block tracking: Select this option to use changed block tracking (CBT) for backups. With CBT, backups only write blocks that have changed since the previous backup. For virtual machines where there is a known issue with CBT, you can turn off CBT to run backups using the cyclic redundancy check (CRC) method instead.
   - No. of readers: Set the number of readers to control how many parallel read operations can be launched during backups.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Virtual machine backup type: Select one of the following options:
  - File system and application consistent: An application consistent backup quiesces the file system and applications while performing the backup.
  - Crash consistent: A crash consistent backup takes a point-in-time snapshot of virtual machine data without quiescing.

6. Click **Save**.

**Editing Subclient Options for Azure Stack**

For an existing subclient, you can modify options that affect backups.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
   The Hypervisors page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. Click the name of a subclient.
   
   The subclient details page appears.
   
   The **Settings** area shows settings that are used to back up the virtual machines in the subclient.

4. In the **Settings** area, click **Edit**.

5. In the **Edit options** dialog box, provide the following information:
   
   - No. of readers: Set the number of readers to control how many parallel read operations can be launched during backups.
   
   - Virtual machine backup type: Select one of the following options:
     
     - File system and application consistent: An application consistent backup quiesces the file system and applications while performing the backup.
     
     - Crash consistent: A crash consistent backup takes a point-in-time snapshot of virtual machine data without quiescing.

6. Click **Save**.

**Editing Subclient Options for Google Cloud Platform**

For an existing subclient, you can modify options that affect backups.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

The **Hypervisors** page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. Click the name of a subclient.
   
   The subclient details page appears.

4. You can edit the following options:
   
   **Backup**: Click **Jobs** to see job history for the selected subclient. Click **Back up now** to run a full, incremental or synthetic full data protection operation.

   **Content**: Click **Manage** to add instances or instance rules to subclient content.

   **Security**: Click **Edit** to define or update security associations on the subclient.

   **Plan**: Click **Edit** to associate a plan to the subclient (storage policy).

   **Storage Targets**: Click **Edit** to select a data storage policy.

   **Schedules**: Click **Add Schedule** to add a new schedule. Click the name of an existing schedule to make changes.

   **Alerts**: Select from the list of existing alerts to add users or groups to notify. If necessary, you can also delete the alert.

---

**Editing Subclient Options for Hyper-V**

For an existing subclient, you can modify options that affect backups.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
   The **Hypervisors** page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. Click the name of a subclient.
   
   The subclient details page appears.

   The **Settings** area shows settings that are used to back up the virtual machines in the subclient.

4. In the **Settings** area, click **Edit**.

5. In the **Edit options** dialog box, provide the following information:
   
   - **Use changed block tracking**: Select this option to use changed block tracking (CBT) for backups.

      With CBT, backups only write blocks that have changed since the previous backup. For virtual machines where there is a known issue with CBT, you can turn off CBT to run backups using the cyclic redundancy check (CRC) method instead.
For Hyper-V, CBT is only available for Hyper-V Server 2012 R2 and later.

- **No. of readers**: Set the number of readers to control how many parallel read operations can be launched during backups.

- **Virtual machine backup type**: Select one of the following options:
  - **File system and application consistent**: An application consistent backup quiesces the file system and applications while performing the backup.
  - **Crash consistent**: A crash consistent backup takes a point-in-time snapshot of virtual machine data without quiescing.

- **Collect file details**: Select this option to collect file and folder information during streaming backups or when creating a backup copy from IntelliSnap backups.

- **Collect file details for snapshot copy**: Select this option to collect file and folder information when creating a snapshot copy from IntelliSnap backups.

  **Note**: Collecting file details increases the time required to perform backups, and is not required to enable recovery of guest files and folders.

6. Click **Save**.

---

**Editing Subclient Options for Nutanix AHV**

For an existing subclient, you can modify options that affect backups.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**. The **Hypervisors** page appears.
2. Click the name of the hypervisor that hosts the virtual machines. The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.
3. Click the name of a subclient. The subclient details page appears. The **Settings** area shows settings that are used to back up the virtual machines in the subclient.
4. In the **Settings** area, click **Edit**.
5. In the **Edit options** dialog box, provide the following information:
   - **No. of readers**: Set the number of readers to control how many parallel read operations can be launched during backups.
   - **Virtual machine backup type**: Select one of the following options:
     - **Application consistent**: An application consistent backup quiesces the file system and applications while performing the backup.
     - **Crash consistent**: A crash consistent backup takes a point-in-time snapshot of virtual machine data without quiescing.
6. Click **Save**.

**Editing Subclient Options for OpenStack**

For an existing subclient, you can modify options that affect backups.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.  
   The **Hypervisors** page appears.
2. Click the name of the hypervisor that hosts the instances.  
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.
3. Click the name of a subclient.  
   The subclient details page appears.  
   The **Settings** area shows settings that are used to back up the instances in the subclient.
4. In the **Settings** area, click **Edit**.
5. In the **Edit options** dialog box, provide the following information:
   - **No. of readers**: Set the number of readers to control how many parallel read operations can be launched during backups.
6. Click **Save**.

**Editing Subclient Options for Oracle Cloud Classic**

For an existing subclient, you can modify options that affect backups.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.  
   The **Hypervisors** page appears.
2. Click the name of the hypervisor that hosts the instances.  
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.
3. Click the name of a subclient.  
   The subclient details page appears.  
   The **Settings** area shows settings that are used to back up the instances in the subclient.
4. In the **Settings** area, click **Edit**.
5. In the **Edit options** dialog box, provide the following information:
   - **No. of readers**: Set the number of readers to control how many parallel read operations can be launched during backups.

6. Click **Save**.

**Editing Subclient Options for Oracle VM**

For an existing subclient, you can modify options that affect backups.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
   The **Hypervisors** page appears.

2. Click the name of the hypervisor that hosts the instances.

   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. Click the name of a subclient.

   The subclient details page appears.

   The **Settings** area shows settings that are used to back up the instances in the subclient.

4. In the **Settings** area, click **Edit**.

5. In the **Edit options** dialog box, provide the following information:

   - **Use changed block tracking**: Select this option to use changed block tracking (CBT) for backups.
     
     With CBT, backups only write blocks that have changed since the previous backup. For virtual machines where there is a known issue with CBT, you can turn off CBT to run backups using the cyclic redundancy check (CRC) method instead.

   - **No. of readers**: Set the number of readers to control how many parallel read operations can be launched during backups.

   - **Datastore freespace required**: Type the percentage of free space that should be available on the datastore before performing the backup.

6. Click **Save**.

**Editing Subclient Options for VMware**

For an existing subclient, you can modify options that affect backups.

**VMware Transport Considerations**

**Licensing**: In vSphere 5.0, the SCSI HotAdd feature is enabled only for vSphere editions Enterprise and higher, which have Hot Add licensing enabled. No separate Hot Add license is available for purchase as an
Virtual Server Protection (VSP) - Version 11 Service Pack 11

add-on. In vSphere 4.1, Hot Add was also enabled in the Advanced edition. Customers with vSphere Essentials or Standard editions are not able to perform proxy-based backup, which relies on SCSI HotAdd. Those customers must use alternate transport modes.

**SCSI Controllers:** HotAdd relies on the SCSI protocol and does not support IDE disks. Use the LSI SCSI controller. The paravirtual SCSI controller (PVSCSI) is not supported for HotAdd.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors.**
   
The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   
The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.
3. Click the name of a subclient.
   
The subclient details page appears.
4. **Snap mount esx host:** For subclients that have a snap plan assigned, click **Edit** and then select an ESX server that can be used to mount snapshots for IntelliSnap backups.
   
The **Settings** area shows settings that are used to back up the virtual machines in the subclient.
5. In the **Settings** area, click **Edit.**
6. In the **Edit options** dialog box, provide the following information:
   - **Use changed block tracking:** Select this option to use changed block tracking (CBT) for backups.
   - With CBT, backups only write blocks that have changed since the previous backup. For virtual machines where there is a known issue with CBT, you can turn off CBT to run backups using the cyclic redundancy check (CRC) method instead.
   - **No. of readers:** Set the number of readers to control how many parallel read operations can be launched during backups.
   - **Virtual machine backup type:** Select one of the following options:
     - **File system and application consistent:** An application consistent backup quiesces the file system and applications while performing the backup.
     - **Crash consistent:** A crash consistent backup takes a point-in-time snapshot of virtual machine data without quiescing.
   - **Transport mode for VMware:** Select one of the following options:
     - **Auto:** The transport mode is selected automatically based on the backup environment:
       - If the datastore is accessible to a physical proxy, SAN is used.
       - If the datastore is accessible to the ESX server for a virtual proxy, HotAdd is used.
       - Otherwise, NBD is used.
     - **SAN:** For directly connected storage using Fibre Channel (FC) or Internet SCCI (iSCSI) protocols. The Virtual Server Agent must have access to the datastore LUNs (logical drives) that provide storage for virtual machine disks. Data is read directly from the storage where virtual machines reside, without going through the ESX host or transferring data over the local area.
network (LAN). The ESX host is contacted only to coordinate access to the LUN. SAN transport mode cannot be used if the proxy computer is a virtual machine.

- **Hot Add**: The Virtual Server Agent is installed on a virtual machine residing on an ESX server. In HotAdd mode, the data volumes containing the virtual machines to be backed up are automatically mounted to the proxy, so they can be accessed by the proxy as a local disk. The ESX host the proxy is running on must have access to all datastores for the virtual machine. If the virtual machine and the proxy are not on the same host, all datastores must be shared between the hosts.

- **NBD**: Data is transferred using the TCP/IP connection between the ESX server and the proxy computer. The local area network (LAN) can be the production network or a dedicated backup network.

- **NBD SSL**: Similar to NBD mode, but data transfer between the proxy computer and the ESX server is encrypted. Encryption should be used for sensitive information, even within a private network.

  - **Datastore freesp ace check**: Select this option to ensure that there is sufficient free space on the datastore before performing the backup.

  - **Datastore freesp ace required**: Type the percentage of free space that should be available on the datastore before performing the backup.

  - **Collect file details**: Select this option to collect file and folder information during streaming backups or when creating a backup copy from IntelliSnap backups.

  - **Collect file details for snapshot copy**: Select this option to collect file and folder information when creating a snapshot copy from IntelliSnap backups.

| Note: Collecting file details increases the time required to perform backups, and is not required to enable recovery of guest files and folders. |

7. Click **Save**.

**Managing Proxies**

Virtual Server Agent (VSA) proxies are used to perform backup and restore operations. Any machine where the VSA is installed can act as a VSA proxy. Different proxies are used for VMware and Hyper-V.

By default, the first available proxy listed for a subclient acts as a coordinator for jobs, distributing operations to any other proxies that are available for the subclient.

You can add or remove proxies for a hypervisor or a subclient, or change the order in which proxies are listed. By default, all subclients for a hypervisor use the proxies for the hypervisor, unless a different list is specified for the subclient.

| Note: If you select a new Hyper-V node as a proxy for a hypervisor, the Admin Console initiates a remote install to push the Virtual Server Agent, MediaAgent, and VSS provider to the new node. At the subclient level, only nodes that are already enabled as VSA proxies are displayed for selection, so no additional installs are required. |
Procedure

Adding or Removing Proxies
1. In the Proxy area for a hypervisor or subclient, click Edit.
   The Edit proxy dialog box lists all proxies that are available for the hypervisor.
   In the Hyper-V hypervisor details, all Hyper-V nodes are displayed. At the subclient level, only nodes that are already enabled as VSA proxies are displayed.
2. In the Edit proxy dialog box, select the check box for each proxy to be used for operations with the hypervisor or subclient, and clear the check box for each proxy that should not be used.
3. Click OK.

Changing the Order of Proxies
1. In the Proxy area for a hypervisor or subclient, click Reorder.
   The Reorder option is only displayed if multiple proxies are specified.
2. Click ▲ to move a proxy up in the list, or ▼ to move a proxy down.
3. Click Save to save the change in sequence.

Managing Schedules

Deprecated: After Service Pack 11 is installed, schedules will not be displayed on new plans. For plans created prior to Service Pack 11, you can continue to update the plan schedules.

You can create or modify a schedule for periodic backups as part of a plan that is assigned to subclient for a hypervisor.

Before You Begin
Identify the plan associated with a subclient.

Procedure
1. From the navigation pane, click Configuration > Plans.
   The Plans page appears.
2. Click the name of the server plan that is assigned to the subclient.
   The plan details page appears.
3. In the Schedules area, perform one of the following actions:
   □ To create a new schedule, click Add schedule.
   □ To modify an existing schedule, click the schedule on the plan details page.
4. In the **Schedules** dialog box, provide the following information:
   - **Name**: Type a descriptive name for the schedule (for example, **Weekly Full Backup**).
   - **Backup level**:
     - **Incremental**: Selected by default. An incremental backup only backs up changes since the last full backup.
     - **Full**: Perform a full backup for a virtual machine that has previously been backed up. A full backup includes virtual machine configuration files and all virtual machine data disks.
     - **Synthetic full**: Create a synthesized backup from the most recent full backup and all subsequent incremental backups. The resulting synthetic full backup is identical to a full backup for the subclient. Unlike full and incremental, a synthetic full backup does not actually transfer data from a client computer to the backup media, and does not use any resources on the client computer.

   A full backup is always performed for the first backup of any virtual machine.
   - **Frequency**: Select one of the following options:
     - **Daily**: Select this option and specify a value for the **Time** settings.
     - **Weekly**: After selecting this option, specify a value for the **Time** settings and select one or more days of the week.
     - **Monthly**: After selecting this option, specify a value for the **Time** settings; then select **On day** and type the day of the month, or select **Custom weeks/days** and set the desired parameters for the interval.

   For **Time** settings, click **AM** or **PM** to toggle between morning and afternoon.

   For daily, weekly, or monthly schedules, you can use the **Repeat** area to refine the backup schedule. For example, you can create a daily backup schedule that runs every other day by typing 2 in the **Every** box, or a backup that runs multiple times each day by selecting **Repeat Every** and specifying the interval and end time.

   To specify exceptions to the schedule, click **Exceptions** in the **Repeat** area. In the **Exceptions** dialog box, select **On day** and select a day of the month, or select **Custom weeks/days** and select the week and day. Click **Save** to save the exception and return to the **Add schedule** dialog box.

5. Click **Save** to save the schedule.

---

**VMs for a Hypervisor or Subclient**

The details page for a hypervisor or subclient shows a **VM status** diagram indicating the number of protected and unprotected virtual machines. You can click the bar showing the number of VMs to view a page with additional details.

On the **VMs for** page, you can perform the following actions to control which virtual machines are included in the report:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Time Range: Select the beginning of a time range; or choose Custom, set the beginning and end of the range, and click Submit.
- Collection: Choose a specific subclient or All.
- Status: Specify a status: All, Protected, Not protected, or Backed up with error.

Reports for protected or unprotected virtual machines show summary information for each virtual machine:

- **VM Name**: Name of the virtual machine.
- **Backup status**: Whether the VM is protected.
- **VM size**: Size of the virtual machine.
- **Backup size**: The amount of data written during backup.
- **Subclient**: The subclient to which the VM belongs.
- **Last backup time**: The date and time when the last backup was performed.

Live Mounts

Live Mount enables you to run a virtual machine directly from a stored backup for that VM.

You can use this feature to validate that backups are usable for a disaster recovery scenario, to validate the content on the backup, or to access data from the virtual machine directly instead of restoring guest files.

Virtual machines that are live mounted are intended for short term usage and should not be used for production. Changes to live mounted VMs or their data are not retained when the virtual machine expires. The VM expiration period is set through a VM Lifecycle Management policy.

You can include a policy option to migrate live mounted VMs to a different datastore after the initial live mount expires. The migration option is only supported for streaming backups and IntelliSnap backup copies.

Considerations

- Live Mount is supported for VMware hypervisors and from streaming backups, IntelliSnap backup copies, or IntelliSnap backups using NetApp snapshot engines.
- Live mounts must specify a destination that is different from the source VM. Only out-of-place live mounts are supported.
- The virtual machine owner or the user group associated with the VM owner must have a role that includes Browse and Live Browse permissions. The user or user group must be associated with the life cycle policy for live mounts.
- A MediaAgent can perform up to five Live Mount operations at a time.

Configuration

- To enable the Live Mount feature, create a life cycle policy (on page 132) that identifies resources and specifies parameters for live mount users.
Performing a Live Mount

Perform a live mount to run a virtual machine directly from a stored backup.

You can use this feature to validate that backups are usable for a disaster recovery scenario, to validate the content on the backup, or to access data from the virtual machine directly instead of restoring guest files.

Virtual machines that are live mounted are intended for short term usage and should not be used for production. Changes to live mounted VMs or their data are not retained when the virtual machine expires. The VM expiration period is set through a VM Lifecycle Management policy.

Before You Begin

- Run a backup for any VMs that will be live mounted.
- You must be associated with a life cycle policy that supports live mount operations.

Procedure

1. From the navigation pane, go to Solutions > Virtualization > Virtual Machines.
2. Under Actions, click and select Live mount.
   The Live mount dialog box appears.
3. Provide the following information:
   - **Live mount policy**: Select the policy to be used for the live mount operation.
   - **Virtual machine name**: Enter a display name for the live mounted VM.
   - **Network**: Select one of the following options:
     - **No network**: Mount the VM without a network connection.
     - **Original network**: Mount the VM with the same network connection as the source VM.
     - **Select network**: Mount the VM with the network specified in the live mount policy.
   - **Copy precedence**: Select the copy to use as a source for the live mount operation.
4. Click Submit.

Monitoring Live Mounts

You can monitor live mounts from a life cycle policy or from a VM.

Procedure

1. From the navigation pane, use one of the following paths to view active mounts:
   - **For a VM**: Go to Solutions > Virtualization > Virtual machines.
     The Life cycle policies page appears.
For all VMs mounted using a policy: Go to Configuration > Life cycle policies. The VMs page appears.

2. Under Actions, click and select View active mounts.
   The Active mounts page appears.

3. The following information is included for active mounts:
   - **Name**: The name of the live mounted VM.
   - **State**: Whether the VM is running or stopped.
   - **IP address**: The IP address assigned for the VM.
   - **Operating system**: The operating system for the VM.
   - **Creator**: The user who initiated the live mount.
   - **Expiration date**: The date and time when the live mount is scheduled to expire.
   - **Actions**:
     - **Delete**: Select and confirm this action to delete the live mount.
     - **Renew**: Select this option to specify a new expiration date for the VM.
Replication for VMware Virtual Machines

As part of the Virtualization solution, you can configure VMware virtual machines (VMs) for replication to one or more secondary sites. Replication uses backups of primary VMs to create destination VMs, and uses continued incremental backups to keep destination VMs updated.

Destination sites can be VMware or Amazon.

Replication is also referred to as *Live Sync*.

Process for Configuring Replication

You can configure replication in the following ways:

- Replicate all of the VMs in a subclient.
- Replicate selected VMs.

Replicating VMs in a Subclient

A subclient identifies VMs to be backed up, either by selecting specific VMs or by defining rules to discover VMs automatically (on page 40). Using rules enables the list of VMs in a subclient to change dynamically as VMs are added or removed.

To replicate all of the VMs in a subclient or VM group, complete the following tasks:

- Define a Virtualization backup and replication plan (on page 66).
  - A backup and replication plan identifies one or more storage targets, a set of backup schedules, and replication options.
- Create a replication target (on page 67).
- Assign a backup and replication plan to the subclient (on page 73).

When replication is configured for a subclient, the VMs in the subclient are backed up according to the schedule defined in the backup and replication plan, and then replicated to the replication target.

A replication group is automatically created for the VMs in the subclient.

Replicating Selected VMs

To replicate selected VMs, complete the following tasks:

- Create a replication target (on page 67).
- Create a replication group (on page 69).
  - For Live Sync Direct, include a backup and replication plan for the replication group.

When replication is configured for selected VMs, the VMs must be backed up before you can select them for the replication group. VMs are backed up and replicated according to the settings in the replication group.
Monitoring Replication

After configuring replication, you can use the Replication monitor (on page 74) to check the status of replication, or to initiate a failover from a primary site to a secondary site where VMs have been replicated.

Creating a Backup and Replication Plan

A backup and replication plan identifies one or more storage targets, RPOs (recovery point objectives), and replication options.

Procedure

1. From the navigation pane, go to Configuration > Plans.
   The Plans page appears.
2. In the top right corner of the page, click Create and then click Virtualization plan.
   The Select Virtualization plan type page appears.
3. Click the Backup and replication tile.
   The plan wizard launches and displays the Backup page.
4. Enter the Plan name.
   The first storage copy is always Primary.
   For other settings, you can use the default values, or you can specify a different storage pool, retention period, or RPO (recovery point objective) options, such as the backup frequency and the backup window.
   The Backup frequency value is used to set the intervals for daily incremental backups.
5. Click Next.
   A confirmation page asks whether you wish to create another copy. Additional copies can be useful for having backup data at a secondary location, such as a disaster recovery (DR) site.
6. To create a secondary copy of backup data, click I want to create another copy.
   A new Storage target dialog box appears.
7. Enter the Storage copy name and provide other configuration values for the secondary copy.
8. Click Next.
   The Replication page appears.
9. Provide the following information:
   o Backup source: Select the storage copy to be used as the source for replication.
   o Target: Select an existing replication target or click Create replication target to add a new target (on page 67).
   o Schedule: Replication is performed Immediately after the backup job completes (the only value).
10. Click **Advanced options** to enter other configuration values:

   - **Validate destination VM**: Verify that the destination VM is bootable by powering it on and then powering off. Changes resulting from the power on are not preserved. If hypervisor tools are not installed on the source VM, validation is skipped even when this option is selected.
     
     If validation fails, the destination virtual machine reverts back to its last valid (bootable) state.

   - **Overwrite if it already exists**: When this option is selected, the first replication replaces an existing virtual machine with the same name in the target location, even if the destination VM is running. Replications from incremental backups are not affected by this setting:
     
     - Subsequent incremental backups and replication updates are applied to the destination VM without overwriting the VM.
     
     - If the destination VM is currently running, the replication fails.

   - **Disk Provisioning**: Select the disk provisioning type for the destination VM: **Original, Thick Lazy Zero, Thin**, or **Thick Eager Zero**.

   - **Transport mode for VMware**: Use **Auto** to have the transport mode selected automatically based on the environment, or select a different value from this list: **SAN, Hot Add, NBD, NBD SSL**, or **NAS**.

11. Click **Next**.

12. Click **Save**.

---

**Creating a Replication Target**

A replication target defines a destination hypervisor and host, identifies a proxy that can be used for the operation, and provides other configuration values for replicated VMs. The replication target can be created as part of a backup and replication plan, or created independently and then associated with an existing plan.

**Before You Begin**

- Test failover is supported only for replication to VMware.
- To configure an isolated network for test failover operations, download a gateway template and copy it to a location where it can be accessed from Admin Console.

**Procedure**

To create a replication target independently, perform the following steps:

1. From the navigation pane, go to **Configuration > Replication targets**.
   
   The **Replication target** page appears.

2. In the top right corner of the page, click **Add replication target**.
   
   The **Add replication target** page appears.

3. From the **Select type** list, select **Amazon** or **VMware**.
   
   The **Add replication target** page displays **General** options.
4. Provide the following information:
   - **Replication target name**: Enter a descriptive name for the replication (for example, **DR site 1**).
   - **Destination hypervisor**: Select a hypervisor to manage the replicated VMs.
   - **Proxy**: Select a proxy to perform the replication.
   - **Amazon**:
     - **Instance display name**: Select **Prefix** or **Suffix**, and then enter a string that will be appended to source instances to create the display name for each destination instance.
     - **Availability zone**: Select the destination zone.
     - **Network**: Select a network interface for the destination instances.
     - **Auto select security group**: To specify a specific security group, clear this selection and, from the **Security groups** list, select a security group for the destination instances.
     - **Amazon buckets**: From this list, select a bucket for the instance volumes. Buckets are logical containers that provide secure access to objects (such as instance volumes).
     - **Auto select instance type**: To specify a specific instance type, clear this selection and from the **Instance type** list, select an instance type that provides the available CPU cores and memory for the instance.
   - **VMware**:
     - **VM display name**: (VMware) Select **Prefix** or **Suffix**, and then enter a string that will be appended to source VMs to create the display name for each destination VM.
     - **Destination host**: (VMware) Enter the name or IP address for an ESX server, or click **Browse** to select an ESX host or cluster for the hypervisor.
     - **Datastore**: (VMware) Select a datastore for virtual machine data. By default, virtual machine disks (VMDKs) for the replicated VM are added to the same datastore where the source VM disks resided; but you can specify a different datastore.
     - **Resource pool**: (VMware) Select a destination resource pool for all replicated VMs.
     - **Destination network**: (VMware) Select a network that is available for the destination.
       - If you select **Not Connected** or do not select a destination network, virtual machines are restored with network interfaces in disconnected state.

5. To configure advanced options, click **Additional Options** and provide the following information:
   - **Users and user groups**: Select items from the list and click **OK** to associate users or user groups with the replication target.
   - **Test failover options**: To enable the replication target to be used for test failover operations, select this option and provide the following information:
     - **Expiration time**: Select **Hours** or **Days** and specify the amount of time that live mounted VMs can run before they expire.
       - To keep VMs available beyond the expiry time, select the **Migrate VMs** option.
     - **Configure isolated network**: To use an isolated network with VMs mounted for a test failover operation, select this option and then click **Browse** to select the gateway template.
       - If you do not select this option and identify a gateway template, the VMs in the test failover operation will not have a network connection.
Migrate VMs: To enable live mounted VMs to be mounted to the destination datastore for extended availability, select this option.

6. Click Add.

Creating a Replication Group

A replication group is a set of virtual machines that can be replicated to a replication target (secondary site).

VMs can be replicated to VMware or Amazon from streaming backups, or to VMware using Live Sync Direct from an IntelliSnap backup.

Before You Begin

- For traditional live sync, virtual machines must have been backed up at least once to be added to a replication group.
  - This requirement does not apply for Live Sync Direct.
- Create a replication target (on page 67) for the secondary site.

Procedure

1. From the navigation pane, go to Configuration > Replication groups.
2. Click Configure replication group.
   The Configure replication group wizard start page appears.
3. Click Virtualization.
   - To replicate from streaming backups, click Live Sync.
   - To replicate from an IntelliSnap backup, click Live Sync Direct.
     With Live Sync Direct configurations, a maximum of three VM snapshots are retained on source VMs.
   The wizard displays the Select content page.
4. Provide the following information:
   - Hypervisors: Select the hypervisor for the source VMs.
   - Name: Enter a descriptive name for the replication group.
   - Select VMs: Select the virtual machines to be replicated and click OK.
     Only VMs that have been backed up are displayed.
   - Plan: (Live Sync Direct only) Select a previously defined backup and replication plan for the group.
5. Click Next.
   The wizard displays the Select target page.
6. Provide the following information:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Target**: Select a previously defined replication target or click Create replication target to create a new replication target (on page 67).

- **Schedule**: The only available option is Immediately after the backup job completes.

- Click Advanced options to configure the following parameters:
  - **Validate destination VM (Power ON and OFF)**: Select this option to verify that the destination VM is bootable by powering it on and then powering off. Changes resulting from the power on are not preserved. If guest tools are not installed on the source VM, validation is skipped even when this option is selected.
    
    If validation fails, the destination virtual machine reverts back to its last valid (bootable) state.

  - **Unconditionally overwrite if it already exists**: When this option is selected, the first Live Sync operation replaces an existing virtual machine with the same name in the target location, even if the destination VM is running.
    
    Live Synchs from incremental backups are not affected by this setting. Subsequent incremental backups and Live Sync updates are applied to the destination VM without overwriting the VM. If the destination VM is currently running, the Live Sync fails.

  - **Disk Provisioning**: (VMware target only) Select the disk provisioning type for the destination VM: Original, Thick Lazy Zero, Thin, or Thick Eager Zero.
    
    When configuring a domain controller VM for live sync, select Thick Lazy Zero.

  - **Transport mode for VMware**: (VMware target only) Use Auto to have the transport mode selected automatically based on the environment, or select a different value from this list: SAN, Hot Add, NBD, or NBD SSL.

7. Click Next.

   The wizard displays the Override options page.

8. To change the destination settings for a VM, select the VM from the Virtual machine list. You can enter the following information:

   - **Amazon target**:
     - **Change instance display name to**: Enter the display name for the destination instance.
     - **Availability zone**: Select the destination zone.
     - **Network**: Select a network interface for the destination instances.
     - **Auto select security group**: To specify a specific security group, clear this selection and, from the Security groups list, select a security group for the destination instances.
     - **Amazon buckets**: From this list, select a bucket for the instance volumes. Buckets are logical containers that provide secure access to objects (such as instance volumes).
     - **Auto select instance type**: To specify a specific instance type, clear this selection and from the Instance type list, select an instance type that provides the available CPU cores and memory for the instance.
     - **Specify guest credentials**: Select this option to enable required drivers to be installed on the Amazon guest instance, and then provide values for the Domain / Computer name, Username, and Password boxes.

   - **VMware target**:
     - **VM display name**: Enter the display name for the destination VM.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Destination host**: Click **Browse** to select a host for the destination VM.
- **Datastore**: Select a datastore to be used for virtual machine disks.
- **Resource pool**: Select a resource pool for the destination VM.
- **Network settings**: Click **Add** to create a new mapping between a source network and a destination network.
- **IP address settings**: Click **Add** to customize IP address settings (on page 128).

9. Click **Next**.
   The wizard displays the **Summary** page showing the settings for the group definition.

10. Click **Finish** to create the replication group.

**Result**

The wizard creates a replication schedule and a replication group that includes the selected source VMs.

**Editing a Replication Group**

After creating a replication group, you can modify the contents of the group.

**Procedure**

1. From the navigation pane, go to **Configuration > Replication groups**.
2. Click an entry under the **Group Name** column.
   A summary page for the replication group appears.
3. Click **Manage content**.
   The **Edit replication group** wizard displays the **Select content** page.
4. Provide the following information:
   - **Hypervisors**: Displays the hypervisor for the source VMs. You cannot change this setting.
   - **Name**: You can edit the name of the replication group.
   - **Select VMs**: Select the virtual machines to be replicated and click **OK**.
     Only VMs that have been backed up are displayed.
5. Click **Next**.
   The wizard displays the **Replication options** page. You cannot change any of these options.
6. Click **Next**.
   The wizard displays the **Override options** page.
7. To change the destination settings for a VM, click **Yes** and select the VM from the **Virtual machine** list.
   You can edit the following options:
   - **Validate destination VM**
Unconditionally overwrite if it already exists

You can enter the following information:

Amazon target:

- **Change instance display name to**: Shows the display name for the destination instance. You can only change this value when adding a new instance.
- **Availability zone**: Displays the destination zone. You can only change this value when adding a new instance.
- **Network**: Select a network interface for the destination instances. You can only change this value when adding a new instance.
- **Auto select security group**: To specify a specific security group, clear this selection and, from the **Security groups** list, select a security group for the destination instances. You can only change this value when adding a new instance.
- **Amazon buckets**: From this list, select a bucket for the instance volumes. Buckets are logical containers that provide secure access to objects (such as instance volumes). You can only change this value when adding a new instance.
- **Auto select instance type**: To specify a specific instance type, clear this selection and from the **Instance type** list, select an instance type that provides the available CPU cores and memory for the instance. You can only change this value when adding a new instance.

VMware target:

- **VM display name**: Shows the display name for the destination VM. You can only change this value when adding a new VM.
- **Destination host**: Displays the host for the destination VM. You can only change this value when adding a new VM.
- **Datastore**: Displays the datastore to be used for virtual machine disks. You can only change this value when adding a new VM.
- **Resource pool**: Displays the resource pool for the destination VM. You can only change this value when adding a new VM.
- **Network settings**: Click **Add** to create a new mapping between a source network and a destination network.
- **IP address settings**: Click **Add** to customize IP address settings (on page 128).

8. Click **Next**.

The wizard displays the **Summary** page showing the settings for the group definition.

9. Click **Finish** to create the replication group.

---

**Customizing Views for Replication Targets**

You can create views to control the display of entries on the Replication target page.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

**Procedure**

1. From the navigation pane, go to **Configuration > Replication targets**.
   
The Replication target page appears.
2. Click the ‣ icon next to the **Actions** column and then select **Create view**.
3. The Create view dialog box appears.
4. In the **Save view as** box, enter a descriptive name for the view.
5. To make the view the default for the Replication target page, select **Set as default**.
6. To identify targets for the view, click **Add rule**, select one of the following options, and enter a value:
   - **Replication target name**: Enter a name or name pattern to identify replication targets.
   - **Type**: Displays all targets for the hypervisor platform (VMware).
   - **Destination hypervisor**: Enter a name or name pattern to identify hypervisors.
   - **Host**: Enter a name or name pattern to identify host machines.
   - **Proxy**: Enter a name or name pattern to identify proxies.
7. Click **Save**.
   
The Replication target page appears with the label for the currently selected view displayed to the right of the page title.
8. Click the down arrow to the right of the view label and select a view.
   
   Alternatively, click **Reorder** to change the sequence of views, and then click **Apply**. The view listed first identifies the default view for the page.

**Adding a Plan to a Subclient or VM Group**

You can add a virtualization backup and replication plan to a subclient or VM group.

**Procedure**

1. From the navigation pane, display a specific subclient or VM group:
   - Go to **Solutions > Virtualization > Hypervisors**, select a hypervisor, and then select a subclient under the hypervisor.
   - Go to **Solutions > Virtualization > VM groups** and select a group.
2. In the **Plan** area for the subclient or VM group, click **Edit**.
3. From the **Plan** list, select a backup and replication plan.

When a backup and replication plan is assigned, all VMs for a subclient or VM group are replicated according to the settings in the plan.

For more information, see the following topics:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Subclients (VM Groups)
- Adding a Subclient

Monitoring Replication

Use the Replication monitor to view sync status information.

You can also perform failovers for selected VMs.

Procedure

1. From the navigation pane, go to Monitoring > Replication monitor.

The Replication monitor page displays the following information:
   - **VM name**: Name of the virtual machine.
   - **Destination**: Hypervisor for replicated VMs.
   - **Last sync time**: The time when the snapshot was taken during the latest backup of the source VM. The time is shown in the time zone of the backup server.
   - **Last backup time**: The time the last backup was completed.
   - **Backups pending to sync**: Displays the job IDs for any backups that have been performed since the last replication.
   - **Replication schedule**: The name of the schedule created for the replication.
   - **Sync status**: Displays the status of replication operations:
     - **Sync Enabled**: Replication is enabled.
     - **Needs Sync**: The latest backup changes have not yet been replicated to the destination VM.
     - **Sync in Progress**: Replication to the destination VM is in progress.
     - **Sync Paused**: Replication job has been suspended from the Job Controller.
     - **In Sync**: The destination VM has all changes from the source VM since the last backup, as identified by the value displayed for Last Sync Time.
     - **Failed to Sync**: The last attempt to replicate changes failed, and replication is disabled.
     - **Sync Disabled**: Replication is disabled for the virtual machine displayed in the Replication Monitor.
     - **Validation Failed**: The destination virtual machine could not be powered on after the most recent replication, and reverted to its last valid (bootable) state.
   - **Failover/Failback status**: Displays the status of failover or failback operations:
     - **Failover Complete**: Failover to a secondary site completed successfully.
     - **Failover In Progress**: A failover to a secondary site is in progress.
     - **Failover Paused**: A failover job has been suspended.
     - **Failover Failed**: A failover operation failed.
   - **Replication target**: The destination for replications.
2. You can select one or more VMs and then choose one of the following options under **Replication:**

   - **Enable:** Enable replication for the selected VMs. When replication is disabled and then re-enabled, the next scheduled replication will perform full replication on the destination VM.
   - **Disable:** Disable replication for the selected VMs.
   - **Mark for full replication:** Replicate the entire VM from the latest full or synthetic full backup and any subsequent incremental backups. This option is only available for a single VM, and is not available if the **Sync status** for the VM is Sync Disabled, Failed to Sync, Sync in Progress, or Sync Paused. When a VM has been marked for full replication, the status changes to Needs Sync.

3. To initiate a failover to a replication target, select one or more VMs, select **Failover**, and select one of the following values:

   - **Planned:** Performs a planned failover so that you can test the failover process or perform maintenance on your primary site.
     
     **Note:** Planned failover is only supported when the replication schedule is configured to use regular streaming backups. Planned failover is not supported if the schedule is configured to run from IntelliSnap backup copies.

     This option triggers the following actions:
     
     a. Power off the source VMs.
     b. Perform an incremental backup of the source VMs to capture the latest data.
     c. Run replication to apply the most recent updates for destination VMs in the disaster recovery site.
     d. Disable replication for VMs that have failed over.
     e. Power on the destination VMs at the disaster recovery site with appropriate network connections and IP addresses.

     **Note:** You can only modify destination network settings for Windows VMs as part of replication. Linux VMs are replicated without network connections.

   - **Unplanned:** In the event that the primary site is unavailable, this option disables replication and powers up destination VMs at the disaster recovery site with appropriate network connections and IP addresses.

     **Note:** For an unplanned failover, some changes on the source VM might not be synced to the destination VM. For this reason, it is best to use the **Failback** option only after a planned failover.

   - **Test boot VM:** Powers on the destination virtual machines to verify that they are ready for use in the event of a disaster. To avoid conflicts with the source VM and ensure that the virtual machine is not modified by the test boot, this scenario takes a snapshot of the virtual machine before the test boot, boots destination VMs with network connections disabled, and reverts to the snapshot afterwards.

     **Note:** For Test Boot VM, select virtual machines that are part of the same replication schedule.

4. For virtual machines that have been failed over, you can execute a **Failback** operation.
On the **Replication monitor** page, select the rows for one or more virtual machines, and then click **Failback**.

You can only execute a failback operation for virtual machines from the same schedule.

After a failback operation, the next backup of the source VM will be a full backup.
DR Orchestration and Failover Groups

Failover Groups provide orchestration of disaster recovery (DR) operations for a group of virtual machines (VMs), based on Live Sync replication to a DR site.

You can use failover operations for the following scenarios:

- Validate replicated VMs (Test Boot)
- Test failover
- Switch to a DR site for maintenance of the primary site (Planned Failover)
- Make the DR site active in an emergency (Unplanned Failover)

After a failover, you can perform a failback operation to return operations to the primary site.

Failover Groups are available for VMware.

**Test Boot VM**

Test Boot VM allows you to test your DR setup by performing these steps:

1. Take a snapshot of VMs on the DR site.
2. Disable network adapters on VMs on the DR site.
3. Start the VMs on the DR site.
4. Verify the status of VM tools.
5. Revert snapshots of VMs on the DR site.
6. Delete snapshots of VMs on the DR site.

**Test Failover**

A Test Failover operation validates the failover operation for a group of VMs by live mounting replicated VMs to a test site:

1. Run selective backups of VMs on the primary site.
2. Replicate VMs from the primary site.
3. Perform live mounts for the VMs in a failover group based on configured priorities.
4. Based on pre-configuration, stage the VMs in the failover group with an isolated network or without network connections.
5. Start the VMs on the test site.
Planned Failover

A planned failover allows you to back up your production VM and then move production operations to the DR VM by performing these steps:

1. Stop VMs on the primary site.
2. Run selective backups of VMs on the primary site.
3. Replicate VMs from the primary site.
4. Disable Live Sync for VMs on the primary site.
5. Start the VMs on the DR site.

Unplanned Failover

An unplanned failover allows you to power off your production VM and move production operations directly to the DR VM in an emergency situation by performing these steps:

1. Stop VMs on the primary site.
2. Disable Live Sync on VMs on the primary site.
3. Start VMs on the DR site.

Failback

If a failover has completed successfully, then you can perform a failback operation. A failback allows you to update the production VM using an incremental backup of the DR VM and enable Live Sync by performing these steps:

1. Stop VMs on the DR site.
2. Perform incremental backups of VMs on the DR site.
3. Update VMs on the primary site with any changes made since the last full backup.
4. Start VMs on the primary site.
5. Enable Live Sync on VMs on the primary site.

Requirements

- The VSA proxy used for failover and failback operations must be V11 Service Pack 9 or later.
- The source virtual machines in failover groups must meet the following conditions:
  - Configured for replication (Live Sync) (on page 65)
  - Already replicated
  - Running on VMware
• All of the VMs in a failover group must be from the same hypervisor.

**Automatic Failover**

Automatic Failover ensures immediate access to critical virtual machines (VMs) in the event of an outage:

• Continuously monitors VMs that have been configured for Live Sync replication to a secondary site.
• Detects problems with VMs or network access for the primary site.
• Automatically fails over to the secondary site if the VMs in the primary site are disabled or unreachable.
• Brings destination VMs online immediately or after a specified delay.

This feature is available for the Virtual Server Agent with VMware.

**Monitoring and Failover**

To support automatic failover, you must identify three Virtual Server Agent (VSA) proxies that reside in the primary site, to monitor VMs in the source datacenter.

• The first proxy selected during configuration of automatic failover acts as a coordinator to monitor the source VMs.
• Other proxies in the source datacenter act as workers.

Each worker monitors a list of VMs, with the coordinator making assignments as well as monitoring its own list of VMs.

**Monitoring Process**

1. Each worker sends heartbeat packets continuously to the VMs on the list that the worker monitors, and checks responses to determine whether each VM is available or down.
2. Workers communicate with the coordinator to report the states of the VMs they monitor.
3. When necessary, the coordinator initiates an unplanned failover to bring destination VMs online.

**Prerequisites**

• Configure a failover group (on page 80) for virtual machines that need to be monitored.
• Identify three machines in the source datacenter to be used for monitoring. Monitoring machines must meet the following conditions:
  o Use machines that have at least 2 CPU cores.
  o Verify that all monitoring machines are DNS resolvable and can communicate with the Admin Console system, with the virtual machines they are monitoring, and with each other.
  o Set the DNS entries for monitoring machines to the hostnames for the machines.

**Note:** If you define multiple failover groups to support automatic failover, assign a different set of VSA proxies for each failover group.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Verify that all monitoring machines are DNS resolvable and can communicate with the CommServe system, with the virtual machines they are monitoring, and with each other.
- Install the following software on monitoring proxies:
  - Windows Server 2008 R2 or later
  - Virtual Server Agent
  - Java Runtime Environment 8 or later
- Virtual machines being monitored must meet the following requirements:
  - Each virtual machine must have a unique DNS name.
  - VMware Tools must be installed on each VM.

Adding a Failover Group

Add a failover group to provide orchestration for virtual machines from the same hypervisor.

Before You Begin

- To be included in a failover group, virtual machines must already be part of a replication group (on page 69).
- To use a failover group for test failover operations, configure a replication target (on page 67) to support test failover operations.

Procedure

1. From the navigation pane, click Configuration > Failover groups.
   The Failover groups page appears.
2. In the upper right corner of the page, click Add failover group.
   The Add failover group page appears.
3. Enter the following information:
   - **Group name**: Enter a descriptive name for the group.
   - **Machines**:
     - **Server groups / Hypervisors**: You can select server groups or servers (hypervisors) to add all virtual machines that are part of the group or hypervisor and have been configured for replication.
       After adding a group or server, select the check box to the left of each virtual machine that you want to include in the failover group.
     - When you add virtual machines, the table in the **Machines** area is populated.
     - **Name**: Shows the name of the source VM.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Destination name**: Shows the destination name for the VM at the DR site, based on the configuration of the VM for replication.

- **Last sync time**: The time when the snapshot was taken during the latest backup of the source VM.

- **Priority**: As needed, set the priority for each virtual machine. VMs with lower priority numbers will be processed first during failover or failback operations.

- **Actions**: Click the icon to select an action: Add pre script or Add post script.

  - **Group details**:
    - **Priority interval**: Enter a value in minutes to specify how long the failover or failback operation should wait between processing VMs of different priorities.
      
      This setting can be used to enable higher priority machines to start before processing the next set of machines.
    
    - **Continue to next priority on failure**: To continue failover or failback operations when a VM cannot be included in the operation, select this option.
      
      If you do not select this option, the failover or failback operation stops when a VM cannot be processed successfully.
    
    - **Approval required to run tasks**: If failover or failback operations should pend until they are approved by an administrator, select this option.
      
      If you selected Approval required to run tasks, this user must provide approval for the operation before it starts, by clicking the appropriate link in the email that is sent to request approval.
    
    - **User for approval or to notify**: Select a user who should be notified of any failover or failback operations.
      
      If you selected Approval required to run tasks, this user must provide approval for the operation before it starts, by clicking the appropriate link in the email that is sent to request approval.

  - **Auto failover options**: (VMware only) To configure the failover group to monitor VMs and automatically initiate a failover if the VMs in the primary site are disabled or unreachable, enter the following information:
    
    - **Monitoring machines**: To identify machines that can monitor the availability of the VMs in the failover group, select three virtual machines that are configured as proxies for the primary site, and then click OK.
      
      The first proxy selected acts as a coordinator to monitor the source VMs.
    
    - **Delay time before declaring outage**: Enter a value in minutes to indicate how long to wait after detecting an outage before initiating a failover.
      
      When you save the failover group after entering auto failover information, automatic failover is enabled and monitoring begins.
    
      To disable auto failover, you can click Stop monitoring on the page for the failover group.

4. Click **Save**.
Adding a Pre Script

Add a pre script to a machine in a failover group to execute an action on the source VM before a failover operation.

Procedure

1. When adding a failover group, click the icon under the Machines listing and then select Add pre script.

   For an existing failover group, click the icon under the Machines listing and then select Edit prescript.

   The Pre script options dialog box appears.

2. Enter the following information:
   - UNC network path: Enter the full UNC network path for the pre script, including the name of the script.
   - Username: Enter the user name for a user account that has permissions to access the network path for the script.
   - Password: Enter the password for the user account.
   - Confirm password: Re-enter the password.
   - VM guest options: Provide guest VM credentials:
     - Username: Enter the user name for a user account that has permissions to run scripts on the guest VM.
     - Password: Enter the password for the user account.
     - Confirm password: Re-enter the password.

3. Click Save.

Adding a Post Script

Add a post script to a machine in a failover group to execute an action on the destination VM after a failover operation.

Procedure

1. When adding a failover group, click the icon under the Machines listing and then select Add post script.

   For an existing failover group, click the icon under the Machines listing and then select Edit postscript.

   The Post script options dialog box appears.

2. Enter the following information:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- UNC network path: Enter the full UNC network path for the pre script, including the name of the script.
- Username: Enter the user name for a user account that has permissions to access the network path for the script.
- Password: Enter the password for the user account.
- Confirm password: Re-enter the password.
- VM guest options: Provide guest VM credentials:
  - Username: Enter the user name for a user account that has permissions to run scripts on the guest VM.
  - Password: Enter the password for the user account.
  - Confirm password: Re-enter the password.

3. Click Save.

Testing Failover

A Test Failover operation validates the failover operation for a group of VMs by live mounting replicated VMs that are part of a failover group to a test site.

Before You Begin

- Create a replication target (on page 67) that includes test failover options.
- Create a failover group (on page 80) that identifies the VMs to be included. The failover group must specify a replication target that supports test failover operations.

Procedure

1. From the navigation pane, go to Configuration > Failover groups.
   The Failover groups page appears.

2. Under the Actions column, click the icon and select Test failover.

Result

When the test failover operation completes successfully, the users who was configured to receive notifications for failovers receives an email notification that provides a summary of the test failover operation and a link that can be used to access the failover group.
Scheduling Planned Failovers and Test Boots

After you create a failover group, you can edit the group to add schedules for planned failovers or test boots.

Procedure

1. From the navigation pane, click Configuration > Failover groups.
   The Failover groups page appears.
2. Click the name of a failover group.
   The page for the group appears.
3. In the Planned failover schedules area, click Add schedule to create a recurring schedule for planned failovers.
4. In the Test boot schedules area, click Add schedule to create a recurring schedule for test boots of the VMs in the DR site.

Editing a Group

After you create a failover group, you can edit the group to delete the group, change group information, add schedules, add VMs, or perform actions on VMs.

Procedure

1. From the navigation pane, click Configuration > Failover groups.
   The Failover groups page appears.
2. Click the name of a failover group.
   The page for the group appears.
3. To delete the group, click Delete in the upper right corner of the page.
4. To edit the group information, click Edit.
5. In the Planned failover schedules area, click Add schedule to create a recurring schedule for planned failovers.
6. In the Test boot schedules area, click Add schedule to create a recurring schedule for test boots of the VMs in the DR site.
7. In the **Machines** area, click ![icon] and then select an action to perform on a VM.

**Running Orchestration Jobs**

You can perform failover, test boot, or failback operations for groups or for specific machines.

**Procedure**

1. From the navigation pane, click **Configuration > Failover groups**. The **Failover groups** page appears.

2. From the **Actions** column for a group, click ![icon] and then select an action to perform on the group:
   - Delete
   - Planned failover
   - Test boot
   - Test failover
   - Unplanned failover
   Depending on the status of each machine, some failover options might not be completed on all VMs.

3. From the page for a failover group, you can choose failover or failback operations for specific machines.
   The options that are available depend on the current status of the machine. For example, you can request a failback for a machine that has failed over.

4. From the Replication monitor page (on page 74), you can choose failover or failback operations for specific machines.
   The options that are available depend on the current status of the machine. For example, you can request a failback for a machine that has failed over.

You can view the progress of orchestration jobs in the Jobs page (on page 147).

**Backups**

You can run a backup from a subclient for a hypervisor. The storage to be used for backups is configured as part of the subclient.

If backups cannot be performed simultaneously, the backup jobs are queued.
Performing a Virtual Machine Backup

You can run an immediate backup to capture complete virtual machine information or to capture information that has changed since a previous backup. To schedule periodic backups, see Managing Schedules (on page 60).

Note: For virtual machines that are hosted on an SMB share, a Microsoft limitation prevents restore operations from reading file and folder information from a snap backup. To enable restores of guest files and folders from Microsoft Hyper-V backups using a snap plan (on page 137), use the Collect file details option for the subclient.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. In the Subclients area, click the name of the subclient that contains the virtual machines to back up.
4. In the Backup area, click Back up now.
5. In the Backup options dialog box:
   o **Backup level**: Select the backup type. (A full backup is always performed for the first backup of any virtual machine.)
     ▪ **Full**: Perform a full backup for a virtual machine that has previously been backed up. A full backup includes virtual machine configuration files and all virtual machine data disks.
     ▪ **Incremental**: Selected by default. An incremental backup only backs up changes since the last full backup.
     ▪ **Synthetic full**: Create a synthesized backup from the most recent full backup and all subsequent incremental backups.
       An incremental backup is performed first to ensure that the synthetic full backup will be up to date.
       The resulting synthetic full backup is identical to a full backup for the subclient. Unlike full and incremental, a synthetic full backup does not actually transfer data from a client computer to the backup media, and does not use any resources on the client computer.
6. Click OK to begin the backup operation.

Results

The backup operation runs and alerts are triggered based on the success or failure of the backup job. To view the alerts created for your virtual machine backup jobs, go to the Triggered alerts page and filter on the following alert definitions:
VM Backup succeeded
VM Backup failed
VM Backup succeeded with errors

For information about alerts, see Alerts (on page 144).

Backing Up Individual VMs On Demand

You can request an on-demand backup for a specific virtual machine from the Virtual Machines listing.

Before You Begin

- Virtual machines must be backed up at least once before you can request a backup on demand.
- An on-demand VM backup is always an incremental backup.
- If a VM is included in multiple subclients, an on-demand backup is run for the subclient that performed the latest backup of the VM.

Procedure

1. From the navigation pane, select Solutions > Virtualization > Virtual Machines.
2. On the VMs page, click a virtual machine in the Name column.
   The Virtual machines detail page for the VM appears.
3. In the top right corner of the page, click Backup now.
   The Backup options dialog box appears.
4. Click OK.

In the job details, Interactive is displayed as the value for Job started from.

Restores

You can restore virtual machines or virtual machine data from a hypervisor or subclient.

Note: To enable file recovery for UNIX VMs, you must configure a File Recovery Enabler for Linux (on page 36).
Amazon Restores

For Amazon, you can restore full instances or guest files and folders, or restore a volume and attach it to an existing instance.

Restoring Guest Files and Folders for Amazon

You can restore files and folders from an Amazon instance backup to a VSA proxy.

When restoring files from a Linux instance, the File Recovery Enabler specified for the hypervisor (on page 36) is used to recover files.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the instances.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. In the Subclients area, click Restore for the subclient that contains the instance.
4. In the Select restore type page, select Guest files and folders to restore files or folders to the source instance, to another instance, or to a guest agent.
5. In the Restore page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the Name column to browse within an item. For hierarchical data such as files, folders, and disks, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - Show latest backups: Only display data for the most recent backups.
   - Show backups as of a specific date: Only display data up to the date you specify.
   - Show backups for a date range: Only display data within the data range you specify.
6. Click Restore.
7. In the Restore to dialog box, specify the destination for recovered files.
   By default, files are restored to the proxy that performed the backup.
   - To restore in place, leave the value in the Destination list.
   - To restore to a different proxy:
     a. Change the value in the Destination list to use a different proxy.
     b. Optional: To use the Impersonate user option, type the host name and credentials for the new destination.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

By default, the Local System account on the destination client is used to perform the restore operation; but you can use the Impersonate user option to provide credentials for another user account.

The user must have permissions to create files in the specified location on the destination.

c. For the Path box, type a full path or click Browse to select a destination folder.

8. To delete an existing file and replace it with the restored file, select Overwrite if it already exists.
9. Click Submit to run the restore job.

Attaching a Volume to an Existing Amazon Instance

From Amazon instance backups, you can restore an instance volume and attach it to an existing instance.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.

The Hypervisors page appears.

2. Click the name of the hypervisor that hosts the instances.

The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.

3. In the Subclients area, click Restore for the subclient that contains the instance.

4. On the Select restore type page, select Attach volume to restore individual volumes and attach volumes to an existing instance.

5. On the Restore page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the Name column to browse within an item. For hierarchical data such as files, folders, and volumes, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.

In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:

- Show latest backups: Only display data for the most recent backups.
- Show backups as of a specific date: Only display data up to the date you specify.
- Show backups for a date range: Only display data within the data range you specify.

6. Click Restore.

7. In the Restore options dialog box, provide the requested information:

   a. To restore to an instance on a different hypervisor, select the hypervisor name from the Virtualization client list.

   b. Optional: To use a different proxy, select the proxy from the Proxy client list.

      By default, the instance volume is restored using the same proxy as the backup.

   c. To delete an existing volume and replace it with the restored volume, select Overwrite if it already exists.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

d. For each volume you are restoring:
  - **Optional**: Enter a new volume name in the **Change volume name to** box.
    
    If a volume name was not specified for a volume under the source instance, the volume ID for the source volume is displayed for the volume, and the volume ID is used to name the restored volume unless you enter a different value in the **Change volume name to** box for the volume.
  - Click **Browse** next to **Restore to existing instance** and select the instance to which the restored volume should be attached.

8. Click **Submit** to run the restore job.

**Restoring Full Instances for Amazon**

You can restore instances to the original location or to a different location. By default, an instance is restored to the original hypervisor, using the same proxy as the backup.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
   The **Hypervisors** page appears.
2. Click the name of the hypervisor that hosts the instances.
   
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.
3. In the **Subclients** area, click **Restore** for the subclient that contains the instance.
4. In the **Select restore type** page, select **Full instance** to restore a full instance.
5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item.
   
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   
   - **Show latest backups**: Only display data for the most recent backups.
   - **Show backups as of a specific date**: Only display data up to the date you specify.
   - **Show backups for a date range**: Only display data within the data range you specify.
6. Click **Restore**.
7. In the **Restore options** dialog box, provide the requested information:
   
   a. To restore to a hypervisor, select the virtualization client for the cluster from the **Destination Client** list.
   
   b. **Optional**: By default, the preferred VSA proxy for the hypervisor is used for the restore.

      If you select a proxy that is outside of Amazon, the restore uploads volume information to S3 and uses the volumes to create the instance.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

c. **Only required if you chose a proxy that is not an Amazon instance:** From the Amazon buckets list, select a bucket for the instance volumes. Buckets are logical containers that provide secure access to objects (such as instance volumes).

d. **Optional:** Select Power on instance after restore (the default) to start the instance automatically.

e. **Optional:** To delete an existing instance and replace it with the restored instance, select Overwrite instances if they already exist.

f. If you are restoring multiple instances, click the **All Instances** tab on the bottom left to specify configuration values for all instances you are restoring, or the name of each instance to specify values individually. Specify the following values:
   - **Optional:** To change the names of destination instances, select Enable edit destination instance name.
   - **Optional:** When restoring multiple instances, select Prefix or Suffix and enter a string to be appended to the original display name to create new destination instance names.
   - **Optional:** To change the name of an individual instance, select the instance and then enter the new display name in the Change instance display name to box.
     If an existing instance with the same name exists on the destination host and you do not select Overwrite instances if they already exist, the restore job fails.
   - Click Browse to select a value for the Availability zone.
   - From the Instance type list, select an instance type that provides the available CPU cores and memory for the instance.
   - For the Network setting, click Browse to select an EC2 or a VPC network for the restored instances.
   - From the Security groups list, select a security group for the specified network.

8. Click **Submit** to run the restore job.

Azure Restores

For Microsoft Azure, you can restore full VMs or guest files and folders.

**Restoring Guest Files and Folders for Azure**

You can restore files and folders from an Azure virtual machine backup.
Before You Begin

- Use different subclients for UNIX and Windows VMs. You cannot browse and restore files for both operating systems in the same job.
- You cannot restore guest files and folders from Azure backups if Storage Spaces or storage pools were configured inside the guest VM. As a workaround, restore the full virtual machine.
- To restore UNIX files for ext2, ext3, ext4, XFS, JFS, HFS, HFS Plus, and Btrfs file systems, configure the hypervisor to use a File Recovery Enabler for Linux (on page 36).

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. In the Subclients area, click Restore for the subclient that contains the virtual machine.
4. In the Select restore type page, select Guest files to restore files or folders.
5. In the Restore page, expand the tree on the left and select the objects to be restored on the right.
   Select an item or click on an entry in the Name column to browse within an item. For hierarchical data such as files, folders, and disks, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - Show latest backups: Only display data for the most recent backups.
   - Show backups as of a specific date: Only display data up to the date you specify.
   - Show backups for a date range: Only display data within the data range you specify.
6. Click Restore.
7. In the Restore to dialog box, specify the destination for recovered files.
   By default, files are restored to the proxy that performed the backup.
   - To restore in place, leave the value in the Destination list.
   - To restore to a different proxy:
     a. Change the value in the Destination list box to use a different proxy.
     b. Optional: To use the Impersonate user option, type the host name and credentials for the new destination.
        By default, the Local System account on the destination client is used to perform the restore operation; but you can use the Impersonate user option to provide credentials for another user account.
        The user must have permissions to create files in the specified location on the destination.
     c. For the Path box, type a full path or click Browse to select a destination folder.
8. To delete an existing file and replace it with the restored file, select **Overwrite if it already exists**.

9. Click **Submit** to run the restore job.

---

**Restoring Full VMs for Azure**

You can restore virtual machines to the original location or to a different location. By default, a virtual machine is restored to the original hypervisor, using the same proxy as the backup.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**. The **Hypervisors** page appears.

2. Click the name of the hypervisor that hosts the virtual machines.

   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. In the **Subclients** area, click **Restore** for the subclient that contains the virtual machine.

4. In the **Select restore type** page, select **Full virtual machine** to restore one or more full virtual machines.

5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item.

   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - **Show latest backups**: Only display data for the most recent backups.
   - **Show backups as of a specific date**: Only display data up to the date you specify.

6. Click **Restore**.

7. In the **Restore options** dialog box, provide the requested information:
   - The **Azure subscription** list displays the hypervisor for the Azure subscription. Select the Azure subscription client for the restore operation. The subscription type of the virtualization client (Classic or Azure Resource Manager) must match the type of the client for the source VM.
   - Select **Power on VMs after restore** to start the VM automatically.
   - To delete an existing virtual machine and replace it with the restored VM, select **Overwrite VMs if they already exist**.
   - If you are restoring multiple VMs, click the **All VMs** tab on the bottom left to specify configuration values for all VMs you are restoring, or the name of each VM to specify values individually. Specify the following values:
     - **Optional**: To change the names of destination VMs, select **Enable edit destination VM name**.
     - **Optional**: When restoring multiple VMs, select **Prefix** or **Suffix** and enter a string to be appended to the original display name to create new destination VM names.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Optional:** To change the name of an individual VM, enter the new display name in the **Change VM display name to** box.
- **Azure Classic only:** Enter a name in the **Cloud service** box to specify the Cloud Services group for the restored VM.
- **Azure Resource Manager only:** Enter a name in the **Resource group** box to specify the Resource Group for the restored VM.
- For **Storage account**, select the storage account for a virtual machine or disk.
  You can specify any storage account in the same region as the selected cloud service (Classic) or resource group (ARM).
- For **VM size**, select a size specification for the restored virtual machine.
- For **Network interface**, select a network connection for the restored VM, or leave the default value of **Auto Select**.
- **Azure Resource Manager only:** If a public IP address is not required on restored VMs, clear the **Create Public IP** checkbox.
- **Azure Resource Manager only:** For **Security Group**, specify a network security group for the restored VM or leave the default value of **Auto Select**.

8. Click **Submit** to run the restore job.

### Azure Stack Restores

For Microsoft Azure Stack, you can restore full VMs.

### Restoring Full VMs for Microsoft Azure Stack

You can restore virtual machines to the original location or to a different location. By default, a virtual machine is restored to the original hypervisor, using the same proxy as the backup.

### Procedure

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   The **Hypervisors** page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.
3. In the **Subclients** area, click **Restore** for the subclient that contains the virtual machine.
4. In the **Select restore type** page, select **Full virtual machine** to restore one or more full virtual machines.
5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item.

   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - **Show latest backups**: Only display data for the most recent backups.
   - **Show backups as of a specific date**: Only display data up to the date you specify.

6. Click **Restore**.

7. In the **Restore options** dialog box, provide the requested information:
   a. The **Azure subscription** list displays the hypervisor for the Azure Stack subscription. Select the Azure Stack subscription client for the restore operation.
   b. Select **Power on VMs after restore** to start the VM automatically.
   c. To delete an existing virtual machine and replace it with the restored VM, select **Overwrite VMs if they already exist**.
   d. If you are restoring multiple VMs, click the **All VMs** tab on the bottom left to specify configuration values for all VMs you are restoring, or the name of each VM to specify values individually. Specify the following values:
      - **Optional**: To change the names of destination VMs, select **Enable edit destination VM name**.
      - **Optional**: When restoring multiple VMs, select **Prefix** or **Suffix** and enter a string to be appended to the original display name to create new destination VM names.
      - **Optional**: To change the name of an individual VM, enter the new display name in the **Change VM display name to** box.
      - Enter a name in the **Resource group** box to specify the Resource Group for the restored VM.
      - For **Storage account**, select the storage account for a virtual machine or disk.
        You can specify any storage account in the same region as the selected cloud service (Classic) or resource group (ARM).
      - For **VM size**, select a size specification for the restored virtual machine.
      - For **Network interface**, select a network connection for the restored VM, or leave the default value of **Auto Select**.
      - If a public IP address is not required on restored VMs, clear the **Create Public IP** check box.
      - For **Security Group**, specify a network security group for the restored VM or leave the default value of **Auto Select**.

8. Click **Submit** to run the restore job.

---

**Google Cloud Restores**

You can restore instances in place or to a new destination. Restores are supported for both Windows and Linux clients.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

**Restore Process**

1. Create disks that were attached to the instance during backup.
2. Attach disks to proxy.
   
   For each proxy, the maximum number of disks that can be attached is 32. This maximum includes disks belonging to the proxy in addition to disks for an instance being restored.
3. Write data to the disks from the MediaAgent.
4. Detach the disks after writes are complete.
5. Create an instance using the configuration from the config file that was backed up.
6. Attach the restored disks to the instance.

**Restoring Full Instances for Google Cloud Platform**

You can restore one or more instances at a time. Instances can be restored in place (overwriting the source instances) or out of place (with a different instance name, or to a different Google Cloud Platform service account).

**Note:** If an instance is added to subclient content or to a filter by browsing and selecting the instance display name, discovery is performed based on the GUID for the instance. If that instance is later restored in place from a backup, a new GUID is generated, and that instance is no longer identified correctly. To identify that instance, you must remove the old rule, then add a new rule or use a name pattern to select the instance.

**Before You Begin**

- To restore an instance to a different Google Cloud Platform service account, a virtualization client for the service count must exist.
- When restoring out of place, you must specify the destination zone, machine type, and network settings.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
   The **Hypervisors** page appears.
2. Navigate to the hypervisor that hosts the instances, and then click **Restore** for that hypervisor.
3. Select the subclient or instance to restore, and then click **Select Content**.
4. In the **Select restore type** page, select **Full instance** to restore a complete instance to Google Cloud Platform.
5. In the **Restore** page, select the objects to be restored. Select an item or click on an entry in the **Name** column to browse within an item.
In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:

- **Show latest backups**: Only display data for the most recent backups.
- **Show backups as of a specific date**: Only display data up to the date you specify.
- **Show backups for a date range**: Only display data within the data range you specify.

6. Click **Restore**.

7. In the **Restore options** dialog box, provide the requested information:
   - **Destination hypervisor**: To restore to a different Google Cloud Platform deployment, select the hypervisor from the list.
   - **Proxy**: To use a different proxy for the restore, select it from the list.
   - **Restore in place**: By default, this option is enabled. Clear the check box to restore out of place (with a different instance name, or to a different Google Cloud Platform service account).

   When restoring out of place, you must specify the following:
   - **Instance display name**: (when restoring a single instance) Type a new instance name to be used for the restored instance.
   - **All VMs**: (when restoring multiple instances) Select a specific instance from the list so that you can type a new instance name to be used for the restored instance.
   - **Zone**: Click **Browse** to select the destination zone for the out-of-place restore.
   - **Machine Type**: Select the machine type for the out-of-place restore.
   - **External IP**: By default, this option is enabled. Clear the check box to disable.
   - **Network Interface**: Select the network settings.

8. Click **Next**.
   - **Power on VMs after restore**: Select this option to start restored VMs automatically.
   - **Unconditionally overwrite if it already exists**: To delete an existing instance and replace it with the restored instance, select this option.

   **Note**: If an existing instance with the same name exists on the destination host and you do not select **Unconditionally overwrite if it already exists**, the restore job fails.

9. Click **Submit** to run the restore job.

### Hyper-V Restores

For Hyper-V, you can restore full VMs, guest files and folder, or virtual disk files.
Restoring Guest Files and Folders for Hyper-V

You can restore files and folders from a Hyper-V virtual machine backup to the source VM, to another VM, or to a guest agent.

Before You Begin

- For virtual machines that are hosted on an SMB share, a Microsoft limitation prevents restore operations from reading file and folder information from a snap backup. To enable restores of guest files and folders from Microsoft Hyper-V backups using a snap plan (on page 137), enable the Collect file details option on the subclient before performing the backup.

- To restore to a VM, ensure that the following requirements are met:
  - The proxy for the restore must be Hyper-V Server 2012 R2 or later.
  - The guest operating system for the destination VM must be Windows 2008 R2 SP1 or later.
  - The destination VM must have the latest integration services installed.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. In the Subclients area, click Restore for the subclient that contains the virtual machine.
4. In the Select restore type page, select Guest files to restore files or folders to the source virtual machine, to another virtual machine, or to a guest agent.
5. In the Restore page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the Name column to browse within an item. For hierarchical data such as files, folders, and disks, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.

   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - Show latest backups: Only display data for the most recent backups.
   - Show backups as of a specific date: Only display data up to the date you specify.
   - Show backups for a date range: Only display data within the data range you specify.
6. Click Restore.
7. In the Restore options dialog box, provide the requested information:
   a. To restore in place:
      i. Ensure that the source VM is selected (the default option).
      ii. Optional: Change the value in the Proxy box to use a different proxy.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

For Hyper-V, all Hyper-V nodes are displayed.

b. To restore to a different VM:
   i. Select Other VM.
      By default, the same proxy that was used for the backup performs the restore.
   ii. Optional: Change the value in the Proxy box to use a different proxy.
      The proxy must be Hyper-V Server 2012 R2 or later.
   iii. If the destination VM resides on another hypervisor, select the host name of the hypervisor from the Destination hypervisor list, and then browse to select the destination VM.
      The guest operating system for the destination VM must be Hyper-V 2008 R2 SP1 or later, and the destination VM must have the latest integration services installed.
   iv. In the Virtual machine login area, type the username and password for the destination VM.

c. To restore to a guest agent:
   i. Select Guest agent.
   ii. Select the guest agent from the Destination list.
      By default, the Local System account on the destination client is used to perform the restore operation; but you can use the Impersonate user option to provide credentials for another user account.
   iii. Optional: To use the Impersonate user option, type the host name and credentials for the new destination hypervisor.
      The user must have permissions to create files in the specified location on the destination.

8. For the Path box, type a full path for the location where files should be restored.

9. To delete an existing file and replace it with the restored file, select Overwrite if it already exists.

10. Click Submit to run the restore job.

Restoring Full Virtual Machines for Hyper-V

You can restore virtual machines to the original location or to a different location. By default, a virtual machine is restored to the original hypervisor, using the same proxy as the backup.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. In the Subclients area, click Restore for the subclient that contains the virtual machine.
4. In the **Select restore type** page, select **Full virtual machine** to restore one or more full virtual machines.

5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item.

   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - **Show latest backups**: Only display data for the most recent backups.
   - **Show backups as of a specific date**: Only display data up to the date you specify.
   - **Show backups for a date range**: Only display data within the data range you specify.

6. Click **Restore**.

7. In the **Restore options** dialog box, provide the requested information:
   a. To restore to a different cluster, select the virtualization client for the cluster from the **Virtualization Client** list.
   b. Select the target host from the **Destination Client** list.
      
      All Hyper-V nodes are displayed.
   c. Select **Power on VMs after restore** to start the VM automatically.
   d. To delete an existing virtual machine and replace it with the restored VM, select **Overwrite VMs if they already exist**.
   e. Select **Register virtual machine with failover cluster** to enable the restored VM to migrate to another node in the cluster.
   f. For **Restore location**, leave the default (**Original folder**), choose **Select a folder**, or select **Hyper-V default folder**.
   g. Type a new virtual machine name in the **Change VM display name to** box.
      
      This option does not display if you are restoring multiple VMs. If an existing VM with the same name exists on the destination host and you do not select **Overwrite VMs if they already exist**, the restore job fails.
   h. For **Destination folder**, click **Browse** to select a new folder from the list. (Only enabled if you chose **Select a folder**.)

8. Click **Submit** to run the restore job.

---

**Nutanix AHV Restores**

For Nutanix AHV, you can restore full VMs or guest files and folders.

**Restoring Guest Files and Folders for Nutanix AHV**

You can restore guest files and folders from virtual machine backups to a physical or virtual machine. You can only restore files or folders to the source VM if a file system agent is installed on the source VM.
When restoring files from a Linux VM, the File Recovery Enabler specified for the hypervisor (on page 36) is used to recover files.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
   The **Hypervisors** page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.
3. In the **Subclients** area, click **Restore** for the subclient that contains the virtual machine.
4. In the **Select restore type** page, select **Guest files**.
5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right.
   
   Select an item or click on an entry in the **Name** column to browse within an item. For hierarchical data such as files, folders, and disks, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.
   
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   
   - **Show latest backups**: Only display data for the most recent backups.
   - **Show backups as of a specific date**: Only display data up to the date you specify.
   - **Show backups for a date range**: Only display data within the data range you specify.
6. Click **Restore**.
7. In the **Restore to** dialog box, specify the destination for recovered files.
   
   By default, files are restored to the proxy that performed the backup.
   
   a. To restore in place, leave the value in the **Destination** list.
   
   b. **Optional**: To use the **Impersonate user** option, type the host name and credentials for the new destination.
      
      By default, the Local System account on the destination client is used to perform the restore operation; but you can use the **Impersonate user** option to provide credentials for another user account.
      
      The user must have permissions to create files in the specified location on the destination.
   
   c. For the **Path** box, type a full path or click **Browse** to select a destination folder.
8. To delete an existing file and replace it with the restored file, select **Overwrite if it already exists**.
9. Click **Submit** to run the restore job.

**Restoring Full Virtual Machines for Nutanix Acropolis**

You can restore virtual machines to the original location or to a different location. By default, a virtual machine is restored to the original hypervisor, using the same proxy as the backup.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.

3. In the Subclients area, click Restore for the subclient that contains the virtual machine.

4. In the Select restore type page, select Full virtual machine to restore one or more full virtual machines.

5. In the Restore page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the Name column to browse within an item.
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - Show latest backups: Only display data for the most recent backups.
   - Show backups as of a specific date: Only display data up to the date you specify.
   - Show backups for a date range: Only display data within the data range you specify.

6. Click Restore.

7. In the Restore options dialog box, provide the requested information:
   a. To use a different proxy for the restore, select it from the Proxy list.
   b. To restore to a different cluster, select the hypervisor from the Destination hypervisor list.
   c. Select Power on VMs after restore to start the VM automatically.
   d. To delete an existing virtual machine and replace it with the restored VM, select Overwrite if it already exists.
   e. Type a new virtual machine name in the Change VM display name to box.
      This option does not display if you are restoring multiple VMs. If an existing VM with the same name exists on the destination host and you do not select Overwrite VMs if they already exist, the restore job fails.
   f. From the Container list, select a storage location for disks.
   g. From the VLAN ID list, select a network adapter that is available at the destination.

8. Click Submit to run the restore job.

OpenStack Restores

You can restore instances or images in place or to a new destination. You can also restore guest files and folders.

Restores are supported for both Windows and Linux clients.
Note: For both in-place and out-of-place restores, the restored instance is assigned a new instance ID that is different from the source instance.

Restore Processes

The stages of the restore process depend on how the source instance or image was configured.

Restoring Full Instances When the Boot Disk Is an Image

1. Create a cinder volume that is the same size as the OS disk in the source VM.
2. Attach the cinder volume to the VSA proxy.
3. Restore data received from the MediaAgent into the attached volume.
4. Detach the volume.
5. Create a new image from the restored cinder volume.
6. For cinder data volumes, the restore process includes the following stages:
   a. Create cinder volumes.
   b. Attach volumes to the VSA proxy.
   c. Restore data received from the MediaAgent into the attached volumes.
      Up to 25 volumes can be attached to the VSA proxy during restores, occupying device slots vdb-vdz.
   d. Detach the volumes.
7. Launch an instance from the new image.
8. Attached the restored data volumes to the newly launched instance.
9. Delete the operating system volume and image that were created to perform the restore.

Restoring Full Instances When the Boot Disk is a Cinder Volume

1. Create a cinder volume that is the same size as the OS disk in the source VM.
2. Create data volumes.
3. Attach volumes to the VSA proxy.
4. Restore data received from the MediaAgent into the attached volumes.
   Up to 25 volumes can be attached to the VSA proxy during restores, occupying device slots vdb-vdz.
5. Detach the volumes.
6. Launch an instance from the restored operating system volume.
7. Attach the restored data volumes to the newly launched instance.
Restoring a Flat Image

1. Create an image on the specified destination.
2. Restore data received from the MediaAgent into the image using direct uploads.

Restoring Full Instances for OpenStack

You can restore instances or images to the original location or to a different location. By default, an instance is restored to the original hypervisor, using the same proxy as the backup.

Restore Considerations

- If the OS disk was filtered from the backup of an instance, the base image that the instance was based on must be available for the instance to be restored.
- If an instance or image is added to subclient content or to a filter by browsing and selecting the display name, discovery is performed based on the GUID for the instance or image. If that instance or image is later restored in place from a backup, a new GUID is generated, and that instance or image is no longer identified correctly. To identify that instance or image, you must remove the old rule, then add a new rule or use a name pattern to select the instance or image.
- If the user specified for the virtualization client does not have permission to create or delete network ports, the restore fails with error "Failed to create port with request".
- When restoring public images for a project, the user performing the restore should have the Admin role for that project. When a user only has the Member role for a project, that user does not have permission to create public images and can only restore an image as a private image. In that situation, an Admin user could later make the restored image public.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors. The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the instances.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. In the Subclients area, click Restore for the subclient that contains the instance.
4. In the Select restore type page, select Full instance to restore a full instance.
5. In the Restore page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the Name column to browse within an item.
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - Show latest backups: Only display data for the most recent backups.
   - Show backups as of a specific date: Only display data up to the date you specify.
o **Show backups for a date range**: Only display data within the data range you specify.

6. Click **Restore**.

7. In the **Restore options** dialog box, provide the requested information:
   a. **Optional**: By default, the preferred VSA proxy for the hypervisor is used for the restore. You can select a different proxy from the **Proxy** list.
   b. To restore to a hypervisor, select the virtualization client for the cluster from the **Destination hypervisor** list.
   c. **Optional**: Select **Power on instance after restore** to start the instance automatically.
   d. **Optional**: To delete an existing instance and replace it with the restored instance, select **Overwrite if it already exists**.
   e. If you are restoring multiple instances, click the **All Instances** tab on the bottom left to specify configuration values for all instances you are restoring, or the name of each instance to specify values individually. Specify the following values:
      - **Optional**: To change the names of destination instances, select **Enable edit destination instance name**.
      - **Optional**: When restoring multiple instances, select **Prefix** or **Suffix** and enter a string to be appended to the original display name to create new destination instance names.
      - **Optional**: To change the name of an individual instance, select the instance and then enter the new display name in the **Change instance display name to** box.
        If an existing instance with the same name exists on the destination host and you do not select **Overwrite if it already exists**, the restore job fails.
      - From the **Availability zone** list, click **Browse** to browse defined availability zones and select a host.
      - From the **Volume type** list, select a volume type that is defined for the zone of the source volumes.
      - From the **Flavor** list, select a flavor that is at or above the original configuration.
      - From the **Security Group** list, select a predefined security group that defines the required network access.
      - From the **Key Pair** list, select a key pair that identifies the ownership for the converted instance.
      - From the **Network Interface** list, select a network interface that is available in the destination.

8. Click **Submit** to run the restore job.

---

**Restoring Guest Files and Folders for OpenStack**

You can restore files and folders from a backup of an OpenStack instance or image to a VSA proxy.

When restoring files from a Linux instance, the File Recovery Enabler specified for the hypervisor (on page 36) is used to recover files.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Procedure

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   The **Hypervisors** page appears.
2. Click the name of the hypervisor that hosts the instances.
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.
3. In the **Subclients** area, click **Restore** for the subclient that contains the instance.
4. In the **Select restore type** page, select **Guest files and folders** to restore files or folders to the source instance, to another instance, or to a guest agent.
5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item. For hierarchical data such as files, folders, and disks, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - **Show latest backups**: Only display data for the most recent backups.
   - **Show backups as of a specific date**: Only display data up to the date you specify.
   - **Show backups for a date range**: Only display data within the data range you specify.
6. Click **Restore**.
7. In the **Restore to** dialog box, specify the destination for recovered files.
   By default, files are restored to the proxy that performed the backup.
   - To restore in place, leave the value in the **Destination** list.
   - To restore to a different proxy:
     a. Change the value in the **Destination** list to use a different proxy.
     b. **Optional**: To use the **Impersonate user** option, type the host name and credentials for the new destination.
        By default, the Local System account on the destination client is used to perform the restore operation; but you can use the **Impersonate user** option to provide credentials for another user account.
        The user must have permissions to create files in the specified location on the destination.
     c. For the **Path** box, type a full path or click **Browse** to select a destination folder.
8. To delete an existing file and replace it with the restored file, select **Overwrite if it already exists**.
9. Click **Submit** to run the restore job.

Oracle Cloud Classic Restores

From Oracle Cloud Classic backups, you can restore guest files or full instances.
Considerations

Oracle Cloud Classic storage volumes can be up to 2 TB, and a maximum of 10 storage volumes can be attached to each instance. For backups and restores, volumes for an instance are attached to the VSA proxy, and the limit on the number of volumes applies to the total number of volumes for the proxy and the instance being backed up or restored.

Restore Process

1. Read volume information from the instance backup.
2. Create volumes and attach them to the VSA proxy.
3. Restore data received from the MediaAgent into the attached volumes, and then detach the volumes from the VSA proxy.
4. Mark the OS disk as bootable.
5. Read the orchestration JSON file and use the options specified for the restore to create an instance using the Oracle Launch API.

Note: The Oracle Launch API does not create orchestration entries for restored instances or instances created during application migration to Oracle Cloud Classic. As a result, you cannot shut down such instances from the Oracle Cloud Classic interface.

Restoring Guest Files for Oracle Cloud Classic

You can restore guest files and folders from instance backups to a physical machine or an instance. You can only restore files or folders to the source instance if a file system agent is installed on the source VM.

When restoring files from a Linux instance, the File Recovery Enabler specified for the hypervisor (on page 36) is used to recover files.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the instances.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. In the Subclients area, click Restore for the subclient that contains the instance.
4. In the Select restore type page, select Guest files.
5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item. For hierarchical data such as files, folders, and disks, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.

In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:

- **Show latest backups**: Only display data for the most recent backups.
- **Show backups as of a specific date**: Only display data up to the date you specify.
- **Show backups for a date range**: Only display data within the data range you specify.

6. Click **Restore**.

7. In the **Restore to** dialog box, specify the destination for recovered files.

By default, files are restored to the proxy that performed the backup.

a. To restore in place, leave the value in the **Destination** list.

b. **Optional**: To use the **Impersonate user** option, type the host name and credentials for the new destination.

   By default, the Local System account on the destination client is used to perform the restore operation; but you can use the **Impersonate user** option to provide credentials for another user account.

   The user must have permissions to create files in the specified location on the destination.

c. For the **Path** box, type a full path or click **Browse** to select a destination folder.

8. To delete an existing file and replace it with the restored file, select **Overwrite if it already exists**.

9. Click **Submit** to run the restore job.

### Restoring Full Instances for Oracle Cloud Classic

You can restore instances to the original location or to a different location. By default, an instance is restored to the original hypervisor, using the same proxy as the backup.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.

   The **Hypervisors** page appears.

2. Click the name of the hypervisor that hosts the instances.

   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. In the **Subclients** area, click **Restore** for the subclient that contains the instance.

4. In the **Select restore type** page, select **Full instance** to restore a full instance.

5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:

- **Show latest backups**: Only display data for the most recent backups.
- **Show backups as of a specific date**: Only display data up to the date you specify.
- **Show backups for a date range**: Only display data within the data range you specify.

6. Click **Restore**.

7. In the **Restore options** dialog box, provide the requested information:
   a. To restore to a different endpoint, select the hypervisor for the endpoint from the **Destination hypervisor** list.
   b. **Optional**: By default, the preferred VSA proxy for the hypervisor is used for the restore. You can select a different Oracle Cloud Classic proxy from the **Proxy client** list.
   c. **Optional**: Select **Power on instance after restore** (the default) to start the instance automatically.
   d. If you are restoring multiple instances, click the **All Instances** tab on the bottom left to specify configuration values for all instances you are restoring, or the name of each instance to specify values individually. Specify the following values:
      - When restoring a single instance, in the **Change instance display name to** box, enter a new display name for the instance.
      - From the **User account** list, select the user for the destination endpoint.
      - From the **Instance shape** list, select an instance shape that is at or above the level of the source instances.
      - In the **Network** box, select a network for the destination instances.
      - In the **Security groups** box, select a security group for the specified network.
      - In the **SSH keys** box, select a predefined SSH key for the destination instances.

8. Click **Submit** to run the restore job.

Oracle VM Restores

You can restore virtual machines in place or to a new destination. You can also restore guest files and folders.

Restores are supported for both Windows and Linux clients.

Restoring Guest Files for Oracle VM

You can restore guest files and folders from virtual machine backups.

When restoring files from a Linux instance, the File Recovery Enabler specified for the hypervisor (on page 36) is used to recover files.
Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.

2. Click the name of the hypervisor that hosts the instances.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.

3. In the Subclients area, click Restore for the subclient that contains the instance.
   The Select restore type page appears.

4. Select Guest files and folders.

5. In the Restore page, expand the tree on the left and select the objects to be restored on the right.
   Select an item or click on an entry in the Name column to browse within an item. For hierarchical data such as files, folders, and disks, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - Show latest backups: Only display data for the most recent backups.
   - Show backups as of a specific date: Only display data up to the date you specify.
   - Show backups for a date range: Only display data within the data range you specify.

6. Click Restore.

7. In the Restore to dialog box, specify the destination for recovered files.
   By default, files are restored to the proxy that performed the backup.
   a. To restore in place, leave the value in the Destination list.
   b. Optional: To use the Impersonate user option, type the host name and credentials for the new destination.
      By default, the Local System account on the destination client is used to perform the restore operation; but you can use the Impersonate user option to provide credentials for another user account.
      The user must have permissions to create files in the specified location on the destination.
   c. For the Path box, type a full path or click Browse to select a destination folder.

8. To delete an existing file and replace it with the restored file, select Unconditionally overwrite if it already exists.

9. Click Submit to run the restore job.

Restoring Full VMs for Oracle VMs

You can restore one or more virtual machines at a time. A virtual machines can be restored in place (overwriting the source virtual machine) or out of place (with a different VM name, or to a different server).
Note: You cannot restore a virtual machine to a version that is lower than the version of the VM that was backed up.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors. The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. In the Subclients area, click Restore for the subclient that contains the virtual machine.
4. In the Select restore type page, select Full virtual machine to restore one or more full virtual machines.
5. In the Restore page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the Name column to browse within an item.
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - Show latest backups: Only display data for the most recent backups.
   - Show backups as of a specific date: Only display data up to the date you specify.
   - Show backups for a date range: Only display data within the data range you specify.
6. Click Restore.
7. In the Restore options dialog box, provide the requested information:
   - Restore as: Leave the default value, Oracle VM.
   - Destination hypervisor: To restore to a different Oracle VM Manager deployment, select the hypervisor from the list.
   - Proxy: To use a different proxy for the restore, select it from the list.
   If you are restoring multiple VMs, you can select the All VMs tab to specify options for all of the VMs in the job, or a specific VM to specify options for that VM.
   - VM display name: (when restoring a single VM) Type a new virtual machine name to be used for the restored VM.

   Note: If an existing VM with the same name exists on the destination host and you do not select Unconditionally overwrite if it already exists, the restore job fails.

   - Enable edit destination VM name: (when restoring multiple VMs) Select this option and enter a prefix or suffix to be added to the source VM name to create each destination VM name.
   - Destination server: Click Browse to select the destination server to host the restored VM.
   - Repository: Select a repository for virtual machine disks from the list.
8. Click Next.
   - Power on VMs after restore: Select this option to start restored VMs automatically.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Unconditionally overwrite if it already exists**: To delete an existing virtual machine and replace it with the restored VM, select this option.
- **Disk Provisioning**: Select one of the following options:
  - **Original**: Use the same disk provisioning method as the source VM.
  - **Sparse**: Use sparse provisioning to write data to disk as needed.
  - **Non-sparse**: Use non sparse provisioning to write the entire disk when it is provisioned.

9. Click **Submit** to run the restore job.

VMware Restores

For VMware virtual machines, you can restore full VMs, guest files and folders, or disk files, and you can restore a disk and attach it to an existing VM.

You can also convert a VMware VM backup to Hyper-V.

Restoring Guest Files and Folders for VMware

You can restore files and folders from a VMware virtual machine backup to the source VM, to another VM, or to a guest agent.

When restoring files from a Linux VM, the File Recovery Enabler specified for the hypervisor (on page 36) is used to recover files.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**. The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   - The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. In the Subclients area, click **Restore** for the subclient that contains the virtual machine.
4. In the Select restore type page, select **Guest files** to restore files or folders to the source virtual machine, to another virtual machine, or to a guest agent.
5. In the Restore page, expand the tree on the left and select the objects to be restored on the right.
   - Select an item or click on an entry in the Name column to browse within an item. For hierarchical data such as files, folders, and disks, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.
   - In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
     - **Show latest backups**: Only display data for the most recent backups.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Show backups as of a specific date**: Only display data up to the date you specify.
- **Show backups for a date range**: Only display data within the data range you specify.

6. Click **Restore**.

7. In the **Restore options** dialog box, specify the destination for recovered files.
   By default, files are restored to the source VM, using the same proxy as the backup.
   a. To restore in place:
      i. Select the radio button for the source VM.
      ii. **Optional**: Change the value in the **Proxy** box to use a different proxy.
      iii. In the **Virtual machine login** area, type the username and password for the destination VM.
   b. To restore to a different VM:
      i. Select **Other VM**.
         By default, the same proxy that was used for the backup performs the restore.
      ii. **Optional**: Change the value in the **Proxy** box to use a different proxy.
      iii. If the destination VM resides on another hypervisor, select the host name of the hypervisor from the **Destination hypervisor** list, and then browse to select the destination VM.
      iv. In the **Virtual machine login** area, type the username and password for the destination VM.
   c. To restore to a guest agent:
      i. Select **Guest agent**.
      ii. Select the guest agent from the **Destination** list.
         By default, the Local System account on the destination client is used to perform the restore operation; but you can use the **Impersonate user** option to provide credentials for another user account.
      iii. **Optional**: To use the Impersonate user option, type the host name and credentials for the new destination hypervisor.
         The user must have permissions to create files in the specified location on the destination.

8. For the **Path** box, type a full path or click **Browse** to select a destination folder. (For VMware, this value is only needed when you are restoring to a guest agent.)

9. To delete an existing file and replace it with the restored file, select **Overwrite if it already exists**.

10. Click **Submit** to run the restore job.

**Attaching a Disk to an Existing VM for VMware**

From VMware virtual machine backups, you can restore a virtual machine disk and attach it to an existing VM.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Procedure

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
   The Hypervisors page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. In the **Subclients** area, click **Restore** for the subclient that contains the virtual machine.

4. On the **Select restore type** page, select **Disk Level** to restore individual VMDK files and attach VMDKs to an existing virtual machine.

5. On the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item. For hierarchical data such as files, folders, and disks, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.

   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   
   - **Show latest backups**: Only display data for the most recent backups.
   - **Show backups as of a specific date**: Only display data up to the date you specify.
   - **Show backups for a date range**: Only display data within the data range you specify.

6. Click **Restore**.

7. In the **Restore options** dialog box, provide the requested information:
   
   a. **Optional**: To use a different proxy, select the proxy from the **Proxy** list.
      
      By default, the virtual machine disk is restored using the same proxy as the backup.
   
   b. To restore to a VM on a different hypervisor, select the hypervisor name from the **Destination hypervisor** list.
   
   c. To delete an existing virtual disk file and replace it with the restored file, select **Overwrite if it already exists**.
   
   d. For **Disk Provisioning**, use the default value (**Original**) to retain the provisioning method used at the time of backup. Select a value from the **Disk Provisioning** list to force a specific disk provisioning method: **Thick Lazy Zero, Thin, or Thick Eager Zero**.
   
   e. For **Transport mode for VMware**, select one of the following options:
      
      - **Auto**: The transport mode is selected automatically based on the backup environment:
         
         If the datastore is accessible to a physical proxy, SAN is used.
         
         If the datastore is accessible to the ESX server for a virtual proxy, HotAdd is used.
         
         Otherwise, NBD is used.
      
      - **SAN**: For directly connected storage using Fibre Channel (FC) or Internet SCCI (iSCSI) protocols. The Virtual Server Agent must have access to the datastore LUNs (logical drives) that provide storage for virtual machine disks. Data is read directly from the storage where virtual machines reside, without going through the ESX host or transferring data over the local area network (LAN). The ESX host is contacted only to coordinate access to the LUN. SAN transport mode cannot be used if the proxy computer is a virtual machine.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Hot Add**: The Virtual Server Agent is installed on a virtual machine residing on an ESX server. In HotAdd mode, the data volumes containing the virtual machines to be backed up are automatically mounted to the proxy, so they can be accessed by the proxy as a local disk. The ESX host the proxy is running on must have access to all datastores for the virtual machine. If the virtual machine and the proxy are not on the same host, all datastores must be shared between the hosts.

- **NBD**: Data is transferred using the TCP/IP connection between the ESX server and the proxy computer. The local area network (LAN) can be the production network or a dedicated backup network.

- **NBD SSL**: Similar to NBD mode, but data transfer between the proxy computer and the ESX server is encrypted. Encryption should be used for sensitive information, even within a private network.

f. For each disk you are restoring, click **Browse** next to **Destination VM** and select the virtual machine to which the restored disk should be attached.

g. To use a different datastore for the restored VM disk, select the new datastore from the **Datastore** list.

8. Click **Submit** to run the restore job.

**Restoring Full Virtual Machines for VMware**

You can restore virtual machines to the original location or to a different location. By default, virtual machines are restored to the original hypervisor, using the same proxy as the backup.

If the hypervisor is configured to support vCloud Director (on page 36), you can restore a virtual machine to vCloud.

**Live Recovery**

The Live Recovery feature enables virtual machines (VMs) to be recovered and powered on from a backup without waiting for a full restore of the VM. This feature can be used to recover a VM that has failed and needs to be placed back in production quickly, or to validate that a backup can be used in a disaster recovery scenario.

Live recovery is supported from streaming backups or from IntelliSnap backups using the Pure Storage array.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.

   The **Hypervisors** page appears.

2. Click the name of the hypervisor that hosts the virtual machines.

   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. In the **Subclients** area, click **Restore** for the subclient that contains the virtual machine.
4. In the **Select restore type** page, select **Full virtual machine** to restore one or more full virtual machines.

5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item.

   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - **Show latest backups**: Only display data for the most recent backups.
   - **Show backups as of a specific date**: Only display data up to the date you specify.
   - **Show backups for a date range**: Only display data within the data range you specify.

6. Click **Restore**.

   The **Restore options** dialog box appears.

7. To restore to a different hypervisor, select the target environment from the **Restore as** list.

   By default, the **Restore as** list shows the source hypervisor.

   The options for the restore vary depending on the hypervisor type.

   **Amazon**:
   - **Destination client**: Select the virtualization client for the cluster from the list.
   - **Proxy client**: By default, the preferred VSA proxy for the hypervisor is used for the restore.
     - If you select a proxy that is outside of Amazon, the restore uploads volume information to S3 and uses the volumes to create the instance.
   - **Amazon buckets**: Select a bucket for the instance volumes. Buckets are logical containers that provide secure access to objects (such as instance volumes).
   - **Power on instance after restore**: Select this option to start the instance automatically.
   - **Unconditionally overwrite if it already exists**: Select this option to delete an existing instance and replace it with the restored instance.
   - **Change instance display name to**: Enter the new display name for the instance.
   - **Availability zone**: Select the destination zone.
   - **Instance type**: Select an instance type that provides the available CPU cores and memory for the instance.
   - **Network**: Click **Browse** to select an EC2 or a VPC network for the restored instances.
   - **Security groups**: Select a security group for the specified network.

   **VMware vCenter**:
   - **Destination hypervisor**: To restore to a different vCenter, select the hypervisor for the vCenter from the list.
   - **Proxy**: (Optional) To use a different proxy, select the proxy from the list.
   - **Select a different vCenter**: To restore to a different vCenter, select this option and provide the vCenter name and credentials.
     - a. In the **vCenter** box, enter the IP address of the vCenter or an ESX server.
     - b. Provide the user credentials in the **Username** and **Password** boxes.
   - **Restore in place**: This option is selected by default. Clear the selection to provide information for an out-of-place restore.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- VM display name: Type a new virtual machine name in the box.
  If an existing VM with the same name exists on the destination host and you do not select **Overwrite VMs if they already exist**, the restore job fails.

- Destination host: To restore to a different host, click **Browse** and select the host. By default, the original host is shown as the destination host.

- Datastore: To use a different data store for the restored VM and disks, select the new data store from the list.

- Resource pool: To restore to a resource pool, select the destination from the list.

**Note:** The Resource pool list is only displayed when you are restoring to a vCenter.

- VM folder path: To restore to a folder, click **Browse** and select the destination folder.

- Network settings: The Network settings dialog box shows the source source and destination networks for the VM being restored.
  Click the pencil icon to edit a network mapping, or **Add** to add a new mapping.
  - Source network: Select the source network, or select Any Network to map all network connections for the source VM to a different network for the restored VM.
  - Destination network: Select a network connection for the restored VM, or select No Connection to restore without a network connection.
  Click OK to save changes.

- IP address settings: Click the pencil icon to edit a IP address mapping, or **Add** to add a new mapping.
  The Edit IP address settings or IP address settings dialog box appears.
  Specify address mappings as needed:
  IP address mapping (on page 128)
  Click OK to save changes.

**vCloud restores:** If the hypervisor supports vCloud Director, select **Restore to vCloud** to display additional vCloud options.

- Show vCloud options: Select this option to display vApp configuration settings.

- Restore vApp configuration: Select this option to restore the vApp configuration.
  Selecting this option restores the vApp network configuration, lease configuration, and virtual machine startup order of the source VM to the new vApp.

- Provide the following information:
  - Organization: Enter the name of the target organization.
  - Org vDC: Enter the name of the organization vDC to be used for the restored VM.
  - vApp name: Enter the name of the vApp to which the VM should be restored. If the specified vApp does not exist, one will be created using the name you enter.
  - vApp owner: Enter the name of the user who owns the destination vApp.
  - Network adapter: Select a network adapter for the restored VM.

8. Click **Next**.
The second page of the **Restore options** dialog box appears.

Provide the following information:

- **Power on VMs after restore**: Select this option to start the VM automatically.
- **Unconditionally overwrite if it already exists**: Select this option to delete an existing virtual machine and replace it with the restored VM.
- **Disk Provisioning**: Use the default value (**Original**) to retain the provisioning method used at the time of backup. Select a value from the **Disk Provisioning** list to force a specific disk provisioning method: **Thick Lazy Zero**, **Thin**, or **Thick Eager Zero**.
- **Transport mode for VMware**: Select one of the following options:
  - **Auto**: The transport mode is selected automatically based on the backup environment:
    - If the datastore is accessible to a physical proxy, SAN is used.
    - If the datastore is accessible to the ESX server for a virtual proxy, HotAdd is used.
    - Otherwise, NBD is used.
  - **SAN**: For directly connected storage using Fibre Channel (FC) or Internet SCCI (iSCSI) protocols. The Virtual Server Agent must have access to the datastore LUNs (logical drives) that provide storage for virtual machine disks. Data is read directly from the storage where virtual machines reside, without going through the ESX host or transferring data over the local area network (LAN). The ESX host is contacted only to coordinate access to the LUN. SAN transport mode cannot be used if the proxy computer is a virtual machine.
  - **Hot Add**: The Virtual Server Agent is installed on a virtual machine residing on an ESX server. In HotAdd mode, the data volumes containing the virtual machines to be backed up are automatically mounted to the proxy, so they can be accessed by the proxy as a local disk. The ESX host the proxy is running on must have access to all datastores for the virtual machine. If the virtual machine and the proxy are not on the same host, all datastores must be shared between the hosts.
  - **NBD**: Data is transferred using the TCP/IP connection between the ESX server and the proxy computer. The local area network (LAN) can be the production network or a dedicated backup network.
  - **NBD SSL**: Similar to NBD mode, but data transfer between the proxy computer and the ESX server is encrypted. Encryption should be used for sensitive information, even within a private network.
- **Restore virtual machine using live recovery (vMotion)**: Select this option to use the live recovery option.
  - **Redirect writes to datastore**: (Optional) Select a datastore for redirect writes. The redirect writes datastore must be different from the destination datastore for the restored VM.
  - **Delay migration**: Delay the migration of the VM to the destination location for the specified time (0-12 hours). You can still use the VM when delaying the migration.

9. Click **Submit** to run the restore job.

**Restoring Virtual Machine Disk Files**

You can restore virtual machine disk files for VMware or Hyper-V.
Procedure

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   The **Hypervisors** page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. In the **Subclients** area, click **Restore** for the subclient that contains the virtual machine.

4. In the **Select restore type** page, select **Virtual machine files** to restore virtual machine configuration and disk files to the file system of the proxy.

5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item. For hierarchical data such as files, folders, and disks, you can click an entry in the path listing above the right pane to return to a higher level of the hierarchy.

   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - **Show latest backups**: Only display data for the most recent backups.
   - **Show backups as of a specific date**: Only display data up to the date you specify.
   - **Show backups for a date range**: Only display data within the data range you specify.

6. Click **Restore**.

7. In the **Restore options** dialog box, provide the requested information:
   a. To restore to a different hypervisor, select the hypervisor name from the **Destination hypervisor** list.
      By default, virtual machine disk files are restored to the original hypervisor.
   b. **Optional**: Use the **Impersonate user** option to provide credentials for another user account.
      By default, the Local System account on the destination client is used to perform the restore operation. The user must have permissions to create files in the specified location on the destination.
   c. For the **Path** box, type a full path or click **Browse** to select a destination folder.
   d. To delete an existing file and replace it with the restored file, select **Overwrite if it already exists**.

8. Click **Submit** to run the restore job.

Cross-Hypervisor Restores (VM Conversion)

When restoring from a virtual machine backup, you can choose to convert a virtual machine to be used with a different hypervisor.

The following conversions are supported:
Restoring a VMware VM as an Amazon Instance

When restoring a VMware virtual machine from backup, you can choose to restore the VM as an Amazon instance.

Before You Begin

- Create an Amazon hypervisor (on page 23).
- Back up the VMware virtual machine that you plan to convert.
- The VSA proxy machine must be able to connect to ec2.amazonaws.com. To route communications through an HTTP or HTTPS proxy, see Configuring a Firewall for a VSA Proxy in the Cloud (on page 20). To use an HTTPS proxy, you must provide authentication details.
- You can use any VSA proxy to perform the conversion, either running on an Amazon instance or externally with connectivity into the Amazon account.
  - Using an Amazon proxy provides faster performance. By using a VSA proxy running on an Amazon instance, the restore operation can write directly to Elastic Block Storage (EBS) and inject Amazon drivers that are required for destination instances. You must provide credentials for the guest VM. The restore is performed using the HotAdd method.
  - Using an external proxy avoids the cost associated with running an Amazon instance. With an external proxy, you must select an S3 bucket for the restore. The restore is performed using the Import method.
- On any VM that you want to import into an Amazon EC2 instance, you might need up to 2 GB of available disk space in the OS disk for installing drivers and other software.
- See the following pages for information about Amazon considerations and limitations:
    - Prerequisites (http://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html#prerequisites-image)
    - Limitations (http://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html#limitations-image)
- Operating system requirements:
  - For information about supported virtual machine operating systems, see Importing a VM as an Image Using VM Import/Export (https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html).
**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
   The **Hypervisors** page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. In the **Subclients** area, click **Restore** for the subclient that contains the virtual machine.

4. In the **Select restore type** page, select **Full virtual machine** to restore one or more full virtual machines.

5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item.
   
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   
   o **Show latest backups**: Only display data for the most recent backups.
   
   o **Show backups as of a specific date**: Only display data up to the date you specify.
   
   o **Show backups for a date range**: Only display data within the data range you specify.

6. In the **Restore options** dialog box, provide the requested information:
   
   a. From the **Restore as** list, select **Amazon**.
   
   b. From the **Destination client** list, select an Amazon hypervisor.
   
   c. From the **Proxy client** list, select the VSA proxy to be used for the restore. By default, the preferred VSA proxy for the hypervisor is used for the restore.
      
      - If you select a proxy running in Amazon, you must enter the guest VM credentials so that Amazon drivers can be injected for the restored VM.
      
      - If you select a proxy that is outside of Amazon, you must select a bucket from the **Amazon buckets** list. The restore uploads volume information to S3 and uses the volumes to create the instance.

   d. **Only required if you chose a proxy that is not an Amazon instance**: From the **Amazon buckets** list, select a bucket for the instance volumes. Buckets are logical containers that provide secure access to objects (such as instance volumes).

   e. **Optional**: Select **Power on instance after restore** (the default) to start the instance automatically.

   f. **Optional**: To delete an existing instance and replace it with the restored instance, select **Overwrite instances if they already exist**.

   g. If you are restoring multiple instances, click the **All Instances** tab on the bottom left to specify configuration values for all instances you are restoring, or the name of each instance to specify values individually. Specify the following values:
      
      - **Optional**: To change the names of all destination instances, select **Enable edit destination instance name**. Then select **Prefix** or **Suffix** and enter a string to be appended to the original display name to create new destination instance names.
Optional: To change the name of an individual instance, select the instance and then enter the new display name in the Change instance display name to box.

If an existing instance with the same name exists on the destination host and you do not select Overwrite instances if they already exist, the restore job fails.

For the Availability zone, click Browse to select a value.

From the Instance type list, select an instance type that provides the available CPU cores and memory for the instance.

For the Network setting, click Browse to select an EC2 or a VPC network for the restored instances.

From the Security groups list, select a security group for the specified network.

Required if you chose an Amazon proxy: Select Specify guest credentials and then enter the guest VM credentials, including the Domain / Computer name, Username, and Password.

7. Click Submit to run the restore job.

Results

After VM conversion, if a source VM had dynamic disks that use spanned or striped volumes, the volumes in the converted VM might be marked as Failed in Disk Management. You must bring these disks online manually using Disk Management. To bring the disks back online, perform an Import Foreign Disks operation on the guest VM for the disk group that contains failed disks. As noted in Description of Disk Groups in Windows Disk Management (https://support.microsoft.com/en-us/help/222189/description-of-disk-groups-in-windows-disk-management), import the entire disk group in one operation rather than performing a partial import.

RAID partitioned volumes are not supported for conversion and import into Amazon.

This consideration also applies to GPT-partitioned OS disks. (Operating system disks must use MBR-partitioned volumes.)

Restoring a VMware VM as an Azure VM

When restoring a VMware virtual machine from backup, you can choose to restore the VM as an Azure VM. Conversion creates Generation 1 VMs.

Before You Begin

• Configure a Microsoft Azure hypervisor (on page 24).

• Before performing backups of source VMs:
  o Remote Desktop Protocol (RDP) must be enabled on the source VM and the user performing the conversion should be able to log in to the VM.
  o For Linux VMs, integration services should be enabled on the source VMs if they will be powered on automatically after conversion.
Azure Standard or Premium general-purpose storage accounts are required for VM conversion to Azure.

To enable deployment in Azure Resource Manager:
  - Define one or more resource groups for the application associated with the Azure virtualization client.

Commvault Considerations
- Conversion of virtual machines to Azure is not supported from IntelliSnap snap copies, but is supported from IntelliSnap backup copies.
- If the **Auto** option is selected and the disk operating system type cannot be determined from the configuration file, the job will fail. The job can be resubmitted by selecting the proper OS during the restore.
- The **Power on VMs after restore** option is selected by default. If this option is not selected when the VM is restored, only the operating system disk is registered, and any remaining disks are uploaded to the Azure storage account. In this case, VHDs must be created manually through the Azure management portal, using the Create VHD option on the Disk tab:
  - For each disk, browse to the storage location and open the disk from which the VHD is to be created. Opening the disk registers it as a VHD, so that it can be attached to a new or existing VM.
  - Select the VM to which the VHD is to be attached, and attach one or more registered VHDs from the storage location.

Azure VM Considerations
- The VM name can only contain alphanumeric characters or the '-' character; the name cannot contain any Unicode Transformation Format (UTF) characters.
- The RAM and disk specification for the source VM should match the format of the Azure destination VM. For example, if the source VM RAM is less than 1.75 GB, only two disks will be uploaded to Azure if **Auto** is selected as the VM size for the conversion, because of Azure restrictions.
- Virtual machines with a VM size of A8 or A9 can only be created in new Azure cloud services without any instances. You cannot create A8 or A9 VMs in existing cloud services.

Procedure
1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   The **Hypervisors** page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.
3. In the **Subclients** area, click **Restore** for the subclient that contains the virtual machine.
4. In the **Select restore type** page, select **Full virtual machine** to restore one or more full virtual machines.
5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:

- **Show latest backups**: Only display data for the most recent backups.
- **Show backups as of a specific date**: Only display data up to the date you specify.
- **Show backups for a date range**: Only display data within the data range you specify.

6. In the Restore options dialog box, provide the requested information:

a. From the Restore as list, select Azure.

b. Select an Azure hypervisor from the Virtualization Client list.

   The Azure subscription list displays the hypervisor for the Azure subscription. Select the Azure subscription client for the restore operation. The subscription type of the virtualization client (Classic or Azure Resource Manager) must match the type of the client for the source VM.

c. Select the target host from the Destination Client list.

d. **Optional**: By default, the preferred VSA proxy for the hypervisor is used for the restore. You can select a different proxy from the Proxy client list.

e. Select **Power on VMs after restore** to start the VM automatically.

f. To delete an existing virtual machine and replace it with the restored VM, select **Overwrite VMs if they already exist**.

g. If you are restoring multiple VMs, click the All VMs tab on the bottom left to specify configuration values for all VMs you are restoring, or the name of each VM to specify values individually. Specify the following values:

   - **Optional**: To change the names of destination VMs, select Enable edit destination VM name.
   
   - **Optional**: When restoring multiple VMs, select Prefix or Suffix and enter a string to be appended to the original display name to create new destination VM names.
   
   - **Optional**: To change the name of an individual VM, enter the new display name in the Change VM display name to box.

   - Azure Classic only: Enter a name in the Cloud service box to specify the Cloud Services group for the restored VM.

   - **Azure Resource Manager only**: Enter a name in the Resource group box to specify the Resource Group for the restored VM.

   - For **Storage account**, select the storage account for a virtual machine or disk.

     You can specify any storage account in the same region as the selected cloud service (Classic) or resource group (ARM).

   - **For VM size**, select a size specification for the restored virtual machine.

   - **For Network interface**, select a network connection for the restored VM, or leave the default value of Auto Select.

   - **Azure Resource Manager only**: If a public IP address is not required on restored VMs, clear the Create Public IP checkbox.

   - **Azure Resource Manager only**: For **Security Group**, specify a network security group for the restored VM or leave the default value of Auto Select.
7. Click Submit to run the restore job.

Results

If the source VM had dynamic disks that use simple disk spanning, RAID, striped, or mirrored layouts, after VM conversion, the disks in the converted VM might be marked as Failed in Disk Management. You must bring these disks online manually using Disk Management. To bring the disks back online, perform an Import Foreign Disks operation on the guest VM for the disk group that contains failed disks. As noted in Description of Disk Groups in Windows Disk Management (https://support.microsoft.com/en-us/help/222189/description-of-disk-groups-in-windows-disk-management), import the entire disk group in one operation rather than performing a partial import.

Restoring a VMware VM as a Hyper-V VM

When restoring a VMware virtual machine from backup, you can choose to restore the VM as a Hyper-V virtual machine.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Hypervisors.
   The Hypervisors page appears.
2. Click the name of the hypervisor that hosts the virtual machines.
   The hypervisor details page appears. The Subclients area displays summary information for any existing subclients.
3. In the Subclients area, click Restore for the subclient that contains the virtual machine.
4. In the Select restore type page, select Full virtual machine to restore one or more full virtual machines.
5. In the Restore page, expand the tree on the left and select the objects to be restored on the right.
   Select an item or click on an entry in the Name column to browse within an item.
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:
   - Show latest backups: Only display data for the most recent backups.
   - Show backups as of a specific date: Only display data up to the date you specify.
   - Show backups for a date range: Only display data within the date range you specify.
6. In the Restore options dialog box, provide the requested information:
   - From the Restore as list, select Microsoft Hyper-V.
   - Select a Hyper-V hypervisor from the Virtualization Client list.
   - Select the target host from the Destination Client list.
     All Hyper-V nodes are displayed.
d. Select **Power on VMs after restore** to start the VM automatically.

e. To delete an existing virtual machine and replace it with the restored VM, select **Overwrite VMs if they already exist**.

f. Select **Register virtual machine with failover cluster** to enable the restored VM to migrate to another node in the cluster.

g. For **Restore location**, leave the default (**Original folder**), choose **Select a folder**, or select **Hyper-V default folder**.

h. Type a new virtual machine name in the **Change VM display name to** box.
   
   This option does not display if you are restoring multiple VMs. If an existing VM with the same name exists on the destination host and you do not select **Overwrite VMs if they already exist**, the restore job fails.

i. For **Destination folder**, click **Browse** to select a new folder from the list. (Only enabled if you chose **Select a folder**.)

7. Click **Submit** to run the restore job.

---

### Restoring a VMware VM as an Oracle Cloud Classic Instance

When restoring a VMware virtual machine from backup, you can choose to restore the VM as an Oracle Cloud Classic instance.

---

**Before You Begin**

- Configure a hypervisor for Oracle Cloud Classic (on page 30).
- The proxy for the conversion must be an instance running in Oracle Cloud Classic.
- The source VM must reside on an ESXi host 6.0 or later.
- Make the following changes before backing up source VMs that are to be converted:

  **For Linux source VMs:**
  - Remove all MAC addresses in Ethernet configuration files so that DHCP can be enabled.
  - Enable DHCP on boot.
  - Enable console logging.
  - Update the kernel version to one of the following:
    - Oracle Linux 6.7
    - Other Linux OS using Unbreakable Enterprise Kernel (UEK) Release 3 or Red Hat Compatible Kernel (RHCK)

  **For Windows source VMs:**
  - Enable Remote Desktop Protocol (RDP) connection for the VM.
  - In environments that include a firewall, open a port for RDP connections.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Install Oracle VM Paravirtual (PV) drivers.

**Procedure**

1. From the navigation pane, click **Solutions > Virtualization > Hypervisors**.
   
   The **Hypervisors** page appears.

2. Click the name of the hypervisor that hosts the virtual machines.
   
   The hypervisor details page appears. The **Subclients** area displays summary information for any existing subclients.

3. In the **Subclients** area, click **Restore** for the subclient that contains the virtual machine.

4. In the **Select restore type** page, select **Full virtual machine** to restore one or more full virtual machines.

5. In the **Restore** page, expand the tree on the left and select the objects to be restored on the right. Select an item or click on an entry in the **Name** column to browse within an item.
   
   In the top right corner of the page, a "Showing" message indicates what backup data is being displayed. You can click the down arrow beside this message and select any of the following options:

   - **Show latest backups**: Only display data for the most recent backups.
   - **Show backups as of a specific date**: Only display data up to the date you specify.
   - **Show backups for a date range**: Only display data within the data range you specify.

6. In the **Restore options** dialog box, provide the requested information:
   
   a. From the **Restore as** list, select **Oracle Cloud**.
   
      b. Select an Oracle Cloud Classic hypervisor from the **Virtualization Client** list.
   
      c. Select the target host from the **Destination Client** list.
   
      d. **Optional**: By default, the preferred VSA proxy for the hypervisor is used for the restore. You can select a different Oracle Cloud Classic proxy from the **Proxy client** list.
   
      e. **Optional**: Select **Power on instance after restore** (the default) to start the instance automatically.
   
      f. If you are restoring multiple instances, click the **All Instances** tab on the bottom left to specify configuration values for all instances you are restoring, or the name of each instance to specify values individually. Specify the following values:

         - When restoring a single instance, in the **Change instance display name to** box, enter a new display name for the instance.
         - From the **User account** list, select the user for the destination endpoint.
         - From the **Instance shape** list, select an instance shape that is at or above the level of the source instances.
         - In the **Network** box, select a network for the destination instances.
         - In the **Security groups** box, select a security group for the specified network.
         - In the **SSH keys** box, select a predefined SSH key for the destination instances.

7. Click **Submit** to run the restore job.
IP address settings

When virtual machines are restored to a destination that uses a different network connection, you can specify parameters for IP address mapping. If source VMs running Windows use static IP addresses, you can configure IP address mappings for destination VMs.

**Source VM Settings:** Specify values for source VMs:
- **IP Address:** Enter a full IP address or an IP address pattern for source VMs.
- **Subnet Mask:** Enter a full IP address or an IP address pattern for the subnet mask.
- **Default Gateway:** Enter a full IP address or an IP address pattern for the default gateway.

**Destination VM Settings:** Specify settings to be used for destination VMs:
- **Use DHCP:** Automatically assign available IP addresses to be used with the specified destination network.
- **IP Address:** Enter a full IP address or an IP address pattern for destination VMs.
- **Subnet Mask:** Enter a full IP address or an IP address pattern for the subnet mask.
- **Default Gateway:** Enter a full IP address or an IP address pattern for the default gateway.
- **Preferred DNS Server:** Identify the primary DNS server for the destination.
- **Alternate DNS Server:** Identify a secondary DNS server for the destination.
- **Preferred WINS Server:** Identify the primary WINS server for the destination.
- **Alternate WINS Server:** Identify a secondary WINS server for the destination.

**IP Address Mapping Examples**

The following examples show how IP address settings can be used to remap addresses for a different destination network.

**Example 1**

With the following settings, IP addresses for source VMs are remapped if they match the pattern 172.20.10.* (for example, 172.20.10.5 would be mapped to 172.30.10.5).

<table>
<thead>
<tr>
<th>Settings</th>
<th>Source VM</th>
<th>Destination VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>172.20.10.*</td>
<td>173.30.10.*</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>172.20.1.*</td>
<td>172.30.1.*</td>
</tr>
</tbody>
</table>

**Example 2**

With the following settings, IP addresses for source VMs are remapped if they match the pattern 172.20.*.* (for example, 172.20.65.10 would be mapped to 172.30.65.10).
Viewing Virtual Machine Information

You can view virtual machines that you own, see the latest backup or jobs that included a virtual machine, or initiate a restore.

Procedure

1. From the navigation pane, click Solutions > Virtualization > Virtual Machines.
   The VMs page shows the VM name, hypervisor, backup size, last backup time, host, and the VSA proxy that performed the backup.

   **Note:** You can click the button at the right side of the VM table header to add or remove columns or to enable filtering.

2. To view details for a specific VM, click the VM name.

3. From the summary display for a VM, you can perform any of the following tasks:
   - **Last Backup:** View the most recent backup job for the VM.
   - **Jobs:** View all jobs for the VM.
   - **Restore:** Start a restore job for the VM.

The Summary area for a VM includes the following information:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Source VM</th>
<th>Destination VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>172.20.<em>.</em></td>
<td>172.30.<em>.</em></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.0.0</td>
<td>255.255.0.*</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>172.20.1.*</td>
<td>172.30.1.*</td>
</tr>
</tbody>
</table>
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Backup status**: PROTECTED, NOT PROTECTED, or BACKED UP WITH ERROR.
- **Hypervisor**: The name of the hypervisor that hosts the VM.
- **Subclient**: The name of the subclient that includes the VM.
- **Proxy**: The proxy that performed the last backup. This entry is blank if the last backup was a synthetic full backup.
- **VM size**: Size of the VM (GBs).
- **Backup size**: The amount of data written during the last backup (GBs).
- **Last backup time**: The date and time when the last backup was performed. This entry is blank if the last backup was a synthetic full backup.
- **Guest OS**: The guest operating system for the VM.
- **Guest size**: The actual space used on the storage volume where the virtual machine resides.
- **Host**: The name of the server where the Admin Console is running.
- **Total backup time**: The total time used for the most recent backup.

In the **Security** area, the **Associations** tab shows users or groups who have rights to the VM, along with their associated roles. The **Owners** tab shows users who have ownership rights to the VM.

You can click **Edit** to modify security settings for the VM.

---

**Reports for Virtualization**

You can access reports from the Virtualization dashboard, or by clicking **Reports** in the navigation pane and then selecting a report.

---

**Virtualization SLA**

The Virtualization SLA page shows information about performance against expected backup schedules.

To access the report:

- From the navigation pane, click **Reports > SLA**.

The top section of the report shows SLA performance graphically.

The **Virtual Machine Details** section shows the following information for each VM:

- **VM Name**: The name of the virtual machine. Click the name to view more information about the VM.
- **SLA Status**: Displays one of the following values:
  - **Missed SLA**: Backups did not run in the expected time range, or backups failed.
  - **Excluded**: Backups were disabled.
  - **Met SLA**: Backups were performed successfully.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Last Protected Time:** The date and time of the last successful backup.
- **Category:** Additional information about the reasons for the SLA status. The following entries can be displayed in this column:
  - Backup Activity Disabled
  - Protected
  - No Schedule
  - No job within SLA Period
  - Failed

Backup Job Summary

The Backup Job Summary report for virtualization shows all backup jobs that ran in the past week.

To access the report:
- From the navigation pane, click **Reports > Backup Job Summary**.

The top row of the report shows the number and date of backup jobs that ran in the past week, followed by the number of jobs that ran for each hypervisor type (Hyper-V, Nutanix Acropolis, or VMware).

The **Details** section provides the following information for each backup job:
- **Client:** The hypervisor for which the job ran.
- **Instance:** The hypervisor type.
- **Subclient:** The collection of VMs for the job.
- **Backup Type:** The type of backup (Full, Incremental, or Synthetic full)
- **Job Status:** The results of the job (such as Completed, Failed, or Killed).
- **Application size:** The total amount of data backed up for all virtual machines in the job.
- **Start Date:** The date and time the job began.
- **End Date:** The date and time the job ended.
- **Protected VMs:** The number of virtual machines that were backed up.
- **Failed VMs:** The number of virtual machines in the subclient that were not backed up successfully.

Restore Job Summary

The Restore Job Summary report for virtualization shows all restore jobs that ran in the past week.

To access the report:
- From the navigation pane, click **Reports > Restore Job Summary**.

The first row of the report shows the number of jobs for each job status (such as Completed, Failed, or Killed).
Virtual Server Protection (VSP) - Version 11 Service Pack 11

The Details section provides the following information for each restore job:

- **Source Client**: The hypervisor where source VMs resided.
- **Destination Client**: The hypervisor where VMs were restored.
- **Backupset**:
- **Status**: The results of the job (such as Completed, Failed, or Killed).
- **Start Date**: The date and time the job began.
- **End Date**: The date and time the job ended.
- **Application size**:

### Storage Utilization

The Storage Utilization report shows used and free space for each defined storage target.

To access the report:

- From the navigation pane, click **Reports > Storage Utilization**.

The first row shows the percentage of used and free space for each storage target.

The Details section includes the following information for each storage target:

- **Library**: Name of the storage target. Click on the name to display the definition page for the storage target.
- **MediaAgent**: The MediaAgent that communicates with the storage target to transfer data.
- **Mount Path**: The path used to write data to storage.
- **Status**: The status of the storage device.
- **Free Space (TB)**: The amount of free space on the storage target.
- **Total Capacity (TB)**: The total space on the storage target.
- **Used Space (TB)**: The amount of used space on the storage target.
- **Free Space (%)**: The percentage of free space on the storage target.

### Creating a Life Cycle Policy

Create a life cycle policy for the following scenarios:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- To identify resources that can be used for live mounts and to specify parameters for live mount operations.
- To enable testing failover operations for VMs using live mounts.
- To support Virtualize Me operations.

Before You Begin

- For Virtualize Me policies, download the required Windows or UNIX ISO files and copy them to a location on the destination host.

Procedure

1. From the navigation pane, go to Configuration > Life cycle policies.
2. Click Add policy.
   The Create policy wizard displays the General page.
3. Provide the following information:
   - Policy name: Enter a descriptive name for the policy.
   - Select type: Select VMware from the list.
   - Destination hypervisor: Select the hypervisor where the VM will be mounted.
4. Click Next.
   The Configuration page appears. The information you enter will be used for all operations using the policy.
5. Provide the following information:
   - Destination host: Click Browse to select an ESX host that can be used for VMs.
   - VM display name: Select Prefix or Suffix, and then enter a string that will be appended to the source VM name to create the VM display name for the destination VM.
   - Datastore: Select a destination datastore.
   - Destination network: Select a network that can be used by destination VMs.
6. Click Next.
   The Settings page appears.
7. Provide the following information:
   - Resource and quota limits:
     - No of VMs (per user): Select the number of concurrent VMs that each user can run using this policy.
   - User membership and expiration:
     - User and user groups: Select users or user groups that should have access to the policy.
     - Live mount options: Select this option to display settings that are specific to live mount operations.
       - Expiration time: Select Hours or Days and specify the amount of time that live mounted VMs can run before they expire.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

To keep VMs available beyond the expiry time, select the **Migrate VMs** option. Users can also renew or delete VMs (on page 63).

**MediaAgent**: To use a specific MediaAgent for live mounts, select this option and then choose a MediaAgent from the list.

- **Additional settings:**
  - **Virtualize Me options**: Select this option to display options that are specific to Virtualize Me.
  - **Iso path (Windows)**: Click **Browse** to select the path for the Windows ISO file.
  - **Iso path (Unix)**: Click **Browse** to select the path for the UNIX ISO file.
  - **Migrate VMs**: To enable live mounted VMs to be mounted to the destination datastore for extended availability, select this option.
  - **Wait before migration (in hours)**: To specify a delay between live mounting VMs and migrating the VMs to a datastore for extended availability, specify the number of hours.

8. Click **Finish**.

## Plans

You create plans to protect your data. In the plan you define what to back up, where to back up your data, and how often to run the backup job. You can create base plans that can be used as templates to create derived plans.

There are plan types that include the data protection parameters that apply to the type of data you want to protect.

<table>
<thead>
<tr>
<th>Plan Type</th>
<th>Applies To</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System</td>
<td>UNIX and Windows File System agents</td>
</tr>
<tr>
<td>Server</td>
<td>File System agents</td>
</tr>
<tr>
<td></td>
<td>Exchange applications</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Laptop agents</td>
</tr>
<tr>
<td>Exchange Plans</td>
<td>Exchange Mailbox</td>
</tr>
<tr>
<td>Database</td>
<td>Oracle and SQL agents</td>
</tr>
<tr>
<td>Snap</td>
<td>Pure Storage and Nutanix storage arrays</td>
</tr>
</tbody>
</table>

Copyright © 2018 Commvault Systems, Inc. All rights reserved.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Plan Type | Applies To
---|---
Virtualization | Backup
| Backup and replication
| Virtualization subclients can also use snap plans

Predefined Plans

Some applications in Admin Console offer predefined plans:

<table>
<thead>
<tr>
<th>Plan</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Gold** | • An incremental backup is run every four hours starting at midnight.  
• A synthetic full backup is run every Friday starting at 8 p.m.  
• A full backup is run on the last Saturday of every month starting at 8 p.m.  
• The retention period is 30 days. |
| **Silver** | • An incremental backup is run daily every 12 hours starting at midnight.  
• A synthetic full backup is run every Friday starting at 8 p.m.  
• A full backup is run on the last Saturday of every month starting at 8 p.m.  
• The retention period is 30 days. |
| **Bronze** | • An incremental backup is run daily every 24 hours starting at midnight.  
• A synthetic full backup is run every Friday starting at 8 p.m.  
• A full backup is run on the last Saturday of every month starting at 8 p.m.  
• The retention period is 30 days. |

Server Plans

You can create a server plan to specify the following:

• The storage pool that stores the backup data
• The data retention period
• The backup frequency to use to automatically back up the data
Creating a Server Plan

You must create a server plan to start protecting your data.

Before You Begin

Create a storage pool. For information on storage pools, see Storage Pool (on page 143).

Procedure

1. From the navigation pane, expand Configuration, and then click Plans.
   The Plans page appears.
2. In the upper right of the page, click Create plan, and then click Server.
   The Create server backup plan dialog box appears.
3. In the Plan name box, type the name of the plan.
4. Under Storage pool, set the storage options:
   a. To store the data that is backed up, in the Primary storage list, click the storage pool.
   b. Optional: In the Retention period box, type the number of days data is retained.
   c. To configure an auxiliary copy, select the Enable secondary storage check box:
      i. In the Secondary storage list, click a storage pool to store the copy of your backed up data.
      ii. Optional: In the Retention period box, type the number of days data is retained.
5. Optional: Under RPO (recovery point objective), update the RPO options:
   a. To update how often data is backed up, in the Backup frequency box, enter how often backup jobs will run.
   b. To update the backup window, click the text next to Backup window, and in the Edit backup window dialog box, select the days and times when backup jobs will run.
6. To make this plan act as a template when you create more plans, see Creating a Base Plan.
7. Click Save.

Result

The software creates a plan and a storage policy.

When you configure secondary storage, an auxiliary copy job automatically runs every 30 minutes.

What to Do Next

You can assign the plan or storage policy to subclients.
Modifying a Server Plan

You can modify the following server plan properties:

- The storage pools to use for the primary and auxiliary data copies
- The data retention period
- The RPO (recovery point objective) options used to automatically back up the data

**Procedure**

1. From the navigation pane, click **Configuration > Plans**.
   The Plan page appears.
2. Click the plan name.
   The plan details page appears.
3. To modify the RPO options, do the following:
   a. To update how often data is backed up, click **Edit**, and in the Backup frequency box, enter how often backup jobs will run.
   b. To update the backup window, click the text next to Backup window, and in the **Edit backup window** dialog box, select the days and times when backup jobs will run.
4. To modify the storage pools, under **Storage**, click **Edit**.
   The Storage pool dialog box appears. If you have configured secondary storage for the plan, secondary storage options are available.
   a. From the Primary storage list, select the pool.
   b. In the Retention period box, type the number of days that the software will retain the primary data copy.
   c. From the Secondary storage list, select the pool for the secondary copy.
   d. In the Retention period box, type the number of days that the software will retain the secondary data copy.
5. Click **Save**.

**Result**

The new values are used when the next backup operation runs.

**Snap Plans**

Snap plans are supported for the following:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- Pure Storage and Nutanix storage arrays
- Microsoft Hyper-V and VMware hypervisors
- Microsoft Windows file system agent

You can create a snap plan to specify the following:
- The storage pool that stores the snapshots
- The backup frequency to use to automatically back up the snapshots
- The retention period in terms of the number of recovery points for the snap copy.

When a snap plan is created the following happen automatically:
- Backup copy operations run daily every three hours
- Snapshot backups are run daily (incremental), weekly (synthetic full), and monthly (full)

**Note:** The synthetic full backup does not apply to all servers.

- A storage policy is created.
- The storage policy creates a primary copy and a primary classic copy.

The Snap plan page shows RPO (recovery point objective), storage pool, and security sections. You can edit the retention of the backup copy and of the snapshot recovery points for the snap copy in the storage pool section.

Creating a Snap Plan

You must create a snap plan to start protecting your data.

**Before You Begin**

Create a storage pool. For information on storage pools, see Storage Pool (on page 143).

**Procedure**

1. From the navigation pane, expand **Configuration**, and then click **Plans**.
   - The **Plans** page appears.
2. In the upper right of the page, click **Create plan**, and then click **Snap**.
   - The **Create snap plan** dialog box appears.
3. In the **Plan name** box, type the name of the plan.
4. Under **Storage pool**, set the storage options:
   a. To store the snapshots, in the **Primary storage** list, click the storage pool.
   b. In the **Number of Snap recovery points** box, type the number of days that the snapshots are retained.
5. **Optional:** Under RPO (recovery point objective), update the RPO options:
   a. To update how often snapshots are taken, in the **Backup frequency** box, enter how often the jobs will run.
   b. To add a backup window, click **Not enabled**, and in the **Edit backup window** dialog box, select the days and times when jobs will run.

6. Click **Save**.

**What to Do Next**

Add a storage array (on page 142).

**Adding a Microsoft Hyper-V Hypervisor to an Array**

Adding a server to an array enables IntelliSnap on the client.

**Before You Begin**

- If you have not done so yet, create a Snap Plan (on page 138) and add an array (on page 142).
- Make sure that the hypervisor is installed correctly and the nodes can be accessed by the Admin Console.

**Procedure**

1. From the navigation pane, click **Storage > Arrays**.
2. In the **Arrays** column, click **array**.
   The **Array** page box appears.
3. In the **Server** area, in the upper-right, click **Associate server**, and then click **New hypervisor**.
   The **Add hypervisor** dialog box appears.
   You can also choose an existing Hyper-V hypervisor.
4. In the **Add hypervisor** dialog box, provide the following information:
   o From the **Select type** list, select **Hyper-V**.
   o In the **Hostname / IP address** box, type the host name or the IP address of the host computer.
   o The **Hypervisor name** is populated with the same **hostname** or **IP address** that you type above. If you need, type a new **Hypervisor name**.
   o In the **Username** and the **Password** boxes, type the credentials for the hypervisor.
   o In the **Select plan** box, select a snap plan.
5. Click **Discover Nodes**.
   The **Nodes** list appears.
6. From the **Nodes** list, select a hypervisor node.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

7. Click **Save**.

**What to Do Next**

Assign the snap plan to subclients (on page 37) to enable IntelliSnap on the subclients.

**Adding a VMware Hypervisor to an Array**

Adding a server to an array enables IntelliSnap on the client.

**Before You Begin**

- If you have not done so yet, create a Snap Plan (on page 138) and add an array (on page 142).
- In the following procedure, when you select **VMware**, a **Proxy** dialog box appears. Make sure that you have access to the proxy computer that you select.

**Procedure**

1. From the navigation pane, click **Storage > Arrays**.
2. In the **Arrays** column, click array.
   The **Array page** box appears.
3. In the **Server** area, in the upper-right, click **Associate server**, and then click **New hypervisor**.
   The **Add hypervisor** dialog box appears.
   You can also choose an existing VMware hypervisor.
4. In the **Add hypervisor** dialog box, provide the following information:
   - From the **Select type** list, select **VMware**.
   - In the **Hostname / IP address** box, type the host name or the IP address of the host computer.
   - The **Hypervisor name** is populated with the same hostname or IP address that you type above. If you need, type a new **Hypervisor name**.
   - In the **Username** and the **Password** boxes, type the credentials for the hypervisor.
   - In the **Proxy** box, type a proxy name or the IP address of the proxy computer.
   - In the **Select plan** box, select a snap plan.
5. Click **Save**.

**What to Do Next**

1. Assign the snap plan to subclients (on page 37) to enable IntelliSnap on the subclients.
2. After assigning the snap plan to a subclient, edit the subclient (on page 51) and set the **Snap mount esx host** option in the subclient details to identify the ESX server that can be used to mount the snapshot.
Adding a Server to an Array

Before You Begin

Adding a server to an array enables IntelliSnap on the client computer.

There is no support for IntelliSnap backup of multiple arrays. It is not possible to associate a server to multiple storage arrays.

Procedure

1. From the navigation pane, click Storage > Arrays.
2. In the Arrays column, click array.
   The Array page box appears.
3. In the Server area, in the upper-right, click Associate server, and then click Existing server.
   The Add existing server dialog box appears.
4. In the Add existing server dialog box, provide the following information:
   - From the Select Hypervisor list, you can choose to do one of the following:
     - Select a server.
     - Select all or none available servers.
     - Search for a server.
   - Optional: Select the Associate all subclients to selected snap plan check box to associate all subclients to the snap plan.
   - If you select the Associate all subclients to selected snap plan check box, then from the Select plan list, select a snap plan.
5. Click Save.
   The Confirm add dialog box appears.
6. Click Yes.

Editing the Backup Copy Schedule of a Snap Plan

Deprecated: After Service Pack 11 is installed, schedules will not be displayed on new plans. For plans created prior to Service Pack 11, you can continue to update the plan schedules.

You can edit the backup copy schedule. A snap plan must have at least one backup copy schedule. If the snap plan has just one backup copy schedule, then the Delete button is grayed out.
Procedure
1. From the navigation pane, click Plans.
2. On the Plans page, from the Plans list, click on a snap plan.
   The Snap plan page appears.
3. In the Backup copy schedule area, click Edit.
   The Edit schedule dialog box appears.
4. Edit the information for the backup copy schedule.
5. Click Save.

Editing the Security Section of a Snap Plan

Procedure
1. From the navigation pane, click Plans.
2. On the Plans page, from the Plans list, click on a snap plan.
   The Snap plan page appears.
3. In the Security area, click Edit to update security information.
4. Click Save.

Adding a Storage Array to the CommServe Database

You can add a storage array into the CommServe database and configure the information for IntelliSnap backups.

IntelliSnap backups are supported for Pure Storage and Nutanix storage arrays.

Before You Begin

Important: After you add a storage array to the CommServe database, you cannot change the Snap Vendor, Name, or Control Host values of the storage array.

You can add an array without entering the credentials, but snapshot operations fail if the communication with the array cannot be established. Check whether you need to enter the credentials on the array documentation.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

**Procedure**

1. From the navigation pane, click **Storage > Arrays**.
2. In the upper-right, click **Add arrays**.
   The **Add array** dialog box appears.
3. In the **Snap vendor** box, select the snap vendor.
   If the snap vendor that you selected has snap configuration properties, then the snap configuration properties appear in the **Add array** dialog box.
4. In the **Array name** box, type the array name.
5. In the **Username** and **Password** boxes, type the credentials for the array.
6. Click **OK**.

**Storage Pool**

Network Storage Pool provides a scalable and easy to configure storage solution. It allows multiple cross platform MediaAgents to access a shared storage pool. The storage capacity can be scaled-out on demand by simply adding more mount paths. The added MediaAgents or the mount paths are automatically shared using the DataServer-IP.

The configuration process is managed behind-the-scenes and requires little user intervention.
Monitoring

You can monitor activity in the Admin Console by creating alert definitions, viewing events, and viewing and controlling jobs.

Alerts

Alerts provide automatic notification about operations, such as failed jobs. Alerts are displayed on the Triggered Alerts page. Users defined in the alert definition receive an email notification when an alert is triggered.

Creating an Alert Definition

You can create alert definitions to provide automatic notification about operations, such as failed jobs. An alert is triggered when conditions within the entity meet the criterion selected in the alert definition.

Procedure

1. From the navigation pane, click Alerts.
2. On the Triggered alerts page, in the upper right of the page, click Alerts definitions.
   The Alerts definition page appears.
3. In the upper right of the page, click Add alert definition.
   The Add alerts definition dialog box appears.
4. In the Alert name box, type the name of the alert.
5. In the Alert type list, click the type of alert you want to create, for example, Backup Job Failed.
6. If the alert type has a variable in it, in the Value for X box, enter a value for the variable.
   For example, you must define the value for X for the Backup Delay by X Hrs alert type.
7. Under Entities, select the entities the alert definition should apply to.
8. Under Users, for each user who should receive notifications for the alert, do one of the following:
   o Type the user email address.
   o Type the user or user group name, and from the generated list, click the user or user group name.
9. Click Add.
10. Click Save.
Editing Alert Definitions

You can enable or disable alerts, and you can change the users who receive notifications when the alert definition is triggered.

Procedure

1. From the navigation pane, click Alerts.
2. On the Triggered alerts page, in the upper right click Alerts definitions.
   Two the Alerts definition page appears.
3. To enable or disable an alert, in the Enabled column, select or clear the check box.
4. To view the definition page for an alert, in the Name column, click the name.
5. To make changes to the users and user groups who receive notifications for the alert definition, do the following:
   a. On the definition page, under User or groups to notify, click Edit.
   b. In the Add new user or group dialog box, do one of the following:
      ▪ Type the user email address.
      ▪ Type the user or user group name, and from the generated list, click the user or user group name.
   c. Click Add.
   d. Click Save.

Viewing Triggered Alerts

An alert is triggered when conditions within the entity meet the criterion selected in the alert definition.

Procedure

- To view alerts, from the navigation pane, click Alerts.
  On the Triggered alerts page, alerts triggered from your alert definitions are listed.
- To see the alert details, on Triggered Alerts page, in the Alert info column, click the descriptive link.

Deleting Triggered Alerts

You can delete triggered alerts.
**Procedure**

- From the navigation pane, click **Alerts**, and on **Triggered Alerts** page, delete alerts:
  - To delete individual alerts, select the check box for the alert and click **Delete**.
  - To delete all of the alerts, select the check box in the table header and click **Delete**.
  
  **Note:** If there are pinned alerts in the list, they are deleted.

**Alert Information for Triggered Alerts**

The **Triggered alert** page provides the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• Major: Indication that a major function is compromised and needs remediation.</td>
</tr>
<tr>
<td></td>
<td>• Critical: Indication that an error occurred and needs remediation.</td>
</tr>
<tr>
<td></td>
<td>• Information: Non-critical information that does not require immediate action.</td>
</tr>
<tr>
<td>Detected criterion</td>
<td>Brief description of the issue.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of event that caused the alert as listed in the alert definition, for example, Data Protection or Data Recovery.</td>
</tr>
<tr>
<td>Detected time</td>
<td>Date and time when the system detected the alert condition.</td>
</tr>
<tr>
<td>Computer name</td>
<td>Identifies the entity to which the alert applies.</td>
</tr>
<tr>
<td>Alert info</td>
<td>Name of the alert. Click to view additional information about the alert.</td>
</tr>
<tr>
<td>Pin</td>
<td>Click to save the alert notification and prevent it from being pruned.</td>
</tr>
</tbody>
</table>

**Viewing Events**

The Events page provides information about jobs and other significant events detected in the Admin Console. In some cases, events can trigger alerts to notify users of events (such as job failures).

**Procedure**

1. From the navigation pane, click **Events**.

   The **Events** page appears.

2. To view details for an event, in the **Event ID** column, click the event ID.
Jobs

On the **Jobs** page, you can control active jobs and view completed jobs. By default, all jobs run in the last 24 hours are available. You can use the **Showing** and **for** lists to filter the jobs, for example, you can view jobs that finished in the last seven days. The **Jobs** page includes jobs that you ran, for example, a backup job, and jobs that the software automatically ran, for example, pruning jobs. For information on the **Jobs** page columns, see Job Information (on page 149).

On the **Severs** page, you can disable and enable entire job categories in your CommCell environment.

Controlling Activities

You can disable and enable job categories in your CommCell environment. For example, you can disable all data management (back up) jobs.

**Procedure**

1. From the navigation pane, click **CommCell**.
2. Under **Activity control**, click the toggle key next to the type of activity you want to disable or enable:
   - All Job Activity
   - Data Management (back up)
   - Data Recovery (restore)
   - Data Aging (pruning)
   - Auxiliary Copy
   - Scheduler
   - Offline Content Indexing

Controlling Jobs

You can control active jobs. For example, you can suspend a job.

**Procedure**

1. From the navigation pane, click **Jobs**.
   
   The **Jobs** page appears.
   
   **Tip:** You can change the jobs you see by using the filter options in the upper right of the page.

2. In the **Actions** column for the job, click the action button and choose your action:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- To kill the job, click **Kill**.
- To suspend the job, click **Suspend**.
- To resume a suspended job, click **Resume**.

Viewing Jobs

You can view jobs for the entities in your application. For example, you can view jobs for servers or devices.

**Procedure**

**All Jobs**

1. From the navigation pane, click **Jobs**.
   
The **Jobs** page appears.
   
   **Tip:** You can change the jobs you see by using the filter options in the upper right of the page.
2. To view the job details, in the **Job ID** column, click the job ID.

**For a Specific Entity**

1. From the navigation pane, click the entity. For example, select **Servers**.
2. From the list of available entities, in the **Name** column, click the entity name.
3. In the upper right of the entity details page, click **Jobs**.
   
   **Note:** Some entities have links to view specific types of jobs. For example, on the device details page, click **Restore jobs** to view the restore jobs for the device.

Sending Log Files

You can use log files to analyze and diagnose problems within the Admin Console. The log files contain the operation processing details.

**About This Task**

The default options for sending the logs are selected based on where you initiate the operation. For example, if you initiate the operation from the **Jobs** page, the **Send log files** dialog box is prepopulated with the job ID.

**Procedure**

1. From the navigation pane, go to the page from where you want to send the logs:
   
   - **CommCell** details page: Click **CommCell**, and then in the upper right of the page click **Send logs**.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- **Servers** details page: Click **Servers**, and then in the upper right of the page click **Send logs**.

- **Jobs** page: Click **Jobs**, in the **Actions** column for the job, click the action button ☐, and then click **Send logs**.

- **Job details** page: Click **Jobs > job ID**, and then in the upper right of the page click **Send logs**.
  The **Send log files** dialog box appears.

2. On the **Computers** tab, select the logs to send:
   - To send the log files for a specific job, click **Job ID** and enter the job ID.
   - To send the log files for a specific set of computers, click **Computers** and choose the computers.

3. On the **Information** tab, select the type of logs that you want to include, for example, **Database logs**.

4. On the **Output** tab, select the **Upload** check box and browse for a storage location.

5. On the **Notifications** tab, select the users who should receive an email about the logs.
   By default, logs are sent to Commvault support.

6. Click **Send logs**.

---

**Job Information**

The **Jobs** page and **Job Details** page provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>The system generated ID for the job. Click the job ID to open the Job Details page.</td>
<td>Job</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Job Details</td>
</tr>
<tr>
<td>Operation</td>
<td>The job type, for example, Backup.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you perform a backup or restore by a using third-party command line interface, for example, RMAN, &quot;3RD&quot; is appended to the operation type.</td>
<td>Job</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Job Details</td>
</tr>
<tr>
<td>Status</td>
<td>This indicates the job status description.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Job</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Job Details</td>
</tr>
<tr>
<td>Size</td>
<td>The amount of data that the job is processing or processed.</td>
<td>Job</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Job Details</td>
</tr>
<tr>
<td>Server</td>
<td>The server that performed the job.</td>
<td>Job</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Job Details</td>
</tr>
<tr>
<td>Collection</td>
<td>This is the collection of data, or subclient that the software used for the job.</td>
<td>Job</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Job</td>
</tr>
<tr>
<td>Start time</td>
<td>The time that the software started the job.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Job</td>
</tr>
<tr>
<td></td>
<td>Job Details</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td><strong>Elapsed Time</strong></td>
<td>The total time that the job ran.</td>
<td></td>
</tr>
<tr>
<td><strong>Logs</strong></td>
<td>The option to send or view the logs.</td>
<td></td>
</tr>
<tr>
<td><strong>JPR</strong></td>
<td>The job pending reason. When the job failed, a code is displayed. Point to the code to see the complete failure description.</td>
<td></td>
</tr>
<tr>
<td><strong>Progress</strong></td>
<td>The job status. Valid values are: • In progress • Completed • Failed</td>
<td></td>
</tr>
<tr>
<td><strong>Job started by</strong></td>
<td>The user that started the job.</td>
<td></td>
</tr>
<tr>
<td><strong>Job started from</strong></td>
<td>This is how the job was started. For jobs that the software automatically starts, the value is &quot;Scheduled.&quot; For third party command line jobs, the value is &quot;Third Party.&quot;</td>
<td></td>
</tr>
<tr>
<td><strong>iDataAgent</strong></td>
<td>The agent type, for example SAP HANA.</td>
<td></td>
</tr>
<tr>
<td><strong>Instance</strong></td>
<td>For database jobs, this is the instance that the job used.</td>
<td></td>
</tr>
<tr>
<td><strong>Transfer time</strong></td>
<td>The time that it took for the software to transfer the data.</td>
<td></td>
</tr>
<tr>
<td><strong>End Time</strong></td>
<td>The time that the job ended.</td>
<td></td>
</tr>
<tr>
<td><strong>Software Compression</strong></td>
<td>The software compression that the job used. Valid values are: • Off • Storage Policy • MediaAgent</td>
<td></td>
</tr>
</tbody>
</table>
Storage Targets

A storage target can be one of the following:

- A cloud library or a disk library that you associate with one or more mount paths. A mount path is a set of partitioned disks or arrays that is associated with a file system. A mount path can be a local disk or networked attached storage on the disk library MediaAgent. This is where data is stored when it is backed up.
- A tape library attached to a MediaAgent.

The Storage Targets page lists the name, status, manufacturer, and model of the storage targets you add.

Available Operations

You can perform the following operations on the Storage Targets page:

- Add a storage target.
- Delete or deconfigure a storage target.
- View the storage target details.
- Manage a Tape library, which includes the following operations:
  - Resetting the library
  - Deconfiguring the library
  - Validating a drive
  - Cleaning a drive
  - Unloading a drive
  - Resetting a drive

Note: Other operations for Tape libraries are currently not supported in the Admin Console. Administrators/users must use the CommCell Console to perform these operations. Similarly, advanced configurations for Tape Libraries must be performed using the Expert Storage Configuration available in the CommCell Console.

Configuring a Disk Library as a Storage Target

You can configure a disk library as a storage target. You must assign a mount path to a disk library. A mount path can be:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

- A local disk drive associated with the MediaAgent
- A disk drive that is on networked-attached-storage (NAS) associated with the MediaAgent

Procedure

1. From the navigation pan, click **Storage targets**.
   The **Storage targets** page appears.
2. Click **Add storage** in the upper right of the page, and then select **Disk**.
3. In the **Add disk storage** dialog box, enter the disk library details:
   a. In the **Name** box, type the name of the library.
   b. From the **MediaAgent** list, select the MediaAgent that will write the data to the disk.
4. To use a local disk as the mount path, click **Local path** and in the **Path** box, type the full path name to the storage location.
5. To use a network drive as the mount path, provide the following information:
   a. Click **Network path**.
   b. In the **User name** and **Password** boxes, type the credentials for a user who has write access to the network device.
   c. In the **Path** box, type the full path name to the storage location.
6. Click **Create**.

Result

The disk library is available. You can associate the disk library with a plan.

Related Topics

Adding a Mount Path (on page 152)

Adding a Mount Path

On the **Storage Target Details** page, you can view the storage capacity and free space for a storage target. The information is the sum of all of the mount paths. If you need additional mount paths, you can add mount paths to the storage target.

Procedure

1. From the navigation pane, go to **Storage Targets** > **storage_target** and in the right of the page, click **Add disk**.
   The **Add path** dialog box is displayed.
2. In the Name box, type the name of the mount path.
3. From the MediaAgent list, select the MediaAgent that will write the data to the disk.
4. To use a local disk as the mount path, click Local path and in the Path box, type the full path name to the storage location.
5. To use a network drive as the mount path, provide the following information:
   a. Click Network path.
   b. In the User name and Password boxes, type the credentials for a user who has write access to the network location.
   c. In the Path box, type the full path name to the storage location.
6. Click Add path.

Result
The mount path is added to the library.

Configuring a Cloud Library as a Storage Target
You can configure a cloud library as a storage target.

Procedure
1. From the navigation pane, click Storage targets.
   The Storage targets page appears.
2. Click Add storage in the upper right of the page, and then select Cloud.
3. In the Add cloud storage dialog box, enter the cloud library details:
   a. In the Name box, type the name of the library.
   b. From the Type list, select the cloud library vendor.
   c. From the MediaAgent list, select the MediaAgent that will write the data to the disk.
   d. The Commvault software populates the Server Host box and credentials boxes with the default values for each vendor, for example, Token_ID.
   e. Provide the cloud library credentials.
      For information on the cloud credentials, see Cloud Provider Information (on page 154).
4. Click Create library.

Results
The cloud library is now available. You can associate the cloud library with a plan.
Cloud Provider Information

When you add a cloud storage library, enter the required information for the selected cloud provider.

<table>
<thead>
<tr>
<th>HCloud Provider</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common options</td>
<td>Name</td>
<td>An user-friendly name for the library.</td>
</tr>
<tr>
<td></td>
<td>MediaAgent</td>
<td>The MediaAgent that writes the data to the cloud library.</td>
</tr>
<tr>
<td></td>
<td>Server Host</td>
<td>The IP address, fully qualified domain name, or URL for the cloud library.</td>
</tr>
<tr>
<td>Alibaba Cloud Object Storage Service</td>
<td>Access_Key_ID</td>
<td>Access key for the account.</td>
</tr>
<tr>
<td></td>
<td>Secret_Access_Key</td>
<td>Secret key for the account.</td>
</tr>
<tr>
<td></td>
<td>Bucket</td>
<td>Container for VM or instance volumes (disks).</td>
</tr>
<tr>
<td>AmazonS3</td>
<td>Access_Key_ID</td>
<td>Access key for the account.</td>
</tr>
<tr>
<td></td>
<td>Secret_Access_Key</td>
<td>Secret key for the account.</td>
</tr>
<tr>
<td></td>
<td>Bucket</td>
<td>Container for VM or instance volumes (disks).</td>
</tr>
<tr>
<td>AT&amp;T Synaptic Storage</td>
<td>Token_ID</td>
<td>Token ID for the account.</td>
</tr>
<tr>
<td></td>
<td>Shared_Secret</td>
<td>Secret associated with the account.</td>
</tr>
<tr>
<td></td>
<td>Root_Folder</td>
<td>Root folder for the account.</td>
</tr>
<tr>
<td>China Mobile oNest</td>
<td>Access_Key_ID</td>
<td>Access key for the account.</td>
</tr>
<tr>
<td></td>
<td>Secret_Access_Key</td>
<td>Secret key for the account.</td>
</tr>
<tr>
<td></td>
<td>Container</td>
<td>Container for instance volumes (disks).</td>
</tr>
<tr>
<td>EMC Atmos</td>
<td>Token_ID</td>
<td>Token ID for the account.</td>
</tr>
<tr>
<td></td>
<td>Shared_Secret</td>
<td>Secret associated with the account.</td>
</tr>
<tr>
<td></td>
<td>Root_Folder</td>
<td>Root folder for the account.</td>
</tr>
<tr>
<td>Google Cloud Storage</td>
<td>Access_Key_ID</td>
<td>Access key for the account.</td>
</tr>
<tr>
<td></td>
<td>Secret_Access_Key</td>
<td>Secret key for the account.</td>
</tr>
<tr>
<td></td>
<td>Bucket</td>
<td>Container for instance volumes (disks).</td>
</tr>
<tr>
<td>HDS Hitachi Content</td>
<td>Username</td>
<td>Name of the user account to access.</td>
</tr>
</tbody>
</table>
## Virtual Server Protection (VSP) - Version 11 Service Pack 11

<table>
<thead>
<tr>
<th>Platform</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>the cloud library.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password</td>
</tr>
<tr>
<td></td>
<td>Password for the user account to access the cloud library.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Namespace</td>
</tr>
<tr>
<td></td>
<td>Container for VM or instance volumes (disks).</td>
</tr>
<tr>
<td>HGST Storage</td>
<td></td>
</tr>
<tr>
<td>Access_Key_ID</td>
<td>Access key for the account.</td>
</tr>
<tr>
<td>Secret_Access_Key</td>
<td>Secret key for the account.</td>
</tr>
<tr>
<td>Bucket</td>
<td>Container for instance volumes (disks).</td>
</tr>
<tr>
<td>Huawei Object Storage</td>
<td></td>
</tr>
<tr>
<td>Access_Key_ID</td>
<td>Access key for the account.</td>
</tr>
<tr>
<td>Secret_Access_Key</td>
<td>Secret key for the account.</td>
</tr>
<tr>
<td>Bucket</td>
<td>Container for instance volumes (disks).</td>
</tr>
<tr>
<td>Microsoft Azure Storage</td>
<td></td>
</tr>
<tr>
<td>Account Name</td>
<td>Subscription ID for the account.</td>
</tr>
<tr>
<td>Access Key</td>
<td>Access key for the account.</td>
</tr>
<tr>
<td>Container</td>
<td>Container for VM or instance volumes (disks).</td>
</tr>
<tr>
<td>OpenStack Object Storage</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>Name of the user account to access the cloud library.</td>
</tr>
<tr>
<td>API_Key</td>
<td>Password for the user account to access the cloud library.</td>
</tr>
<tr>
<td>Container</td>
<td>Container for VM or instance volumes (disks).</td>
</tr>
<tr>
<td>Oracle Cloud Infrastructure</td>
<td></td>
</tr>
<tr>
<td>Archive Storage</td>
<td></td>
</tr>
<tr>
<td>Tenancy OCID</td>
<td>Oracle Cloud ID.</td>
</tr>
<tr>
<td>User OCID</td>
<td>User name for the Oracle Cloud ID.</td>
</tr>
<tr>
<td>Key's fingerprint</td>
<td>PEM key's fingerprint.</td>
</tr>
<tr>
<td>Compartment name</td>
<td>The OCI compartment name.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PEM key filename</td>
</tr>
<tr>
<td></td>
<td>The PEM filename containing the private-key.</td>
</tr>
<tr>
<td></td>
<td>Make sure that the PEM key file is copied and available in all the MediaAgents using the library under the following folder:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;software install folder&gt;/Base/Certificates</code></td>
</tr>
<tr>
<td>Storage Service</td>
<td>Private key's password</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Oracle Cloud Infrastructure Archive Storage</td>
<td>Password for the private key.</td>
</tr>
<tr>
<td>Username</td>
<td>Name of the user account to access the cloud library.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the user account to access the cloud library.</td>
</tr>
<tr>
<td>Container</td>
<td>Container for VM or instance volumes (disks).</td>
</tr>
<tr>
<td>Tenancy OCID</td>
<td>Oracle Cloud ID.</td>
</tr>
<tr>
<td>User OCID</td>
<td>User name for the Oracle Cloud ID.</td>
</tr>
<tr>
<td>Key's fingerprint</td>
<td>PEM key's fingerprint.</td>
</tr>
<tr>
<td>Compartmen name</td>
<td>The OCI compartment name.</td>
</tr>
<tr>
<td>PEM key filename</td>
<td>The PEM filename containing the private-key.</td>
</tr>
<tr>
<td></td>
<td>Make sure that the PEM key file is copied and available in all the MediaAgents using the library under the following folder:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;software install folder&gt;/Base/Certificates</code></td>
</tr>
<tr>
<td>Private key's password</td>
<td>Password for the private key.</td>
</tr>
<tr>
<td>Bucket</td>
<td>Container for VM or instance volumes (disks).</td>
</tr>
<tr>
<td>Oracle Cloud Infrastructure Object Storage Classic</td>
<td>Username</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the user account to access the cloud library.</td>
</tr>
<tr>
<td>Container</td>
<td>Container for VM or instance volumes (disks).</td>
</tr>
<tr>
<td>Rackspace Cloud Files</td>
<td>Username</td>
</tr>
<tr>
<td>API_KEY</td>
<td>Key for the Rackspace account.</td>
</tr>
</tbody>
</table>
Configuring a Tape Library as a Storage Target

You can configure a tape library as a storage target. Before configuring the tape library make sure that the library is attached to the MediaAgent in which it will be configured.

**Procedure**

1. From the navigation pane, click **Storage Targets**.
2. Click **Add storage** in the upper right of the page, and then select **Tape**.
3. In the **Add tape storage**, select the MediaAgent to which the tape library is attached from the **MediaAgent** list.
4. Click **Scan hardware**.
5. The tape library attached to the selected MediaAgent is detected and appears as **Not configured**.
6. Click **Select all** or click the library that you wish to configure.
7. Click **Configure**.
8. The tape library appears as **Configured**.
9. Click **Cancel** to exit the dialog box.

**Result**

The tape library is available. You can associate the tape library with a plan.
Exporting Media

Procedure

1. From the navigation pane, click **Storage Targets** > **tape_library**.
   The **tape_library** page is displayed.
2. Click the **Actions** button ⬤ and click **Export media**.
   The Export media dialog box is displayed.
3. Select the appropriate media to be exported.
4. Select the **New export location** check box and add or choose the location where you want to export the media.
5. Click **OK**.

Result

The media will be moved to the mail slot and an event will be logged. Click **Events** to view the event.

Resetting a Library

The reset library operation un-mounts the media mounted in all the drives, and resets drives so that they are ready for use. The reset library option is especially useful when you have tapes stuck in the drives.

Note that the reset library operation will fail if there are jobs running on the library.

Procedure

1. From the navigation pane, click **Storage Targets**.
2. Click the **Actions** button ⬤ and click **Reset library**.
3. Click **Yes** in the **Confirm reset library** prompt.

Result

The library will be reset and a message will be briefly displayed in the upper right corner. An informational event will be logged in the **Events** page.
Deconfiguring a Library

Deconfiguring a library deletes the library as a storage target and also disables software communications between the MediaAgent and the device.

Note that the de-configure operation will fail in the following situations:

- If there are jobs currently running in the library. If necessary, wait for the jobs to complete or kill the jobs in the library.
- If media is mounted in the drives. If media is mounted, Unload the Media, (on page 160) before de-configuring the library.

Procedure

1. From the navigation pane, click **Storage Targets**.
2. Click the **Actions** button and click **Deconfigure**.
3. Click **Yes** in the **Confirm delete** prompt.

Result

The library will be deleted and an informational event will be logged in the **Events** page.

Validating a Drive

The drive validation process ensures that the drive is functioning properly by mounting a media, writing on the media, re-winding and seeking data and then reading back from the media.

It is recommended that a drive validation operation is performed after configuring the libraries and drives and before performing a data protection operation.

Drive validation can also be performed to check the throughput of the device. In addition, you can verify whether different tape block size is supported by the hardware and operating system, by performing a drive validation operation.

Procedure

1. From the navigation pane, click **Storage Targets** > **tape_library**.
   The **tape_library** page is displayed.
2. Click the **Actions** button and click **Validate drive**.
   The Validate Drive dialog box is displayed.
3. In the **MediaAgent** box, select the MediaAgent that must be used to perform the validation.

4. In the **Drive pool** box, select the drive pool that must be used to perform the validation.

5. In the **Volume block size (KB)** box, select the media block size that must be used by the validation operation to write data on the media.

6. In the **Chunk size** box, select the chunk size that must be used by the validation operation to create a block.

7. In the **Amount to Write** options, select **Write chunks to end of media** option to specify that the validation operation must write chunks to the end of the volume or select the **Write the specific number of chunks** option to specify that the validation operation must write only the specified number of chunks.

8. Click **OK**.

**Result**

This will initiate a Storage Validation job. Click **Jobs** to view the progress of the job.

---

### Cleaning a Drive

The drive cleaning process mounts the cleaning tape and cleans the drive. In addition, this operation also resets the counters that keep track of the number of drive events that have occurred since the drive was cleaned.

**Procedure**

1. From the navigation pane, click **Storage Targets** > **tape_library**.
   
   The **tape_library** page is displayed.

2. Click the **Actions** button ⬜️ and click **Clean drive**.

3. Click **Yes** in the **Confirm clean drive** prompt.

**Result**

This will initiate a Drive Cleaning job. Click **Jobs** to view the progress of the job.

---

### Unloading a Drive

The unload drive operation unmounts the media from the drive.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Procedure

1. From the navigation pane, click **Storage Targets** > **tape_library**. The **tape_library** page is displayed.
2. Click the **Actions** button and click **Unload drive**.
3. Click **Yes** in the **Confirm unload** prompt.

Result

The media will be unloaded from the drive and a message will be briefly displayed in the upper right corner. An informational event will be logged in the **Events** page.

Resetting a Drive

The reset drive operation un-mounts media mounted in the drive, thereby making the drive ready for use. Note that the reset operation will not run if the drive is reserved or in use.

Procedure

1. From the navigation pane, click **Storage Targets** > **tape_library**. The **tape_library** page is displayed.
2. Click the **Actions** button and click **Reset drive**.
3. Click **Yes** in the **Confirm reset** prompt.

Result

The drive will be reset and a message will be briefly displayed in the upper right corner. An informational event will be logged in the **Events** page.

Reports for Tape Storage Targets

The following reports are available for tape storage targets:

All these reports can be accessed as follows:

1. From the navigation pane, click **Storage Targets** > **tape_library**.
2. Click **Report** to access the specific report.
### Report Name | Description
--- | ---
Slot View | Lists the slots and the media stored in each of the slots.
IE Ports | Lists the IE ports and provides a list of media available in each port.
Library Controller Media Agents | Provides information about the library controller associated with the library.
Drive Usage History Report per day | Provides drive usage history for the days.
Tape Media Usage | Provides the tape media usage information in the library.
User Security Settings

You can select the Security option in the navigation pane to configure users, user groups, domains, roles, and identity servers.

Updating Your Password

You can update your password.

Procedure

1. In the upper right of the page next to your user name, click the down arrow, and click User Settings. The Change password page appears.
2. In the Old password box, enter your old password for security purposes.
3. In the New password and Confirm new password boxes, enter your new password.
4. Click Save.

Users and User Groups

Users

You can create, edit, and delete users, and you can control the features the user has access to by making security associations between the user, a role, and entities.

Commvault supports Admin Console users and external users.

User Groups

User groups are a collection of users that make it easy to control a large number of users. Properties and security associations selected for the user group apply to all of the users in the group.

The following user groups are automatically created when the software is installed:

- Master
- View All
Creating a User

You create users to enable access to the Admin Console. When you create a user, you assign the user to a user group that has properties and security associations assigned to it.

Before You Begin

Create a user group (on page 164).

Procedure

1. From the navigation pane, go to Security > Users. The Users page appears.
2. In the upper right of the page, click Add user.
3. In the Add user dialog box, provide the user information.
4. To assign this user to a user group, from the User group list, select the user group.
5. To allow this user to access the Admin Console, select the Enabled check box.
6. Click Save.

Managing Users

You can edit or delete users you created in the Admin Console. Edit the user to update the user password.

Procedure

1. From the navigation pane, go to Security > Users. The Users page appears.
2. Decide if you want to edit or delete a user:
   - To edit a user, click the user name, click Edit, and in the Edit user dialog box, update the user information, and then click Save.
   - To delete a user, in the Actions column for the user, click the action button ..., and then click Delete.

Creating a User Group

A user group is a set of users who perform the same tasks. Create user groups to simplify the administration of the CommCell environment.
Procedure

1. From the navigation pane, go to Security > Users Groups.
   The Users groups page appears.
2. In the upper right of the page, click Add user group.
3. In the Add user group dialog box, provide the user group information.
4. To specify the amount of data that members of the user group can back up, do the following:
   a. Select the Quota enabled check box.
   b. In the Quota limit box, type the maximum number of gigabytes that members of the group can back up.
5. To allow users to inherit the group permissions and associations, select the Group enabled check box.
6. Endpoint: To make this a group for users who share a laptop or desktop, select the Enable for shared laptop usage check box.
   After the end-user Endpoint package is installed on a shared laptop or desktop computer, each user who registers that shared computer is treated as a separate device. For information on the operations you can perform on devices, see Operations.
7. Click Save.

Managing User Groups

You can edit or delete user groups.

Procedure

1. From the navigation pane, go to Security > Users Groups.
   The Users groups page appears.
2. Decide if you want to edit or delete a user group:
   o To edit a user group, click the user group name, under General click Edit, and in the Edit user group dialog box, update the user group information.
   o To delete a user group, in the Actions column for the user group, click the action button and click Delete.
3. If you edited the user group, click Save.

Managing User Group Membership

You can add or remove users from a user group. After a user is added to a user group, properties and security associations selected for the user group apply to the user.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Procedure

1. From the navigation pane, go to **Security > Users Groups**.
   The **Users groups** page appears.
2. Click the user group name.
   The user group details page appears.
3. Decide if you want to add or remove a user from the user group:
   - To add a user, under **Users**, click **Add users**, select the check box next to the user name, and click **Add**.
   - To remove a user, in the **Actions** column, click **Remove**, and then click **Yes** in the confirmation dialog box.

Adding Domains

You can add a domain (name) server so that users who are members of the domain can log on to the Admin Console with their domain credentials.

You can configure the Admin Console to authenticate users through a single sign-on configuration with Active Directory.

Before You Begin

If you want to use single sign-on, configure LDAP on the Active Directory Server.

Procedure

1. From the navigation pane, go to **Security > Domains**.
2. Decide if you want to create, edit, or delete a domain (name) server:
   - To create a domain (name) server, click **Add domain**.
   - To edit a domain (name) server, in the **Actions** column for the server, click the action button and click **Modify**.
   - To delete a domain (name) server, in the **Actions** column for the server, click the action button and click **Delete**.
3. In the **Add domain** or **Edit domain** dialog box, provide the following information:
   a. In the **NETBIOS name** box, type the fully qualified domain name that you use to identify this network resource, for example, my.domain.example.com.
   b. In the **Domain Name** box, type the fully qualified domain name, for example, my.domain.example.com.
   c. In the **User name** and **Password** boxes, type the credentials for a user who has at least read permission for the domain.
d. To allow users to automatically log on, select the **Enable SSO** check box.

4. Click **Save**.

5. If you selected the **Enable SSO** check box, restart the Tomcat services on the Admin Console computer.

---

### Managing Roles

A role is a collection of permissions that defines the level of access granted to a user or a user group. Permissions allow users to perform tasks such as performing backup, restore, and administrative operations (for example, license administration) on entities. To use role-based security, you must create a security association between users or user groups, a role, and entities.

A role can be a part of as many security associations as needed, but each security association can only have one role.

Commvault offers predefined roles that address typical security needs. These roles can be customized by the administrator.

**Procedure**

1. From the navigation pane, go to **Security > Roles**. The **Roles** page appears.

2. Decide if you want to create or edit a role:
   - To create a role, click **Add Role**.
   - To edit a role, click the role name.

3. In the **Add role** or **Edit role** dialog box, add or remove permissions:
   - To add a permission, select the check box next to the permission.
   - To remove a permission, clear the check box next to the permission.

4. Click **Save**.

---

### Adding Identity Servers

You can add third-party identity providers (IdP), such as Okta and ADFS, so that users can be authenticated. SAML metadata is used to share configuration information between the Identity Provider (IdP) and the Service Provider (SP). Metadata for the IdP and the SP is defined in XML files:
The IdP metadata XML file contains the IdP certificate, the entity ID, the redirect URL, and the logout URL. For an example, see Sample SAML IdP Metadata XML (on page 169).

The SP metadata XML file contains the SP certificate, the entity ID, the Assertion Consumer Service URL (ACS URL), and a log out URL (SingleLogoutService). For an example, see Sample SAML SP Metadata XML (on page 169).

Before using SAML to log on to the Web Console or Admin Console, metadata from the IdP must be uploaded and metadata from the SP must be generated. After the SP metadata is generated, it must be securely shared with the IdP. Contact the IdP for instructions on sharing the SP metadata.

Before You Begin

1. Create or get an Identity Provider (IdP) metadata XML file using the SAML protocol. For SAML metadata specifications, go to the Oasis (https://www.oasis-open.org/) website, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0.
   For an example, see Sample SAML IdP Metadata XML (on page 169).
2. Create a keystore file. For information on keystore files, see Creating Certificates for SAML Integration (on page 170).

Procedure

1. From the navigation pane, go to **Security > Identity servers**.
2. To create an identity server, click **Add**.
   The **Add SAML App** dialog box is displayed.
3. In the **Application Name** box, enter an application name.
4. If you are an MSP administrator creating the SAML app for a company, in the **Created for company** box, select the company.
   If you are creating the SAML app for the entire CommCell environment or if you are a tenant administrator, a company is not needed.
5. Upload the IdP metadata:
   a. Next to the **Upload IDP metadata** box, click **Browse**.
   b. Browse to the location of the XML file that contains the IdP metadata, select the file, and click **Open**.
6. Generate the SP metadata:
   a. Under **Generate new SP metadata**, next to the **Upload key store file** box, click **Browse**.
   b. Browse to the location of the keystore file, for example, C:\security\mykeystore.jks, select the file, and click **Open**.
7. Enter the keystore file values for **Alias name**, **Key Store Password**, and **Key Password**.
8. To generate the SP metadata and to save the IdP metadata, click **Save**.
   After the SP metadata is generated, it must be securely shared with the IdP. Contact the IdP for instructions on sharing the SP metadata.
Sample SAML IdP Metadata XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAuthnRequestsSigned="false">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Sample SAML SP Metadata XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true">
    <AssertionConsumerService isDefault="true" index="0" Location="https://client.mydomain.com:443/webconsole/samlAcsIdpInitCallback.do?samAppKey=NjZEOUQ1RDRCQjE1NEI0" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
  </SPSSODescriptor>
</EntityDescriptor>
```
Creating Certificates for SAML Integration

In Service Provider (SP) initiated SAML, a SAML request is prepared by the SP. The SP digitally signs the request using a private key. When the request is received by the Identity Provider (IdP), the digital signature is verified using the public key sent by the SP in a certificate. Certificates are self-signed or signed by a certification authority (CA).

A Java keystore file stores the certificate and the private key. To create the Java keystore file, use the keytool utility, the Java key and certificate management tool. For more information on the keytool utility, go to the Oracle Documentation (http://www.oracle.com/technetwork/documentation/index.html) website, keytool - Key and Certificate Management Tool.

Procedure

Creating a Self-Signed Certificate and a Private Key

Use the keytool utility to create a keystore file that contains a private key and a self-signed certificate that holds a public key.

1. Run the following command from the C:\Program Files\Java\java_version\bin folder after substituting the parameter values.

```
keytool -genkey -keyalg RSA -alias <aliasName> -keystore <file_path>keystoreFilename.jks -validity <daysValid> -keysize 2048
```

2. The command can be run from %JAVA_HOME%\bin if the %JAVA_HOME% environment variable is set.

```
keytool -genkey -keyalg RSA -alias <aliasName> -keystore <file_path>keystoreFilename.jks -validity <daysValid> -keysize 2048
```

3. The following table displays the parameters for the keytool command:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description of Parameter Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>The alias name for the certificate.</td>
</tr>
<tr>
<td>keystore</td>
<td>The file path and file name for the .jks file created by the keytool.</td>
</tr>
<tr>
<td>validity</td>
<td>The number of days the keystore file is valid starting from the day the keystore file is created.</td>
</tr>
</tbody>
</table>

**Example**

```
keytool -genkey -keyalg RSA -alias selfsigned -keystore "C:\mykeystore.jks" -validity 365 -keysize 2048
```

4. When prompted, enter the information requested by the keytool command.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

5. Make note of the following values:
   - name and location of the keystore file
   - alias name
   - keystore password
   - key password

   Use these values to create the SP metadata XML file. For information, see Adding Identity Servers (on page 167).

Creating a CA-signed Certificate and a Private Key

Use the keytool utility to create a keystore file that contains a private key and a CA-signed certificate that holds a public key.

1. Create a keystore file containing a local certificate:
   a. Run the following command from the C:\Program Files\Java\java_version\bin folder after substituting the parameter values.

   The command can be run from %JAVA_HOME%\bin if the %JAVA_HOME% environment variable is set.

   ```
   keytool -genkey -keyalg RSA -alias <aliasName> -keystore <file_path\keystoreFilename.jks>
   ```

   The following table displays the parameters for the keytool command:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description of Parameter Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>The alias name for the certificate. The alias name is used to import the CA-signed certificate.</td>
</tr>
<tr>
<td>keystore</td>
<td>The file path and file name for the .jks file created by the keytool.</td>
</tr>
</tbody>
</table>

   **Example**

   ```
   keytool -genkey -keyalg RSA -alias casigned -keystore "C:\mykeystore.jks"
   ```

   b. When prompted, enter the information requested by the keytool command.

      For CA-signed certificates, the company and location information must be accurate, for example, when prompted for the **Organization Name**, enter the full legal name of your organization.

   c. Make note of the following values:
      - name and location of the keystore file
      - alias name
      - the keystore password
      - the key password

      After the CA-signed certificate is imported into the keystore file, use these values to create the SP metadata XML file. Use these values to create the SP metadata XML file. For information, see Adding Identity Servers (on page 167).

2. Generate a Certificate Signing Request (CSR) and submit it to the CA.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

a. Run the following command from the C:\Program Files\Java\java_version\bin folder after substituting the parameter values.

The command can be run from %JAVA_HOME%\bin if the %JAVA_HOME% environment variable is set.

keytool -certreq -keyalg RSA -alias <aliasName> -file <request_file_name.csr> -keystore <file_path\keystoreFilename.jks>

The following table displays the parameters for the keytool command:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description of Parameter Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>The alias name for the certificate. The alias name is used to import the CA-signed certificate.</td>
</tr>
<tr>
<td>file</td>
<td>The file name of the .csr file.</td>
</tr>
<tr>
<td>keystore</td>
<td>The file path and file name for the .jks file created by the keytool.</td>
</tr>
</tbody>
</table>

Example

keytool -certreq -keyalg RSA -alias casigned -file certreq.csr -keystore "C:\mykeystore.jks"

b. Submit the .csr file to your CA according to their procedure.

3. Import the CA-signed certificate into the keystore file according to the procedure provided by the CA.

Run the following command from the C:\Program Files\Java\java_version\bin folder after substituting the parameter values.

The command can be run from %JAVA_HOME%\bin if the %JAVA_HOME% environment variable is set.

keytool -importcert -file <CertificateFileName> -keystore <keystoreFileName> -alias <AliasName>

The following table displays the parameters for the keytool command:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description of Parameter Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>file</td>
<td>The file name of the .csr file.</td>
</tr>
<tr>
<td>keystore</td>
<td>The file path and file name for the .jks file created by the keytool.</td>
</tr>
<tr>
<td>alias</td>
<td>The alias name for the certificate.</td>
</tr>
</tbody>
</table>

Example

keytool -importcert -file certificate.cer -keystore "C:\mykeystore.jks" -alias casigned

Copyright © 2018 Commvault Systems, Inc. All rights reserved.
Identity Provider Use Cases

In the Admin Console, the procedure for setting up a SAML app for an identity provider (IdP) is the same, but each IdP has their own procedure. The Okta and Active Directory Federation Services (AD FS) use cases demonstrate different methods for setting up an IdP.

AD FS

AD FS (Active Directory Federation Services) is a service that allows the sharing of identities between federation partners. To integrate with AD FS, in AD FS retrieve IdP (identity provider) metadata, in the Admin Console add a SAML application, and in AD FS create a relying party trust.

Before You Begin

- Use the Microsoft Server Manager to install the AD FS role service. For instructions, go to the Microsoft (https://docs.microsoft.com) website, Install the AD FS Role Service.
- Important: AD FS only accepts a relying party trust that has an HTTPS URL in the metadata. This means that your Web Console must use HTTPS.

Procedure

Retrieving the IdP Metadata

1. Open the AD FS Management console:
   - From the Microsoft Server Manager, in the upper right, expand Tools, and then click AD FS Management.
2. In the left navigation pane, expand AD FS > Service, and then click Endpoints.
3. In the right pane, under Endpoints > Metadata, in the Federation Metadata row, copy the URL path.
   - For example, FederationMetadata/2007-06/FederationMetadata.xml
4. Add the host name of the AD FS computer to the URL path you copied: https://hostname/FederationMetadata/2007-06/FederationMetadata.xml.
5. To retrieve the IdP (identity provider) metadata, in a browser, paste the complete URL.
6. Save the IdP metadata as an XML file.
7. Leave the AD FS Management console open.

Creating a SAML app in the Admin Console

1. Open the Admin Console.
2. From the navigation pane, go to Security > Identity servers and create the SAML app using the IdP metadata file you saved.
3. After the SP (service provider) metadata is generated, place the SP metadata on the AD FS machine.

**Creating an Relying Party Trust**

1. From the AD FS Management console, in the left navigation pane, expand **AD FS > Trust Relationships**, right-click **Relying Party Trusts**, and then click **Add Relying Party Trust**.

   The Welcome page of the Add Relying Party Trust Wizard window appears.

2. Click **Start**.

3. On the Select Data Source page, click **Import data about the relying party from a file**.

4. In the Federation metadata file location box, browse to the location of the SP metadata that you placed on the AD FS machine.

5. Click **Next**.

6. Continue to move through the wizard, referring to Microsoft documentation to configure additional features such as multi-factor authentication and issuance authorization rules.
7. After you complete the wizard, click Close.
   The Edit Claim Rules dialog box appears.

   The Select Rule Template page of the Add Transform Claim Rule Wizard window appears.

9. From the Claim rule template list, click Send LDAP Attributes as Claims.

10. Click Next.
    The Configure Rule page appears.

11. In the Claim rule name box, enter a name for the rule.

12. From the Attribute store list, click Active Directory.

13. In the Mapping of LDAP attributes to outgoing claim types table, add the LDAP attribute and outgoing claim type:
   - From the LDAP Attribute list, choose either Email Addresses or User-Principal-Name.
From the **Outgoing Claim Type** list, choose **Name ID**.

14. Click **Finish** and then click **OK**.

**Azure**

Azure Active Directory (Azure AD) is a third-party identity provider that can act as the IdP when your users log on to the Web Console or the Admin Console.

To integrate with Azure AD, add a SAML application in the Admin Console and in your Azure AD account.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Before You Begin

- You must have the Azure Active Directory Premium P1 or Premium P2 edition. For information, go to the Microsoft Azure Active Directory documentation https://docs.microsoft.com/en-us/azure/active-directory/.

Procedure

1. In the Admin Console, begin to configure the SAML application:
   a. Open the Add SAML App dialog box, and in the Webconsole url box, copy the URL.
      For example, https://mycompany:443/webconsole
      For information about adding a SAML application in the Admin Console, see Adding Identity Servers (on page 167).
   b. Keep the Add SAML App dialog box open.

2. From the Microsoft Azure portal https://portal.azure.com, create a new application using SAML as the sign on method:
   a. From the navigation pane, go to Azure Active Directory > Enterprise applications, and click New application (New application).
   b. Under Add an application, click the Non-gallery application tile.
   c. Enter a name for the application, and then click Add.
   d. Review the overview, and complete the following steps required by Microsoft: Assign a user for testing and Create your test user in test.
   e. Click Configure single sign-on.
   f. Under Single sign-on, in the Single Sign-on Mode list, click SAML-based Sign-on.
      The SAML single sign-on options appear.
   g. Under Domain and URLs, in the Identifier and Reply URL boxes, paste the URL you copied from the Admin Console.

   h. Under User Attributes, in the User Identifier box, enter user.userprincipalname.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

i. To download the IdP metadata file, under **SAML Signing Certificate**, in the **DOWNLOAD** column, click **Metadata XML**.

3. In the Admin Console, complete the SAML application:
   a. To upload the IdP metadata XML file, in the open **Add SAML App** dialog box, next to **Upload IDP metadata**, click **Browse**.
   b. Select the IdP metadata XML file that you downloaded from the Microsoft Azure portal.
   c. Complete the application and click **Save**.
      For information about adding a SAML application in the Admin Console, see Adding Identity Servers (on page 167).

**Okta**

Okta is a third-party identity provider that can act as the IdP when your users log on to the Web Console or the Admin Console.

To integrate with Okta, add a SAML application in the Admin Console and in your Okta account.

**Procedure**

1. In the Admin Console, begin to configure the SAML application:
   a. Open the **Add SAML App** dialog box, and in the **Webconsole url** box, copy the URL.
      For example, https://mycompany:443/webconsole
      For information about adding a SAML application in the Admin Console, see Adding Identity Servers (on page 167).
   b. Keep the **Add SAML App** dialog box open.
2. In your Okta account, create a new application using SAML 2.0 as the sign on method:
   a. Follow the wizard for the general settings.
b. Under Configure SAML > SAML Settings, in the Single sign on URL and the Audience URI (SP Entity ID) boxes, paste the URL you copied from the Admin Console.

c. Continue to follow the wizard and accept the default values.

d. Click Finish.

e. Open the application and click Sign On.

f. To download the IdP metadata file, under the View Setup Instructions button, click Identity Provider metadata.

g. Save the IdP metadata file as an XML file.

3. In the Admin Console, complete the SAML application:
Virtual Server Protection (VSP) - Version 11 Service Pack 11

a. To upload the IdP metadata XML file, in the open Add SAML App dialog box, next to Upload IDP metadata, click Browse.

b. Select the IdP metadata XML file that you downloaded from Okta.

c. Complete the application and click Save.

For information about adding a SAML application in the Admin Console, see Adding Identity Servers (on page 167).

Administering the Security Associations of a Server

You can associate users, user groups, and roles to a server to control the operations that the users can perform on the server.

Procedure

1. From the navigation pane, go to Servers.

   A page listing the servers appears.

2. Under Servers, click the server.

   The server details page appears.


   The Security dialog box appears.

4. On the Associations tab, in the user box, type the user or user group name, and from the generated list, click the user or user group name.

5. In the role box, select the role and then click Add.

6. Repeat steps 4 and 5 for each user and user group and role you want to include in the security association.

7. Click Save.

Results

The users and user groups can perform actions on the server based on the permissions defined in the role.
System Settings

You can access system-level information and settings. For example, you can view license information, register your software, brand the Admin Console, and configure your email server.

Applying a License

You can update your CommCell license from the Admin Console. The CommCell license validates the products and features that you use in your CommCell environment.

You might need to apply a new license in the following scenarios:

- You are using an evaluation version of the license and the license is about to expire.
  Evaluation licenses are valid for 30 days. You can choose to extend the expiration date or to obtain a permanent license.
- You want to add more Commvault products to your CommCell environment.
- You want to change the branding settings of the Admin Console. For example, display your company name and logo in the console.

Before You Begin

Obtain the new license from your software provider.

To contact your software provider, send an email to Prodreg@commvault.com. Make sure to include your CommCell ID, which can be found in the License and Registration page of the Admin Console. For instructions on how to access the license page, see the steps in the Procedure.

Procedure

1. From the navigation pane, go to System > License.
2. On the License and Registration page, click Update license.
3. In the Update License dialog box, click Select license file and locate the license file.
4. Click Apply.

Creating Global Exceptions

Global Exceptions are exclusions that filter out data from backup operations. You can create Windows and UNIX exceptions. Global Exceptions support the use of regular expressions (or wildcards).
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Procedure

1. From the notification pane, go to System > Global Exceptions.
   The Global exceptions page appears.
2. Open the Enter path dialog box:
   - If this is the first exception in your Admin Console, click Add windows exception or Add unix exception.
   - If exceptions exist in your Admin Console, under either Windows global exceptions or Unix global exceptions, click Edit.
3. In the Enter path dialog box, type the path to the file or folder you want to exclude from the backup operation.
4. To add multiple paths, press Enter before adding the next path.
5. Click Save.

Creating a Backup Window

By default, backup operations in the Admin Console run for 24 hours without restriction. To prevent operations from running during certain time periods, define a backup window. When backup windows are configured, operations that would start within the operation window go into a queued (as opposed to pending) state. After the backup window ends, the queued operations resume automatically.

Note: If you have backup windows defined at the plan level, the plan backup windows and the global backup windows are combined. For example, if a plan backup window prevents backups from running on Thursday and the global backup window prevents backups from running on Sunday, backup jobs run for that plan will be prevented from running on both Thursday and Sunday.

Procedure

1. From the navigation pane, expand Administration > Operations, and then click Backup window.
   The Backup window appears.
2. Click Add rule.
   The Operation rule dialog box appears.
3. Enter the operation rule.
4. Click Save.

Configuring an Email Server

To send email messages from the Admin Console, you must set up an email server. For example, when you send log files, you can send email notifications to users.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Procedure

1. From the navigation pane, click CommCell.
   The CommCell details page appears.
2. Under Email settings, click Edit.
   The Configure email page appears.
3. Enter the details for the email server:
   a. In the SMTP server box, type the name of the mail server, for example, smtp.mailservername.com.
   b. In the SMTP Port box, type the mail server port. The default port is 25.
   c. In the Sender email box, type an email address.
   d. In the Sender name box, type the sender name.
4. Click Save.

Configuring Private Metrics Reporting

Private Metrics Reporting offers a way for you to host reports in your own network. The Private Metrics Reporting Server must collect data from each CommServe computer in your environment. If you have multiple CommServe computers in your environment, then you must configure data collection for each CommServe computer.

Procedure

1. From the navigation pane, go to System > Monitoring > Metrics Reporting.
   The Metrics Reporting page appears.
2. Next to Private Metrics Reporting, click Edit.
4. To collect information for reports, select any of the report types:
   o To collect information about the wellness of the CommCell, select Health Check.
   o To collect information that will help you determine how your CommCell environment is performing after you upgrade to the latest version, select Post Upgrade Check.
   o To collect information about job success, client size, and errors, select Activity.
   o To collect information about CommCell settings, select Audit.
   o To collect information about protected data sizes used to calculate billing, and to specify time periods for viewing that information, select Chargeback, and then select Daily, Weekly, or Monthly.
5. If the Download URL box is blank, type the download URL for the Private Metrics Reporting Server. For example: http://metricsserver1.domain.com/downloads/sqlscripts/
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Where metrictsserver1 is the name of your organization's Private Metrics Reporting Server. You must include the forward slash (/) at the end of the URL, otherwise the download does not work.

6. If the Upload URL box is blank, type the upload URL for the Private Metrics Reporting Server.
   For example: http://metrictsserver1.domain.com/webconsole/
   Where metrictsserver1 is the name of your organization's Private Metrics Reporting Server. You must include the forward slash (/) at the end of the URL, otherwise the upload does not work.

7. Click Configuration, and then configure client group and data collection settings:
   - To collect information for all client groups, select All Client Groups.
   - To collect information from specific client groups, clear All Client Groups, from the list, select the client groups you want to include, and then click OK.
   - To specify when report data is collected, select Data Collection Time, and then enter a time. Data collection will begin within an hour after the specified time.
   - To specify when data collection results are uploaded, in the Upload Frequency box, enter the number of days between uploads.
     The minimum frequency is one day.

8. Click Save.

Uploading Data for Cloud Metrics Reporting

This procedure is optional. When you activate data collection for the first time, data is collected within the next hour, and then uploaded to your Private Metrics Reporting Server. Once the feature is activated, data collection runs at the same time every 24 hours. Then the upload is compiled and sent to your Private Metrics Reporting Server, depending on the schedule that is configured in the upload frequency setting.

Procedure

1. From the navigation pane, go to System > Monitoring > Metrics Reporting.
   The Metrics Reporting page appears.

2. Next to Private Metrics Reporting, click Upload Now.
   A message appears that asks you to verify that you want to upload data now.

3. Click Yes.

Configuring Cloud Metrics Reporting

Cloud Metrics Reporting offers a way to view Metrics Reports without having to host a Private Metrics Reporting Server. If you want to view reports on our Cloud Services Website, you must register your product and create a login account. When you activate activate data collection for Cloud Metrics Reports, data is automatically uploaded to our Cloud Metrics Reporting Server. Our Cloud Metrics Reporting Server processes the collected data, and then displays reports based on your data on our Cloud Services Website.
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Procedure

1. From the navigation pane, go to System > Monitoring > Metrics Reporting.
   The Metrics Reporting page appears.
2. Next to Cloud Metrics Reporting, click Edit.
4. To collect information for reports, select any of the report types:
   - To collect information about the wellness of the CommCell, select Health Check.
   - To collect information about job success, client size, and errors, select Activity.
5. Click Configuration, and then configure client group and data collection settings:
   - To collect information for all client groups, select All Client Groups.
   - To collect information from specific client groups, clear All Client Groups, from the list, select the client groups you want to include, and then click OK.
   - To specify when report data is collected, select Data Collection Time, and then enter a time. Data collection will begin within an hour after the specified time.
   - To specify when data collection results are uploaded, in the Upload Frequency box, enter the number of days between uploads.
     The minimum frequency is one day.
6. To collect information for additional reports, click Advanced, and then select any of the report types:
   - To collect information that will help you determine how your CommCell environment is performing after you upgrade to the latest version, select Post Upgrade Check.
   - To collect information about user actions and events that can help with troubleshooting, select Audit.
   - To collect information about protected data sizes used to calculate billing, select Chargeback.
   - To allow the Support Team to troubleshoot your environment by collecting log files and other information, select Proactive Support.
7. Click Save.

Uploading Data for Cloud Metrics Reporting

This procedure is optional. When you activate data collection for the first time, data is collected within the next hour and then uploaded to our secure Cloud site. Once the feature is activated, collections run at the same time every 7 days, or according to the frequency setting, and then the upload is compiled and sent to the secure Cloud site.

Procedure

1. From the navigation pane, go to System > Monitoring > Metrics Reporting.
   The Metrics Reporting page appears.
2. Next to **Cloud Metrics Reporting**, click **Upload Now**.

   A message appears that asks you to verify that you want to upload data now.

3. Click **Yes**.

## Registering the Admin Console

Register your software so that you can monitor your environment by using the Worldwide dashboard and the Health report available on the Commvault Cloud website [https://cloud.commvault.com](https://cloud.commvault.com).

### Before You Begin

You must have an account on the Commvault Cloud website [https://cloud.commvault.com](https://cloud.commvault.com).

### Procedure

1. From the navigation pane, go to **System > License**.
2. On the **License and Registration** page, under **Registration details**, click **Register**.
3. In the **Register product** dialog box, type your email address and password.
4. Click **Save**.

### Result

Your Commvault Cloud account is linked to your Admin Console.

## Commvault Enterprise Software

The CommCell Console is a desktop client that provides enterprise data protection and recovery capabilities, including support for additional hypervisors, advanced configuration options, and protection for other kinds of computers and applications.

When you install the Virtual Server Protection, both the Admin Console and the CommCell Console are installed. Both user interfaces provide support for virtual machine protection.

For more information about virtualization support through the CommCell Console, see Virtualization ([http://documentation.commvault.com/commvault/v11/article?p=landing_pages/c_virtualization.htm](http://documentation.commvault.com/commvault/v11/article?p=landing_pages/c_virtualization.htm)).
Terminology

**Backups** provide full protection for virtual machines and data. **Full backups** are performed initially and can be scheduled on a periodic basis. **Incremental backups** can be performed more frequently to capture changes since the last previous backup.

**Commvault software** provides management capabilities through the CommCell Console, including advanced administrative functions in addition to the functions that are available through Virtual Server Protection. Administrative changes and operations can be performed through Virtual Server Protection or the CommCell Console; any changes made through one interface are saved in the application database and are available from either interface.

**Deduplication** identifies each block of data that is backed up and ensures that it is stored only once. Deduplication is automatically enabled for VSP and is managed through the storage policy and its copies.

**Hypervisors** are platforms for hosting virtual machines, such as VMware, Microsoft Hyper-V, Citrix Xen, and Red Hat Enterprise Virtualization.

**Job streams** move content identified in a subclient to a MediaAgent, which manages **data streams** to storage resources. Subclient properties can specify the optimal number of readers or streams. The actual number of job streams is determined by the associated storage policy and the available data paths. Multiple job streams can be included in each data stream. Stream data can use compression, encryption, and deduplication.

**MediaAgents** transmit data between servers and storage media and manage backup data stored on media.

**Retention** determines how long backed up data is retained. Retention controls are available at the subclient, job, media, and policy levels. Retention controls can be used to determine what storage media (for example, disk or tape) are used for different types of data, and when **data aging** can be used to remove or overwrite backed up data.

**Snapshots** capture point-in-time state information. **Hardware snapshots** capture dynamic hardware mirrored volumes that can be quiesced, split apart and mounted on a proxy server, and used as a source for backup, archive, replication, or offline mining to minimize the impact on the production host. A hardware snapshot can also be used to recover a volume that is lost on the production server. **Software snapshots** can be used to get stable, crash-consistent backups when locked or opened files might be a concern.

**Subclients** identify virtual machines to be backed up. They are equivalent to **collections** in the Admin Console.

The **Virtual Server Agent** is installed on computers that can perform backup and restore operations for a specific hypervisor platform such as VMware and Microsoft Hyper-V. For VMware support, the VSA is installed on one or more physical computers or virtual machines. For Microsoft Hyper-V support, the VSA is installed on a standalone Hyper-V server or on Hyper-V servers in a cluster.

**Virtualization clients** enable connections to hypervisors. They are equivalent to **servers** in the Admin Console.

The **Web Console** provides a self-service interface for end users of virtual machines, enabling them to recover VM data and (if configured) provision virtual machines. These components are installed automatically with Commvault software on a production server where IIS is enabled.

**Web Server** software enables the presentation of the Virtual Server Protection interface as a web application.

**Storage Policies** specify data retention and copy settings for storage locations. Virtual Server Protection automatically creates storage policies for disaster recovery and for backup storage.
Disclaimer

Minor revisions and service packs that are released by application and operating system vendors are supported by our software but may not be individually listed in our System Requirements. We will provide information on any known caveat for the revisions and service packs. In some cases, these revisions and service packs affect the working of our software. Changes to the behavior of our software resulting from an application or operating system revision or service pack may be beyond our control. The older releases of our software may not support the platforms supported in the current release. However, we will make every effort to correct the behavior in the current or future releases when necessary. Please send an email to VM@commvault.com (Mailto:VM@commvault.com) for any problem with a specific application or operating system.

Additional considerations regarding minimum requirements and End-of-Life policies from application and operating system vendors are also applicable.
Index

A
Accessing the Admin Console - 10, 12
AD FS - 173
Adding a Failover Group - 79, 80, 83
Adding a Google Cloud Platform Hypervisor - 24
Adding a Hypervisor - 13, 17, 22
Adding a Microsoft Azure Hypervisor - 24, 122
Adding a Microsoft Azure Stack Hypervisor - 25
Adding a Microsoft Hyper-V Hypervisor - 26
Adding a Microsoft Hyper-V Hypervisor to an Array - 139
Adding a Mount Path - 152
Adding a Nutanix AHV Hypervisor - 28
Adding a Plan to a Subclient or VM Group - 65, 73
Adding a Post Script - 82
Adding a Pre Script - 82
Adding a Server to an Array - 141
Adding a Storage Array to the CommServe Database - 139, 140, 142
Adding a Subclient - 13, 17, 37, 140
Adding a VMware Hypervisor - 32
Adding a VMware Hypervisor to an Array - 140
Adding an Amazon Hypervisor - 23, 120
Adding an OpenStack Hypervisor - 29

Adding an Oracle Cloud Infrastructure Classic Hypervisor - 30, 126
Adding an Oracle VM Hypervisor - 31
Adding Domains - 166
Adding Identity Servers - 167, 171, 174, 177, 178, 180
Administering the Security Associations of a Server - 180
Alert Information for Triggered Alerts - 17, 146
Alerts - 87, 144
Amazon Restores - 88
Applying a License - 181
Attaching a Disk to an Existing VM for VMware - 113
Attaching a Volume to an Existing Amazon Instance - 89
Automatic Failover - 79
Azure - 176
Azure Restores - 91
Azure Stack Restores - 94

B
Backing Up Individual VMs On Demand - 87
Backup Job Summary - 18, 131
Backups - 12, 17, 85
Buying VSP or Extending Your VSP License - 8

C
Cleaning a Drive - 160
Cloud Provider Information - 153, 154
Commvault Enterprise Software - 186
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completing the Core Setup Wizard</td>
<td>10, 12, 14</td>
</tr>
<tr>
<td>Configuration for Virtualization</td>
<td>18</td>
</tr>
<tr>
<td>Configuring a Cloud Library as a Storage Target</td>
<td>153</td>
</tr>
<tr>
<td>Configuring a Disk Library as a Storage Target</td>
<td>151</td>
</tr>
<tr>
<td>Configuring a Firewall for a VSA Proxy in the Cloud</td>
<td>20, 120</td>
</tr>
<tr>
<td>Configuring a Tape Library as a Storage Target</td>
<td>157</td>
</tr>
<tr>
<td>Configuring an Email Server</td>
<td>182</td>
</tr>
<tr>
<td>Configuring Cloud Metrics Reporting</td>
<td>184</td>
</tr>
<tr>
<td>Configuring Private Metrics Reporting</td>
<td>183</td>
</tr>
<tr>
<td>Controlling Activities</td>
<td>147</td>
</tr>
<tr>
<td>Controlling Jobs</td>
<td>147</td>
</tr>
<tr>
<td>Creating a Backup and Replication Plan</td>
<td>65, 66</td>
</tr>
<tr>
<td>Creating a Backup Window</td>
<td>182</td>
</tr>
<tr>
<td>Creating a Life Cycle Policy</td>
<td>62, 132</td>
</tr>
<tr>
<td>Creating a Replication Group</td>
<td>65, 69, 80</td>
</tr>
<tr>
<td>Creating a Replication Target</td>
<td>65, 66, 67, 69, 70, 80, 83</td>
</tr>
<tr>
<td>Creating a Server Plan</td>
<td>15, 38, 136</td>
</tr>
<tr>
<td>Creating a Snap Plan</td>
<td>18, 39, 138, 139, 140</td>
</tr>
<tr>
<td>Creating a User</td>
<td>164</td>
</tr>
<tr>
<td>Creating a User Group</td>
<td>164</td>
</tr>
<tr>
<td>Creating an Alert Definition</td>
<td>144</td>
</tr>
<tr>
<td>Creating Certificates for SAML Integration</td>
<td>168, 170</td>
</tr>
<tr>
<td>Creating Disk (Volume) Filters</td>
<td>49</td>
</tr>
<tr>
<td>Creating Global Exceptions</td>
<td>181</td>
</tr>
<tr>
<td>Creating VM (Instance) Filters</td>
<td>13, 45</td>
</tr>
<tr>
<td>Cross-Hypervisor Restores (VM Conversion)</td>
<td>119</td>
</tr>
<tr>
<td>Customizing Views for Replication Targets</td>
<td>72</td>
</tr>
<tr>
<td>Deconfiguring a Library</td>
<td>159</td>
</tr>
<tr>
<td>Deleting Triggered Alerts</td>
<td>145</td>
</tr>
<tr>
<td>DR Orchestration and Failover Groups</td>
<td>77</td>
</tr>
<tr>
<td>Editing a Group</td>
<td>84</td>
</tr>
<tr>
<td>Editing a Replication Group</td>
<td>71</td>
</tr>
<tr>
<td>Editing Alert Definitions</td>
<td>145</td>
</tr>
<tr>
<td>Editing Hypervisor Information</td>
<td>35</td>
</tr>
<tr>
<td>Editing Hypervisor Options</td>
<td>36, 87, 88, 92, 101, 105, 107, 109, 112, 115</td>
</tr>
<tr>
<td>Editing Subclient Options for Amazon</td>
<td>51</td>
</tr>
<tr>
<td>Editing Subclient Options for Azure</td>
<td>52</td>
</tr>
<tr>
<td>Editing Subclient Options for Azure Stack</td>
<td>53</td>
</tr>
<tr>
<td>Editing Subclient Options for Google Cloud Platform</td>
<td>53</td>
</tr>
<tr>
<td>Editing Subclient Options for Hyper-V</td>
<td>54</td>
</tr>
<tr>
<td>Editing Subclient Options for Nutanix AHV</td>
<td>55</td>
</tr>
<tr>
<td>Editing Subclient Options for OpenStack</td>
<td>56</td>
</tr>
<tr>
<td>Editing Subclient Options for Oracle Cloud Classic</td>
<td>56</td>
</tr>
<tr>
<td>Editing Subclient Options for Oracle VM</td>
<td>57</td>
</tr>
<tr>
<td>Editing Subclient Options for VMware</td>
<td>57</td>
</tr>
</tbody>
</table>
Virtual Server Protection (VSP) - Version 11 Service Pack 11

Resetting a Drive - 161
Resetting a Library - 158
Restore Job Summary - 18, 131
Restores - 12, 87
Restoring a VMware VM as a Hyper-V VM - 125
Restoring a VMware VM as an Amazon Instance - 120
Restoring a VMware VM as an Azure VM - 122
Restoring a VMware VM as an Oracle Cloud Classic Instance - 126
Restoring Full Instances for Amazon - 90
Restoring Full Instances for Google Cloud Platform - 96
Restoring Full Instances for OpenStack - 104
Restoring Full Instances for Oracle Cloud Classic - 108
Restoring Full Virtual Machines for Hyper-V - 99
Restoring Full Virtual Machines for Nutanix Acropolis - 101
Restoring Full Virtual Machines for VMware - 115
Restoring Full VMs for Azure - 93
Restoring Full VMs for Microsoft Azure Stack - 94
Restoring Full VMs for Oracle VMs - 110
Restoring Guest Files and Folders for Amazon - 88
Restoring Guest Files and Folders for Azure - 91
Restoring Guest Files and Folders for Hyper-V - 98
Restoring Guest Files and Folders for Nutanix AHV - 100
Restoring Guest Files and Folders for OpenStack - 105
Restoring Guest Files and Folders for VMware - 112
Restoring Guest Files for Oracle Cloud Classic - 107
Restoring Guest Files for Oracle VM - 109
Restoring Virtual Machine Disk Files - 118
Running Orchestration Jobs - 85

S
Sample SAML IdP Metadata XML - 168, 169
Sample SAML SP Metadata XML - 168, 169
Scheduling Planned Failovers and Test Boots - 84
Security Configuration for End Users - 20
Security Configuration for Virtualization - 18
Sending Log Files - 148
Server Plans - 135
Snap Plans - 18, 39, 86, 98, 137
Storage Pool - 136, 138, 143
Storage Targets - 151
Storage Utilization - 18, 132
Subclient Options - 13, 40, 51, 140
Subclients (VM Groups) - 37
System Requirements for Virtualization - 8, 9
System Settings - 181

T
Testing Failover - 83
Virtual Server Protection (VSP) - Version 11 Service Pack 11

U

Unloading a Drive - 159, 160
Updating Your Password - 163
Uploading Data for Cloud Metrics Reporting - 184, 185

User Security Settings - 20, 163
Users and User Groups - 163
Using the Setup Wizard for the Virtualization Application - 11, 12, 14, 18
Using the Virtualization Dashboard to Manage Data Protection - 17

V

Validating a Drive - 159
Viewing Events - 17, 146
Viewing Hypervisor and Subclient Details - 17, 32

Viewing Jobs - 148
Viewing Triggered Alerts - 145
Viewing Virtual Machine Information - 17, 129
Virtual Server Agent (VSA) Requirements - 13
Virtualization - 10, 11
Virtualization SLA - 18, 130
VMs for a Hypervisor or Subclient - 33, 34, 61
VMware Restores - 112
Visit the Commvault Documentation website for complete documentation of Commvault products.