ALIBABA CLOUD

Alibaba Cloud

Hybrid Backup

Product Introduction

Document Version: 20220606

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

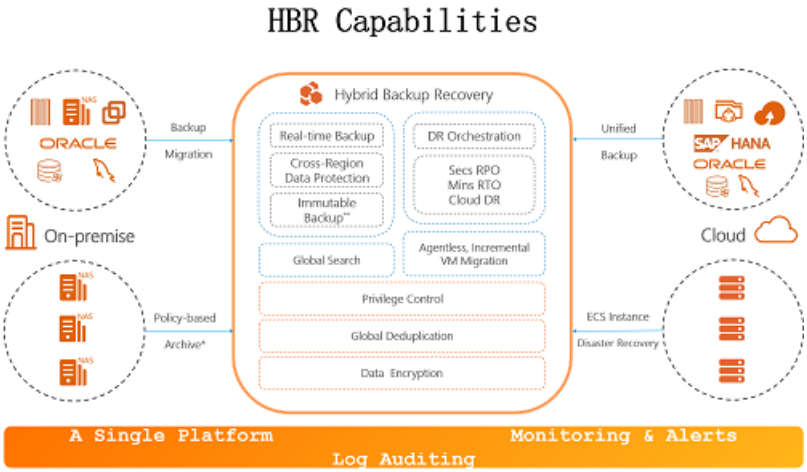
Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is Hybrid Backup Recovery?

Hybrid Backup Recovery (HBR) is a fully-managed online backup service that allows you to back up data to the cloud in a convenient, efficient, and secure manner. You can use HBR to back up data to a cloud vault from Elastic Computing Service (ECS) instances, ECS databases, ECS files, Apsara File Storage NAS file systems, NAS clusters, Object Storage Service (OSS) buckets, and self-managed data centers that store files, databases, virtual machines (VMs), and large scale NAS file systems. You can also implement disaster recovery and archive data based on the archive policies that you configure for the preceding resources.

Architecture



- Back up data to the cloud
  You can efficiently back up important data to a backup vault by using an internal network. Backup data sources include ECS files, self-managed MySQL, Oracle, SQL Server, and SAP HANA databases, NAS file systems, and OSS buckets. You can perform real-time backups of MySQL and Oracle databases with a near-zero recovery point objective (RPO) in real time. In addition, you can back up data from other cloud platforms to a backup vault on Alibaba Cloud.
- Back up on-premises data to the cloud
  You can back up on-premises data from servers, NAS file systems, VMware VMs, and databases to a backup vault on the cloud. You can configure backup policies based on your business requirements.
- Backup and disaster recovery of ECS instances across regions
  - HBR provides mirror vaults for you to back up data across regions. This enhances data security.
  - HBR supports high-performance cross-region disaster recovery with recovery point objective (RPO) in seconds and recovery time objective (RTO) in minutes.
- Migrate VMware VMs to the cloud
  HBR allows you to migrate on-premises VMware VMs to the cloud in an agentless manner. You can also use HBR to perform incremental migration with ease.
- Archive files from on-premises NAS file systems to the cloud
  HBR allows you to archive a large number of files from your on-premises NAS file systems to an archive vault on the cloud. You can customize an archive policy. You can also search on-premises storage space and archive libraries for files in a full-text manner within seconds.

Terms

The following table describes the terms that are used in HBR.

Term	Description
Backup source	The host on which the data that you want to back up is stored, such as a server, a virtual machine, or an ECS instance.
Client	The client that you install on a backup source to back up and restore data. You must install an appropriate client for different backup sources. Each client supports timed retry to guarantee backup stability. This way, data can be backed up even when temporary network jitter occurs.
Region	The physical location of an Alibaba Cloud data center. After a resource is created, you cannot change the region of the resource. For more information, see Supported regions.
Backup vault	The HBR cloud repository that is used to store backup data in the cloud. You can back up data from multiple clients to the same vault. This helps you manage the backup data and reduce management time and costs. Each backup vault supports an unlimited number of clients and storage capacity with data reliability of 99.9999999999% (twelve 9s). You can install a client and extend the storage capacity based on your business requirements. You must specify an appropriate region for each backup vault to improve backup performance and facilitate disaster recovery. After a backup vault is created, you cannot change the region of the backup vault. A backup vault is also the basic unit that you can use to remove duplicates or compress data.

Supported backup sources

Backup source		Operating system
Self-managed data centers	File directories	Windows, Windows Server, or Linux
	NAS	Windows, Windows Server, or Linux
	Images of VMware vSphere virtual machines	Windows, Windows Server, or Linux
	MySQL, Oracle, and SQL Server databases	Windows, Windows Server, or Linux
Alibaba Cloud ECS	File directories of an ECS instance	Windows Server or Linux
	SAP HANA databases that are deployed on an ECS instance	Windows Server or Linux
	MySQL, Oracle, and SQL Server databases deployed on an ECS instance	Windows Server or Linux

Backup source		Operating system
	Cloud disks (system disks and data disks)	N/A
Cloud Storage Gateway (CSG)	File gateways deployed on Alibaba Cloud	N/A
Apsara File Storage NAS	Data stored in Apsara File Storage NAS	N/A
Alibaba Cloud OSS	Data stored in OSS	N/A

2.Advantages

is a unified platform that is developed by Alibaba Cloud for backup and disaster recovery (BDR). HBR provides features such as data backup, disaster recovery, and policy-based archive management.

Necessity of BDR

BDR is an important method for enterprises to protect core business data against ransomware, system failures, natural disasters, and O&M accidents that cause data loss and damage. BDR helps enterprises meet data security and compliance requirements in various industries.

- Data risks
  Ransomware, system failures, natural disasters, and O&M accidents have huge negative impact on business data. This may lead to unexpected data loss and damage.
- Data security and compliance requirements
  The following information security regulations clearly state that **data integrity, confidentiality, and availability shall be maintained**: Multi-level Protection Scheme (MLPS) 2.0, Personal Information Protection Law (PIPL), and Regulation on Protecting the Security of Critical Information.
  In 2020, a core employee of a company deleted a database without authorization. The event disrupted the SaaS business of the company. The company lost over one billion Hong Kong dollar of market value. Millions of merchants suffered temporary business suspension.
  In 2020, a cyber attacker demanded a ransom of CNY 230 million after the attacker encrypted 30 TB of data stored on the core server of a factory by using ransomware.

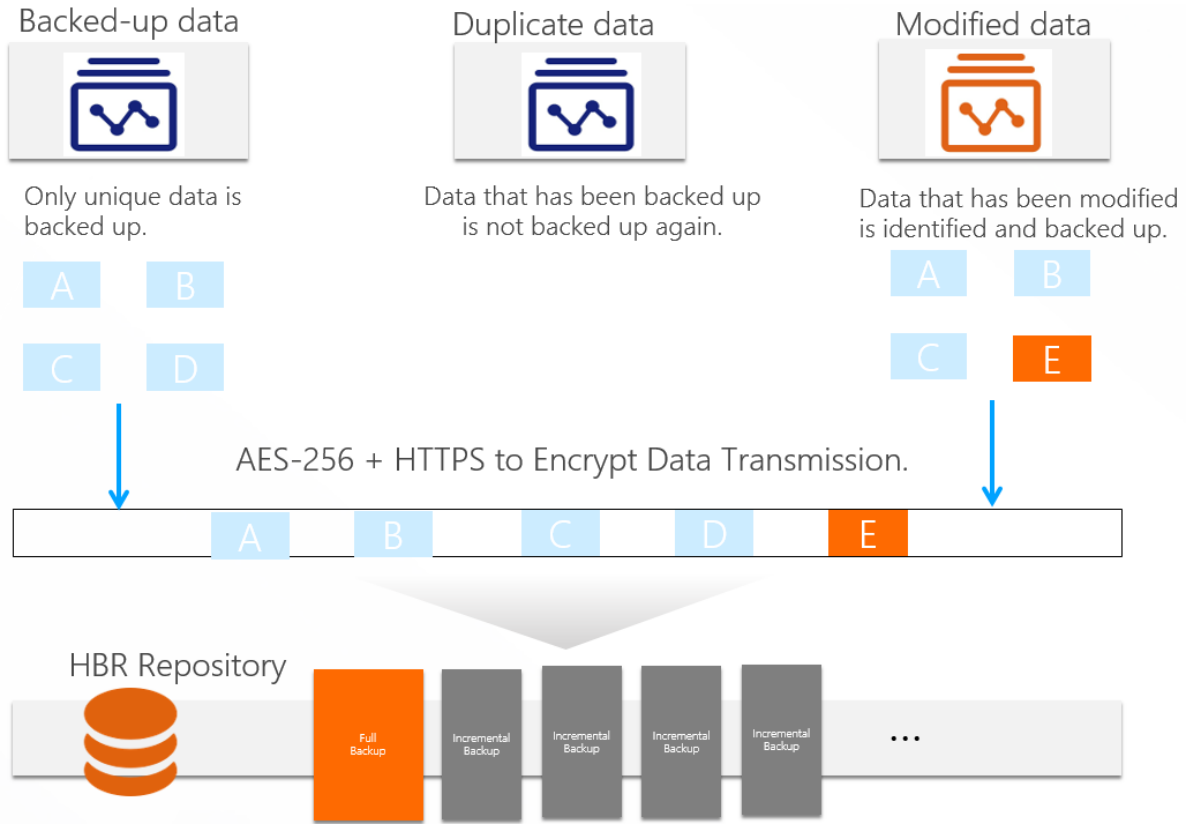
Advantages of HBR cloud disaster recovery

HBR cloud disaster recovery has the following advantages over traditional data centers in terms of cost, deployment efficiency, and O&M.

Item		Traditional data centers
Cost of ownership	You are billed for using HBR resources based on the pay-as-you-go billing method. This reduces the total cost of ownership (TCO).	You need to procure both software and hardware. Upfront costs are high.
Deployment efficiency	HBR is an out-of-the box cloud service. You can deploy the service within only one day.	Several months or years are required to build a data center.
O&M	High scalability, high reliability, and maintenance-free.	Complex O&M and high workloads.
Robustness	Geo-redundancy offers additional protection. You can enable the feature with one click.	Data loss may occur in regional natural disasters.
Recovery drill	You can perform recovery drills based on your business requirements without affecting production.	A long period of time is required to prepare for a recovery drill.

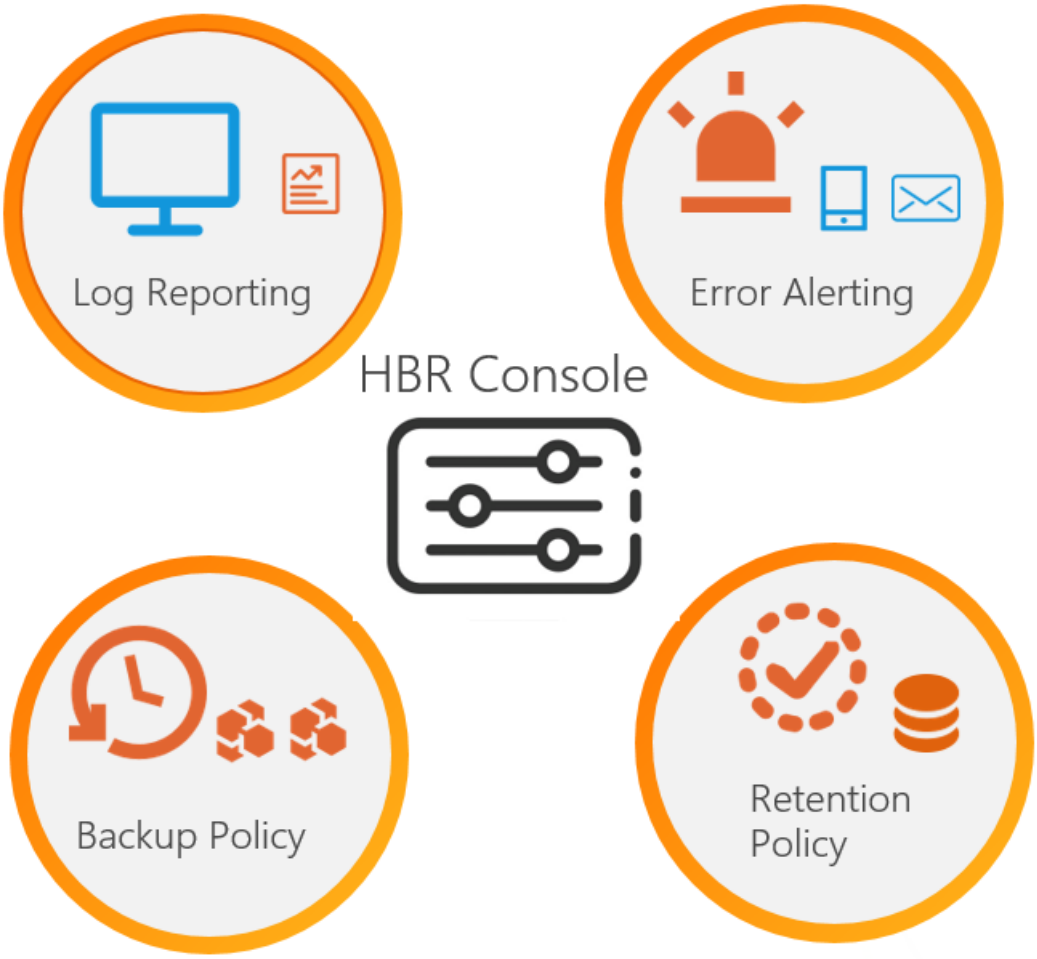
advantages

- Technical advantages
  HBR can identify and delete duplicate data with high accuracy and efficiency.



Item	Description
Features	HBR accurately identifies duplicate data in lengthened data slices and uploads and backs up only the incremental data segments of the data slices. If a data segment already exists in the backup vault, HBR does not upload the data segment to the backup vault again.
Advantages	HBR can duplicate and compress data with high efficiency. The deduplication and compression ratio can reach up to 30:1. In some scenarios, a backup service without the deduplication feature requires 30 times more storage usage than HBR.
Benefits	HBR reduces your backup and storage costs. You can retain your previous backups for a long period of time with an affordable budget. In hybrid cloud scenarios, data is deduplicated at the backup source. This can reduce the bandwidth that is consumed to migrate your business.

- O&M advantages
  Automatic backup and monitoring are supported.



Item	Description
Features	You can configure policies of full backup, incremental backup, log backup, and real-time backup as needed. You can receive alert notifications from multiple channels such as SMS messages and emails. You can also view the details about historical backup jobs and error log reports in the HBR console.
Advantages	You need to configure backup policies only once before the backup process is fully managed by HBR. HBR monitors end-to-end backup jobs and sends alert notifications if errors occur.
Benefits	You do not need to perform O&M. This helps you optimize labor costs. HBR fully manages data backup to ensure data security.

- User experience advantages
  HBR provides a user-friendly GUI. In the HBR console, you can view the list of backup plans, disaster recovery records, and recovery points. You can also start disaster recovery drill with one click.

Item	Description
Features	Interfaces for scenarios such as file backup, database backup, and ECS disaster recovery are specifically designed. Step-by-step guidance is provided for backup and disaster recovery.

Item	Description
Advantages	Backup plans, backup points, and recovery points are clearly displayed in the HBR console. This simplifies disaster recovery.
Benefits	The features provided in the HBR console are easy to learn and use. This minimizes the effect of a turnover of O&M staff.

- Security advantages
  HBR provides the immutable backup feature that can improve the security management of your data backup. This feature protects your data against unexpected operations, malicious attacks, and unauthorized backup or restoration and helps meet data security and compliance requirements. HBR allows you to encrypt your data based on Key Management Service (KMS), enable the immutable backup feature, and isolate backup permissions from recovery permissions. For more information, see Enable the security enhancement feature for backup management.

Item	Description
Features	◦ KMS encryption ◦ Immutable backup ◦ Isolation of backup permissions from recovery permissions
Advantages	You can enable KMS encryption and the immutable backup feature in the HBR console with only one click.
Benefits	You can enable the security enhancement features of HBR to improve the security management of your data backup. These features can protect your data against unexpected operations, malicious attacks, and unauthorized backup or restoration to meet your data security and compliance requirements.

The following table describes the advantages of over an on-premises backup system in a self-managed data center or on the cloud.

Item	On-premises backup system	HBR
Permission management	Not supported. No strict permission management is available. Therefore, misoperations such as accidental data deletion may occur.	Supported. HBR uses Resource Access Management (RAM) to grant different permissions to different roles and allow each role to access only authorized resources.
Deduplication and compression	Not supported. Duplicate backup data increases storage costs and lowers the backup speed.	Supported. HBR uses deduplication and compression technologies that are developed by Alibaba Cloud. This can effectively reduce the amount of transmitted data and storage usage, increase the backup speed, and reduce costs.

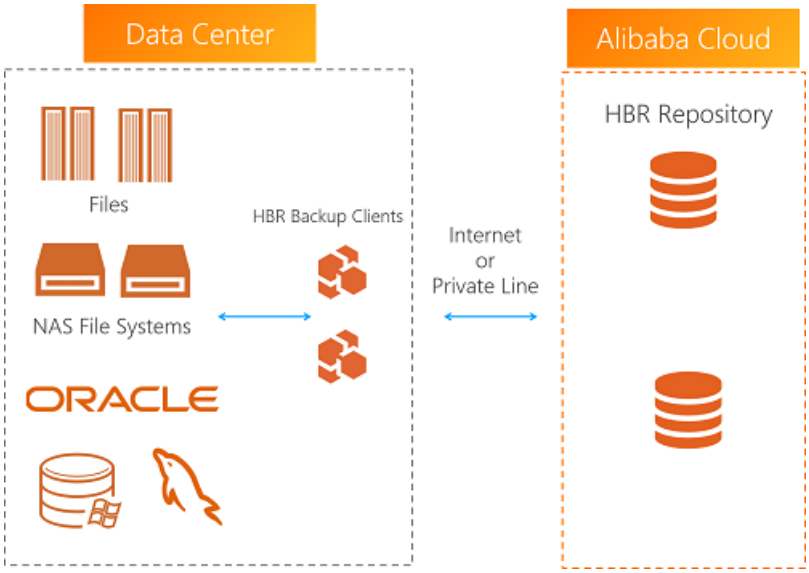
Item	On-premises backup system	HBR
Backup alerting	Not supported. If a backup failure occurs, you must manually track the backup process to identify the failure cause. Otherwise, you may find the backup failure only when you attempt to restore data from the backup.	Supported. HBR provides the backup alerting feature. You can use this feature to send alert notifications to specified contacts if a backup fails or a client is disconnected from a server.
Lifecycle management	You must manually manage the lifecycle of backup data.	HBR automatically manages the lifecycle of backup data.
Remote backup	Not supported.	HBR allows you to create a remote mirror vault for a backup vault. You can use a mirror vault to back up or restore data across regions. For more information, see Back up data across regions.
Data restoration	You must manually restore data from multiple data replicas.	HBR provides backup versions for you to choose when you attempt to restore data. You can also set restore rules.
Management costs	High. You must compile scripts to back up data and dispatch dedicated engineers to manage backups. The complex and difficult O&M reduce resource utilization and increase management costs.	Low. HBR manages your backup data in cloud vaults. You do not need to worry about backup management issues, such as hardware procurement, configuration, cluster scaling, and security.
Data encryption	You must build a system to encrypt data.	HBR uses the Advanced Encryption Standard (AES) 256-bit algorithm or Key Management Service (KMS) to encrypt and transmit data from a backup source and store the backup data in the cloud. During data transmission, HBR also uses HTTPS to encrypt data. For more information, see Enable the security enhancement feature for backup management.

Item	On-premises backup system	HBR
Immutable backup	Not supported.	The immutable backup feature supports the Write Once Read Many (WORM) policy. If you enable this feature, you can write data to all backup vaults only once and read data from the backup vaults multiple times. The feature provides additional protection for your backup vault. For more information, see Enable the security enhancement feature for backup management.
High availability of data	You must manually manage the availability of backup data.	HBR provides the multi-copy redundancy technology and supports zone-redundancy of backup vaults. For more information, see Backup vault for zone-redundant storage (ZRS).

3.Scenarios

You can use Hybrid Backup Recovery (HBR) in multiple scenarios, such as file backup, database backup, fast backup of a large amount of data from Isilon NAS file systems to the cloud, intelligent cloud archive, agentless migration of VMware virtual machines (VMs) to the cloud, agentless backup and disaster recovery of VMware VMs, ECS instance backup across zones or regions, ECS high-performance disaster recovery, and agentless, automatic backup of NAS file systems and OSS buckets.

Back up an on-premises files to the cloud

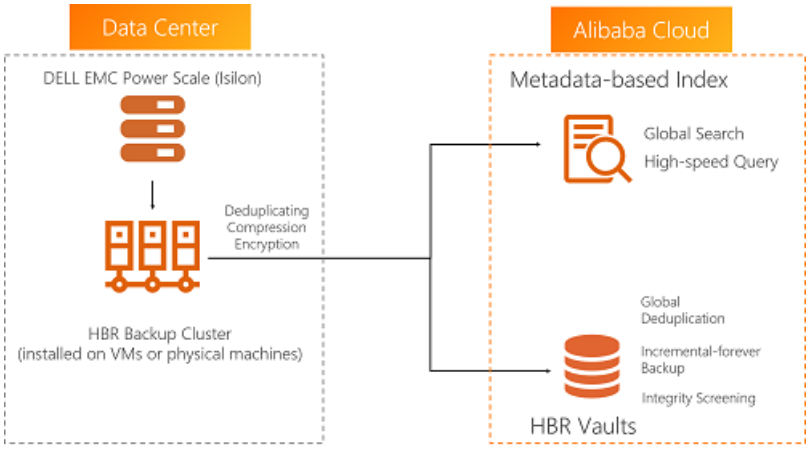


Item	Description
Challenges	• On-premises files scatter in different locations. This complicates backup configuration. • The number of files is huge and the backup requires a long period of time. This does not meet the requirements of the Service Level Agreement (SLA). • The data size is huge and local backup requires large hardware investment.
Solution	• You can use HBR to back up on-premises data to the cloud for simplified, centralized backup management. • You can use HBR to concurrently back up NAS storage systems. This increases the backup speed by more than 300%. • You do not need to purchase or maintain local backup hardware. Backup data is deduplicated and compressed to reduce the storage usage and the bandwidth.
Benefits	• Centralized backup management simplifies backup configuration. • Concurrent backup is performed on a daily basis. The backup frequency exceeds the SLA requirements. • The total cost of ownership (TCO) is reduced by 80%.

Backup on-premises databases to the cloud

Item	Description
Challenges	• The core system of databases depends on simple scripts. This exposes data backups to high risks. • Traditional all-in-one data appliances are complicated to install and the upfront cost is huge. • Geo-redundancy is difficult to build.
Solution	• You can use an HBR backup client to back up your databases to the cloud. • You can connect your databases to Alibaba Cloud over a Virtual Private Network (VPN) or Express Connect circuit to enhance data security.
Benefits	• MySQL, SQL Server, and Oracle databases are all supported. • You do not need to purchase an all-in-one data appliance or perform complicated configuration. • Direct backup to the cloud reduces geo-redundancy costs.

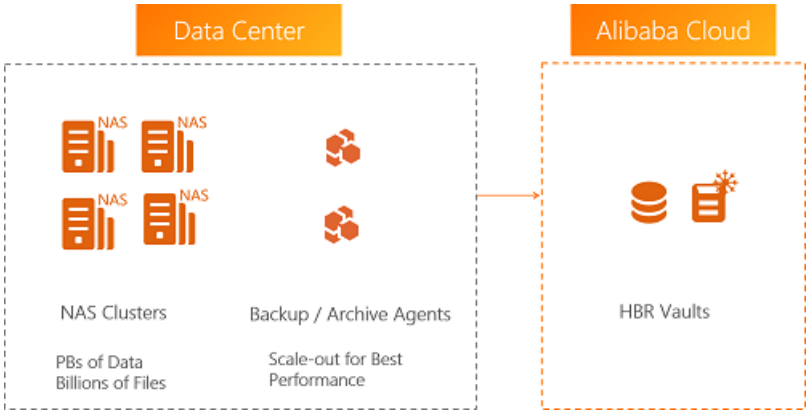
Back up a large amount of data from Isilon NAS storage systems to the cloud



Item	Description
Challenges	• The number of files is huge and the backup requires a long period of time. Each backup may take several days or weeks. • On-premises backup and storage hardware that can accommodate huge data size is usually unaffordable. • Files are difficult to locate in a short time due to the huge data size when you need to restore the files.

Item	Description
Solution	• You can connect HBR to the Isilon Diff API. File scanning is no longer required. This accelerates data backup by more than 1,000%. • You can perform concurrent backup on multiple backup clients to optimize storage and network performance. • You can use the global search feature of HBR to search for files that you want to restore within seconds.
Benefits	• The backup cycle is reduced to once a day to meet your backup requirements. • Global file search improves data management efficiency by more than 500%. • The TCO is reduced by 70%.

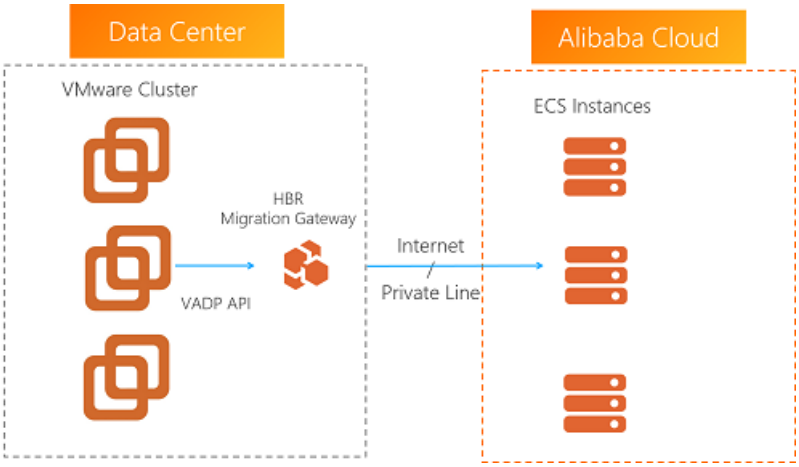
Archive data in the cloud



Item	Description
Challenges	• A large amount of time and cost are required to build and deploy the archive hardware. • You cannot gain insights into your data, configure archive policies, or predict archive performance. • Archived data is difficult to retrieve and inefficient to restore.
Solution	• You can use HBR to analyze the data that you want to archive and visualize data insights in multiple dimensions. Configure archive policies and predict archive performance. • You can store your data to an archive vault at minimal cost. • You can use the global search feature of HBR to locate and restore archived files in a short time.

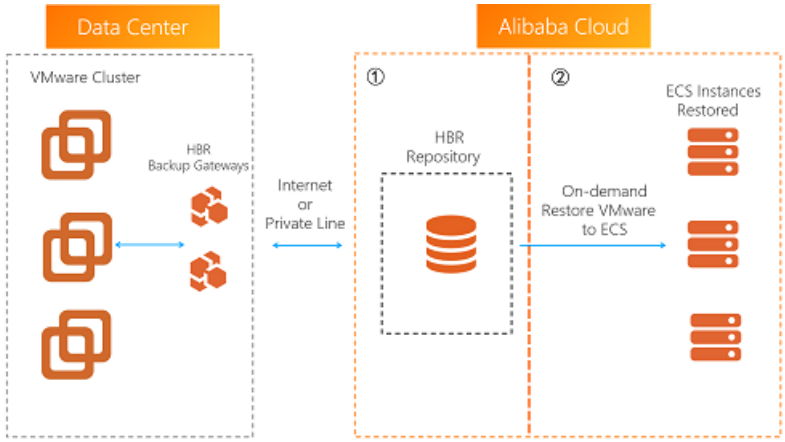
Item	Description
Benefits	• You can configure archive policies based on your business requirements. Archive policies are automatically executed after configuration. • You can search for and restore archived files within seconds. • The TCO is reduced by more than 50%.

Migrate VMware VMs to the cloud in an agentless manner



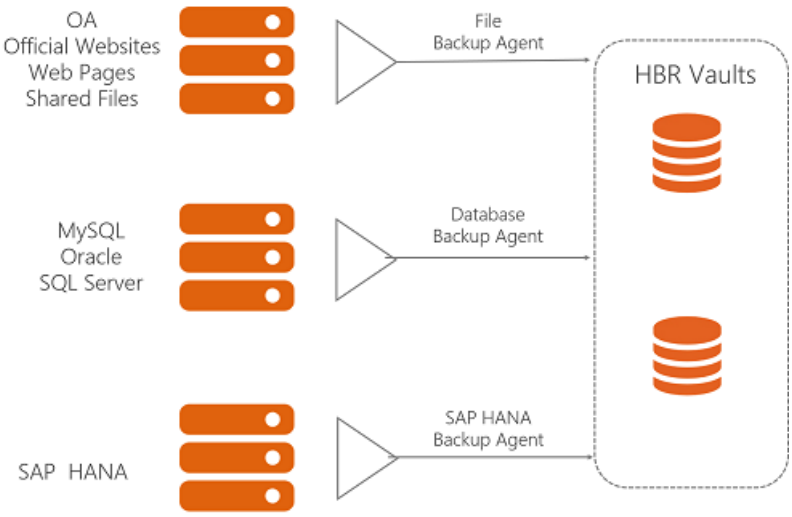
Item	Description
Challenges	• Traditional migration solutions are intrusive to VMware VMs. Therefore, data security may be compromised and the migration process is complex. • Database VMs must be stopped for a long period of time before you can perform a migration for data consistency. • Incremental migration of a large number of files requires a long time.
Solution	• You can use HBR to migrate VMware VMs to the cloud in an agentless and non-intrusive manner. • You can use HBR to perform agentless incremental migration and guarantee data consistency. • You can use HBR to migrate multiple VMs at a time.
Benefits	• You can migrate VMs in a non-intrusive, agentless manner. • You can perform incremental migration with high efficiency. The switchover period for database VMs is reduced to 15 minutes.

Perform backup and disaster recovery of VMware VMs in an agentless manner



Item	Description
Challenges	• Traditional methods that are used to back up VMs require an all-in-one machine, which is complicated to install and configure. • Independent hardware is required for both backup and disaster recovery. This increases costs.
Solution	• You can use HBR to back up VMware VMs to the cloud without the need for backup agents or on-premises hardware devices. • You can restore VMware VM backups to ECS instances on the cloud for disaster recovery.
Benefits	• The TCO is reduced by 80%. • Only one solution is required for backup and disaster recovery.

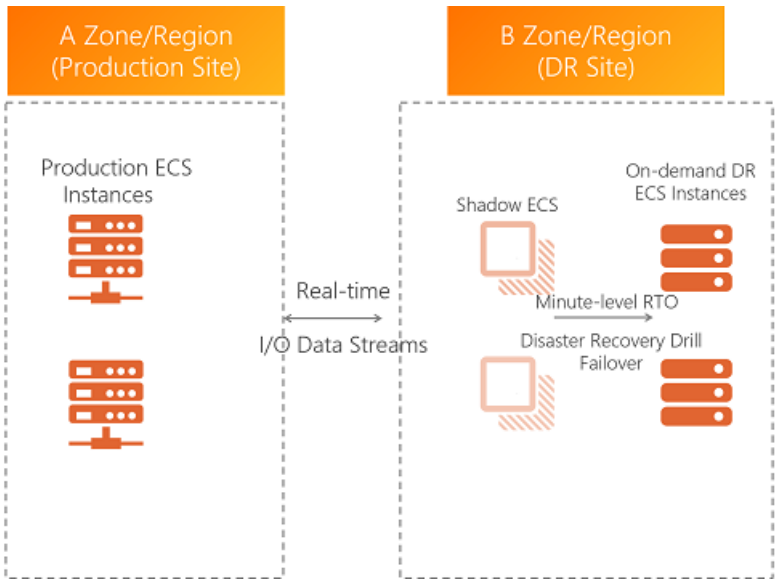
Back up ECS instances



Item	Description

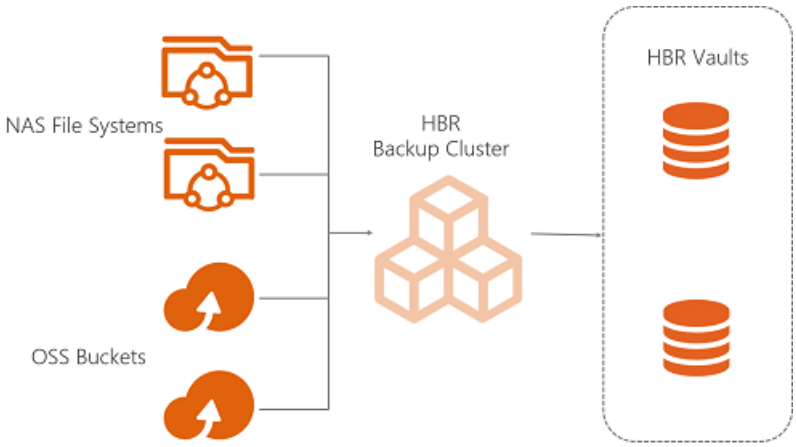
Item	Description
Challenges	• The number of ECS instances is huge and the backup configuration is difficult to manage. • Snapshots cannot be used to protect data by file or database. • Most backup software cannot meet the demanding requirements for database backup. • Backup requirements vary greatly with different data sources. Therefore, backup policies are difficult to configure and backup errors are likely to occur.
Solution	• You can use HBR to back up all types of data that is stored on ECS instances. • You can use HBR to perform full backup, incremental backup, and log backup for the latest and earlier versions of databases deployed on ECS instances. • You can use HBR to back up logs of MySQL and Oracle databases in real time with a near-zero recovery point objective (RPO).
Benefits	• All types of data on ECS instances can be backed up in a unified manner. • The deduplication and compression ratio can reach 5:1 for database backup and 30:1 for file backup. If your backup data is retained for one month, the storage costs are reduced by 60%. • You can use HBR to back up databases on an SAP HANA instance. HBR is an SAP-certified backup service in public cloud. Databases can be backed up at a speed of 500 MB/s and restored at a speed of 260 MB/s. This greatly reduces RTO.

Perform disaster recovery of ECS instances across zones or regions



Item	Description
Challenges	• Low RPO and RTO are required for disaster recovery. Traditional solutions are complicated, unaffordable, and incompatible with cloud platforms. • The disaster recovery process is complex to perform and difficult to drill. Therefore, data integrity is hard to guarantee.
Solution	• HBR allows you to replicate data based on compact disc-recordable (CD-R) to perform high-performance disaster recovery with second-scale RPO and minute-scale RTO. • You can use HBR to perform geo-redundancy of ECS instances without the need to replicate applications. You can configure the disaster recovery with only a few steps and start an application with one click.
Benefits	• RPO is reduced to less than 1 minute and RTO is reduced to less than 15 minutes. • The disaster recovery of an ECS instance is simple and convenient. You can perform recovery drills at any time without affecting your production environment.

Back up NAS file systems or OSS buckets in an automatic and agentless manner



Item	Description
Challenges	• NAS file systems and OSS buckets contain a large amount of data, but does not support scheduled incremental backup. • Traditional solutions require custom scripts or expensive disaster recovery software or ECS instances. The software is complex to install and configure.

Item	Description
Solution	• HBR allows you back up NAS file systems and OSS buckets in an agentless manner. Your ECS resources are not consumed when data is backed up. • Scheduled incremental backups are available to ensure backup efficiency.
Benefits	• You can back up NAS file systems and OSS buckets without the need to consume computing resources. • The incremental backup, deduplication, and compression features can reduce your storage costs by up to 80%. • You can configure backup policies in a simple manner by using the HBR console without the need to perform O&M operations.

4.Service-linked roles for HBR

This topic describes the service-linked roles for Hybrid Backup Recovery (HBR): AliyunServiceRoleForHbrEcsBackup, AliyunServiceRoleForHbrOssBackup, AliyunServiceRoleForHbrNasBackup, AliyunServiceRoleForHbrCsgBackup, AliyunServiceRoleForHbrVaultEncryption, and AliyunServiceRoleForHbrOtsBackup. This topic also describes how to delete these roles.

Background information

HBR needs to access other Alibaba Cloud services to implement a feature. In this case, HBR must assume service-linked roles to obtain required permissions. For more information, see Service-linked roles.
To access Elastic Compute Service (ECS), Virtual Private Cloud (VPC), Object Storage Service (OSS), Apsara File Storage NAS, or Cloud Storage Gateway (CSG), HBR must assume the corresponding service-linked role that is automatically created.

- HBR must assume the AliyunServiceRoleForHbrEcsBackup role so that the ECS backup feature of HBR can access ECS and VPC.
- HBR must assume the AliyunServiceRoleForHbrOssBackup role so that the OSS backup feature of HBR can access OSS.
- HBR must assume the AliyunServiceRoleForHbrNasBackup role so that the NAS backup feature of HBR can access NAS.
- HBR must assume the AliyunServiceRoleForHbrCsgBackup role so that the CSG backup feature of HBR can access CSG.
- To encrypt backup vaults by using Key Management Service (KMS), HBR requires access to KMS. In this case, HBR must assume the AliyunServiceRoleForHbrVaultEncryption role.
- HBR must assume the AliyunServiceRoleForHbrOtsBackup role so that the Tablestore backup feature of HBR can access Tablestore.

Permission policies

This section describes the permission policies that are attached to each service-linked role.

- The following permission policies are attached to the AliyunServiceRoleForHbrEcsBackup role. After HBR assumes the role, HBR can access ECS.

```
{
     "Action": [
       "ecs:RunCommand",
       "ecs:CreateCommand",
       "ecs:InvokeCommand",
       "ecs:DeleteCommand",
       "ecs:DescribeCommands",
       "ecs:StopInvocation",
       "ecs:DescribeInvocationResults",
       "ecs:DescribeCloudAssistantStatus",
       "ecs:DescribeInstances",
       "ecs:DescribeInstanceRamRole",
       "ecs:DescribeInvocations"
     ],
     "Resource": "*",
     "Effect": "Allow"
   },
   {
     "Action": [
```

```
      "Action": [
        "ecs:AttachInstanceRamRole",
        "ecs:DetachInstanceRamRole"
      ],
      "Resource": [
        "acs:ecs:*:*:instance/*",
        "acs:ram:*:*:role/aliyunecsaccessinghbrrole"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "ram:GetRole",
        "ram:GetPolicy",
        "ram:ListPoliciesForRole"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ram:PassRole"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "acs:Service": [
            "ecs.aliyuncs.com"
          ]
        }
      }
    },
    {
      "Action": [
        "ecs:DescribeSecurityGroups",
        "ecs:DescribeImages",
        "ecs:CreateImage",
        "ecs:DeleteImage",
        "ecs:DescribeSnapshots",
        "ecs:CreateSnapshot",
        "ecs:DeleteSnapshot",
        "ecs:DescribeSnapshotLinks",
        "ecs:DescribeAvailableResource",
        "ecs:ModifyInstanceAttribute",
        "ecs:CreateInstance",
        "ecs:DeleteInstance",
        "ecs:AllocatePublicIpAddress",
        "ecs:CreateDisk",
        "ecs:DescribeDisks",
        "ecs:AttachDisk",
        "ecs:DetachDisk",
        "ecs:DeleteDisk",
        "ecs:ResetDisk",
        "ecs:StartInstance",
```

```
        "ecs:StopInstance",
        "ecs:ReplaceSystemDisk",
        "ecs:ModifyResourceMeta"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
```

- The following permission policies are attached to the AliyunServiceRoleForHbrEcsBackup role. After HBR assumes the role, HBR can access VPC.

```
{
      "Action": [
        "vpc:DescribeVpcs",
        "vpc:DescribeVSwitches"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
```

- The following permission policies are attached to the AliyunServiceRoleForHbrOssBackup role. After HBR assumes the role, HBR can access OSS.

```
{
      "Action": [
        "oss:ListObjects",
        "oss:HeadBucket",
        "oss:GetBucket",
        "oss:GetBucketAcl",
        "oss:GetBucketLocation",
        "oss:GetBucketInfo",
        "oss:PutObject",
        "oss:CopyObject",
        "oss:GetObject",
        "oss:AppendObject",
        "oss:GetObjectMeta",
        "oss:PutObjectACL",
        "oss:GetObjectACL",
        "oss:PutObjectTagging",
        "oss:GetObjectTagging",
        "oss:InitiateMultipartUpload",
        "oss:UploadPart",
        "oss:UploadPartCopy",
        "oss:CompleteMultipartUpload",
        "oss:AbortMultipartUpload",
        "oss:ListMultipartUploads",
        "oss:ListParts"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
```

- The following permission policies are attached to the AliyunServiceRoleForHbrNasBackup role. After HBR assumes the role, HBR can access NAS.

```
{
      "Action": [
        "nas:DescribeFileSystems",
        "nas:CreateMountTargetSpecial",
        "nas:DeleteMountTargetSpecial",
        "nas:CreateMountTarget",
        "nas:DeleteMountTarget",
        "nas:DescribeMountTargets",
        "nas:DescribeAccessGroups"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
```

- The following permission policies are attached to the AliyunServiceRoleForHbrCsgBackup role. After HBR assumes the role, HBR can access CSG.

```
{
      "Action": [
        "hcs-sgw:DescribeGateways"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
```

- The following permission policies are attached to the AliyunServiceRoleForHbrVaultEncryption role. After HBR assumes the role, HBR can access KMS.

```
{
 "Statement": [
 {
  "Action": "ram:DeleteServiceLinkedRole",
  "Resource": "*",
  "Effect": "Allow",
  "Condition": {
   "StringEquals": {
    "ram:ServiceName": "vaultencryption.hbr.aliyuncs.com"
   }
  }
 },
 {
  "Action": [
  "kms:Decrypt"
  ],
  "Resource": "*",
  "Effect": "Allow"
 }
 ],
 "Version": "1"
}
```

- The following permission policies are attached to the AliyunServiceRoleForHbrOtsBackup role. After HBR assumes the role, HBR can access Tablestore.

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "otsbackup.hbr.aliyuncs.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ots:ListTable",
        "ots:CreateTable",
        "ots:UpdateTable",
        "ots:DescribeTable",
        "ots:BatchWriteRow",
        "ots:CreateTunnel",
        "ots:DeleteTunnel",
        "ots:ListTunnel",
        "ots:DescribeTunnel",
        "ots:ConsumeTunnel",
        "ots:GetRange",
        "ots:ListStream",
        "ots:DescribeStream"
      ],
      "Resource": "*"
    }
  ]
}
```

Delete a service-linked role

You may need to delete service-linked roles to ensure security. For example, if you no longer need to use the ECS backup feature, you can delete the AliyunServiceRoleForHbrEcsBackup role.

> **Notice**
>
> - Before you delete the AliyunServiceRoleForHbrEcsBackup, AliyunServiceRoleForHbrOssBackup, AliyunServiceRoleForHbrNasBackup, or AliyunServiceRoleForHbrCsgBackup role, make sure that no backup vault exists within the current account. Otherwise, the role fails to be deleted.
> - Before you delete the AliyunServiceRoleForHbrVaultEncryption role, make sure that no KMS-encrypted backup vault exists within the current account. Otherwise, the role fails to be deleted.

To delete the AliyunServiceRoleForHbrEcsBackup role, perform the following steps:

1. Log on to the RAM console.

2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, enter AliyunServiceRoleForHbrEcsBackup in the search box to find the role.
4. Click **Delete** in the **Actions** column.
5. In the **Delete Role** message, click **OK**.

If you want to delete the AliyunServiceRoleForHbrOssBackup, AliyunServiceRoleForHbrNasBackup, or AliyunServiceRoleForHbrCsgBackup role, enter the corresponding role name in the search box.

5.Backup metrics and features

Different backup sources support different metrics and features, including the minimum backup granularity, minimum backup cycle, maximum retention period, and real-time backup. This topic provides an overview of the metrics and features that each backup source supports, and the backup speed and recovery speed.

Backup metrics and features

Category	Backup source	Minimum backup granularity	Minimum backup cycle	Maximum retention period	Real-time backup	Remote backup	Account permission isolation
Backup of on-premises data to the cloud	File	File	Hour	Permanent	Not supported	Supported	Supported
	NAS	File	Hour	Permanent	Not supported	Supported	Supported
	VMware	Virtual machine	Hour	999 years	Not supported	Not supported	Supported
	SQL Server	Database	Hour Minute (for logs)	Permanent	Not supported	Supported	Supported
Cloud backup	MySQL	Instance	Hour	999 years	Supported	Not supported	Supported
	Oracle	Table	Hour	999 years	Supported	Not supported	Supported
	SQL Server	Database	Hour Minute (for logs)	999 years	Not supported	Not supported	Supported
	SAP HANA	Database	Hour Minute (for logs)	Permanent	Not supported	Supported	Supported
	File	File	Hour	Permanent	Not supported	Supported	Supported
	NAS	File	Day	Permanent	Not supported	Supported	Supported

Category	Backup source	Minimum backup granularity	Minimum backup cycle	Maximum retention period	Real-time backup	Remote backup	Account permission isolation
	OSS	Prefix	Day	Permanent	Not supported	Supported	Supported

allows you to configure different backup or recovery permissions for different accounts. For more information, see Create a RAM user and grant permissions to the RAM user.

Backup speed and recovery speed

The backup speed and recovery speed of are obtained in a test environment. The values are provided for reference only. For more information, see Backup speed and recovery speed.

6.Limits

This topic describes the limits that you must take note of when you use .

Database backup

- On-premises database servers must be connected to virtual private clouds (VPCs) by using VPNs or Express Connect circuits. You must also make sure that you can use an HBR client to access one of the following CIDR blocks from an on-premises server: 100.64.0.0/10, 100.64.0.0/11, and 100.96.0.0/11.
- HBR supports a limited number of database versions, operating systems, and backup features. For more information, see Database backup.

File backup

- Backup clients for Windows support Volume Shadow Copy Service (VSS). You can create only one VSS snapshot at a time. If you use VSS, you cannot back up files from multiple paths or Universal Naming Convention (UNC) paths. You cannot use wildcards (*) or exclude files.
- If HBR attempts to back up a file on which HBR has read permissions but the file is being modified by other applications, an incomplete backup occurs. You must ensure the integrity of backup data at the application layer.
- If HBR attempts to back up a file on which HBR does not have read permissions or the file is locked by other processes, an incomplete backup occurs. The status of the backup job is displayed as partially completed when the job ends.

VMware VM backup

- You must install a vSphere Web Client whose version is 5.5, 6.0, 6.5, or 6.7 on each virtual machine for which you want to create a backup file.
- A vCenter Server and an ESXi hypervisor must allow access from a backup gateway by using a fully qualified domain name (FQDN) or an IP address.
- If you want to back up a virtual machine (VM), make sure that no snapshots are created for the VM. Otherwise, the following message appears when you select the VM: **You cannot back up the virtual machine because you have already created a snapshot.** If a snapshot exists, you must delete it before you can back up the VM.
- You cannot back up VMs that have SCSI devices because vSphere VMs do not support shared SCSI devices.
- The name of a VM that you want to back up cannot contain the following characters: ` ^ ~ = ; ! / ( ) [ ] { } @ $ \ & # % +
- If you use Changed Block Tracking (CBT) to perform an incremental backup for a VM, the backup attempt fails in the following scenarios:
  - The hardware version of the VM is earlier than version 7.
  - CBT is disabled on the VM.
  - The disk of the VM uses raw device mapping (RDM) in physical compatibility mode.
  - The disk mode of the VM is independent_persistent or independent_nonpersistent.

SAP HANA backup

You can install only one SAP HANA instance on an ECS instance. Otherwise, the following error message appears: Failed to install SAP HANA.

NAS backup

NAS backup does not support access control lists (ACLs) for Server Message Block (SMB) file systems. For more information, see Features.

OSS backup

- HBR cannot back up or restore symbolic links, object ACLs, or objects in archive buckets.
- To improve the performance of incremental backup, HBR uses the latest OSS inventory list within the previous 7 days to back up data.
  The system may require a short period of time to generate an OSS inventory list. When you use the OSS inventory list, take note of the following limits:
  - If no inventory list is detected by a running backup job, the backup job fails.
  - If a backup job detects that the OSS inventory list remains the same as the OSS inventory list for the previous backup, the backup job fails.
  - If a backup job is triggered, HBR uses only the latest OSS inventory list to back up data. After a backup job is completed, the objects that you add to the OSS inventory list are backed up in the next backup cycle.
  - The interval at which backup jobs are performed must be greater than or equal to the interval at which OSS inventory lists are generated. This way, you can use an OSS inventory list each time you run a backup job.

ECS disaster recovery

If you use the ECS disaster recovery feature, you must take note of the limits on operating systems, architectures, databases, and applications. For more information, see Limits on ECS disaster recovery.

VMware disaster recovery

Before you restore a VMware VM to an ECS instance, read the following limits on the operating system and VMware platform of the ECS instance.

- Windows Server

Item	Description
System limits	○ You must verify the integrity of file systems. ○ You cannot modify critical system files. ○ You must make sure that the system disk has sufficient free space. ○ The configured system disk size must range from 40 GiB to 500 GiB. ○ You must make sure that the logon password for the administrator account meets the complexity requirements. The password must be 8 to 30 characters in length and must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. The following special characters are supported: `( ) ` ~ ! @ # $ % ^ & * - _ + = | { } [ ] : ; ' < > , . ? /`. The password cannot start with a forward slash (/).

Item	Description
Unsupported items	◦ You cannot install the QEMU Guest Agent in the system. If the QEMU Guest Agent is installed, some services that ECS requires may become unavailable. ◦ The following operating system versions are not supported: ▪ Windows XP ▪ Windows 8 ▪ Windows 8.1 ▪ Windows 10 ◦ You cannot install Community Edition virtio drivers in Windows Server operating systems. If Community Edition virtio drivers are installed, you must remove the read-only property of the following files: ▪ *C:\Windows\System32\drivers\netkvm.sys* ▪ *C:\Windows\System32\drivers\balloon.sys* ▪ *C:\Windows\System32\drivers\vioser.sys* ▪ *C:\Windows\System32\drivers\viostor.sys* ▪ *C:\Windows\System32\drivers\pvpanic.sys*

- Linux

Item	Description

Item	Description
System limits	○ You must verify the integrity of file systems. ○ You cannot modify critical system files such as */sbin*, */bin*, and */lib**. ■ You cannot modify */etc/issue**. Otherwise, the distribution of the operating system cannot be identified by ECS and the instance operating system cannot be created. ■ You cannot modify */boot/grub/menu.lst*. Otherwise, the ECS instance cannot be started. ■ You cannot modify */etc/fstab*. Otherwise, abnormal partitions cannot be loaded and the ECS instance cannot be started. ■ You cannot set */etc/shadow* to read-only. Otherwise, the password file cannot be modified and the instance operating system cannot be created. ■ You cannot modify */etc/selinux/config* to enable SELinux. Otherwise, the instance operating system cannot be started. If you need to enable SELinux, see Enable or disable SELinux. ○ You must make sure that the system disk has sufficient free space. ○ You must enable Dynamic Host Configuration Protocol (DHCP). ○ You must install Xen or KVM virtualization drivers. For more information, see Install the virtio driver. ○ You must install cloud-init to configure the hostname, NTP repositories, and YUM repositories. For more information, see Install cloud-init. ○ You must make sure that the logon password for the root account meets the complexity requirements. The password must be 8 to 30 characters in length and must contain three of the following character types: lowercase letters, uppercase letters, digits, and special characters. The following special characters are supported: `( ) ` ~ ! @ # $ % ^ & * - _ + = | { } [ ] : ; ' < > , . ? /` . ○ The GRUB version of the operating system must meet the following requirements: ■ If the VM runs Linux, you must upgrade GRUB to V1.99 or later. ■ If the VM runs Linux of an earlier version, such as CentOS 5 or Red Hat 5, you must upgrade GRUB to V1.99 or later.

Item	Description
Unsupported items	○ You can use only a single network interface to establish connections. ○ IPv6 addresses are not supported. ○ You cannot adjust system disk partitions. Only disks with a single root partition are supported. ○ You cannot install the QEMU Guest Agent in the system. If the QEMU Guest Agent is installed, some services that ECS requires may become unavailable. ○ You cannot create system disk partitions (the root partitions) across disks by using Logical Volume Manager (LVM). If you do so, the ECS instance may not be able to start.

- VMware platform

Item	Description
vCenter version	Only vCenter Server 5.5, 6.0, 6.5, 6.7, and 7.0 are supported. A vCenter Server and an ESXi hypervisor must allow access from a migration gateway by using a fully qualified domain name (FQDN) or an IP address.

VMware VM migration

HBR provides non-intrusive, agentless, and full-copy migration for VMware VMs. HBR migrates data by using VMware VM snapshots and reading data from disks. These features allow you to migrate all the data that is stored on the disks of a VMware VM to the disks of an ECS instance. Before you migrate a VMware VM, read the following limits on the operating system and VMware platform of the ECS instance.

- Windows Server

Item	Description
System limits	○ You must verify the integrity of file systems. ○ You cannot modify critical system files. ○ You must make sure that the system disk has sufficient free space. ○ The configured system disk size must range from 40 GiB to 500 GiB. ○ You must make sure that the logon password for the administrator account meets the complexity requirements. The password must be 8 to 30 characters in length and must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. The following special characters are supported: `( ) ` ~ ! @ # $ % ^ & * - _ + = | { } [ ] : ; ' < > , . ? /`. The password cannot start with a forward slash (/).

Item	Description
Unsupported items	◦ You cannot install the QEMU Guest Agent in the system. If the QEMU Guest Agent is installed, some services that ECS requires may become unavailable. ◦ The following operating system versions are not supported: ■ Windows XP ■ Windows 8 ■ Windows 8.1 ■ Windows 10 ◦ You cannot install Community Edition virtio drivers in Windows Server operating systems. If Community Edition virtio drivers are installed, you must remove the read-only property of the following files: ■ *C:\Windows\System32\drivers\netkvm.sys* ■ *C:\Windows\System32\drivers\balloon.sys* ■ *C:\Windows\System32\drivers\vioser.sys* ■ *C:\Windows\System32\drivers\viostor.sys* ■ *C:\Windows\System32\drivers\pvpanic.sys*

- Linux

Item	Description

Item	Description
System limits	◦ You must verify the integrity of file systems. ◦ You cannot modify critical system files such as */sbin*, */bin*, and */lib**. ■ You cannot modify */etc/issue**. Otherwise, the distribution of the operating system cannot be identified by ECS and the instance operating system cannot be created. ■ You cannot modify */boot/grub/menu.lst*. Otherwise, the ECS instance cannot be started. ■ You cannot modify */etc/fstab*. Otherwise, abnormal partitions cannot be loaded and the ECS instance cannot be started. ■ You cannot set */etc/shadow* to read-only. Otherwise, the password file cannot be modified and the instance operating system cannot be created. ■ You cannot modify */etc/selinux/config* to enable SELinux. Otherwise, the instance operating system cannot be started. If you need to enable SELinux, see Enable or disable SELinux. ◦ You must make sure that the system disk has sufficient free space. ◦ You must enable Dynamic Host Configuration Protocol (DHCP). ◦ You must install Xen or KVM virtualization drivers. For more information, see Install the virtio driver. ◦ You must install cloud-init to configure the hostname, NTP repositories, and YUM repositories. For more information, see Install cloud-init. ◦ You must make sure that the logon password for the root account meets the complexity requirements. The password must be 8 to 30 characters in length and must contain three of the following character types: lowercase letters, uppercase letters, digits, and special characters. The following special characters are supported: `( ) ` ~ ! @ # $ % ^ & * - _ + = | { } [ ] : ; ' < > , . ? /`. ◦ The GRUB version of the operating system must meet the following requirements: ■ If the VM runs Linux, you must upgrade GRUB to V1.99 or later. ■ If the VM runs Linux of an earlier version, such as CentOS 5 or Red Hat 5, you must upgrade GRUB to V1.99 or later.

Item	Description
Unsupported items	○ You can use only a single network interface to establish connections. ○ IPv6 addresses are not supported. ○ You cannot adjust system disk partitions. Only disks with a single root partition are supported. ○ You cannot install the QEMU Guest Agent in the system. If the QEMU Guest Agent is installed, some services that ECS requires may become unavailable. ○ You cannot create system disk partitions (the root partitions) across disks by using Logical Volume Manager (LVM). If you do so, the ECS instance may not be able to start.

- VMware platform

Item	Description
vCenter version	Only vCenter Server 5.5, 6.0, 6.5, 6.7, and 7.0 are supported. A vCenter Server and an ESXi hypervisor must allow access from a migration gateway by using a fully qualified domain name (FQDN) or an IP address.

7.Security and compliance

7.1. Access control

supports user-based Resource Access Management (RAM) policies and temporary access authorization based on Security Token Service (STS). These features allow you to manage access permissions and control access to Hybrid Backup Recovery (HBR) resources.

User-based RAM policies

Alibaba Cloud RAM is a service that helps control access to resources. You can configure RAM policies based on the user. You can configure RAM policies to manage users, such as employees, systems, and applications, and grant permissions on the required resources to a user.

A RAM policy is in the JSON format. You can write a RAM policy that includes the Action, Effect, Resource, and Condition elements in the Statement section. You can add multiple statements to a policy to implement flexible authorization. For more information, see RAM overview.

Temporary access authorization based on STS

RAM policies allow you to access resources for a long period of time. If you need to access resources only for a short period of time, you can use STS to create temporary credentials. You can use STS to generate temporary AccessKey pairs and tokens. You can send these credentials to temporary users to access resources. The permissions that are obtained by using STS are strictly restricted and have time limits. Therefore, the leak of temporary credentials does not significantly affect the system security.

You can use STS to authorize temporary access to resources. You can also use STS to create an access credential that has a custom validity period and custom permissions for a third-party application or a RAM user.

7.2. Data encryption

supports backup-source encryption and encryption in transit based on the SSL or TLS protocol. These features help protect cloud data from potential security risks.

Backup-source encryption

allows you to use Key Management Service (KMS) to encrypt data at rest. Alibaba Cloud KMS is a secure and easy-to-use management service. You can use KMS to ensure the privacy, integrity, and availability of your keys at a low cost. KMS allows you to use the keys in a secure and convenient manner. You need only to focus on how to efficiently use these keys to encrypt or decrypt data. You can view and manage the keys in the KMS console. For more information, see Overview.

Encrypt data in transit based on the SSL or TLS protocol

supports access over HTTP and HTTPS. SSL or TLS is a Layer 4 protocol that helps ensure data privacy and data integrity between two communication applications.

8.Supported resources

This topic describes the servers, operating systems, and databases that are supported by .

Servers

Server type	Support backup source and version
Physical server	• File backup: supported • Database backup: MySQL, Oracle, and SQL Server
VM	• File backup: supported • Image backup: vSphere 5.5, vSphere 6.0, vSphere 6.5, vSphere 6.7, and vSphere 7.0
ECS instance	• File backup: supported • SAP HANA backup: SAP HANA 2.0 • Database backup: MySQL, Oracle, and SQL Server

Operating systems

Operating system	Supported version
Windows	Windows 7, 8, and 10
Windows Server	Windows Server 2008 R2, 2012, 2012 R2, 2016, and 2019
RHEL	RHEL 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 7.8, 8, 8.1, and 8.2
CentOS	CentOS 6.5, 6.9, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, and 8.3
Ubuntu	Ubuntu 14.04, 16.04, 18.04, and 20.04
SUSE Linux Enterprise Server	SUSE Linux Enterprise Server 11, 12, and 15
Alibaba Cloud Linux	2, 3

Databases

Database	Supported version
MySQL	MySQL 4.1, 5, 5.0, 5.1, 5.4, 5.5, 5.6, 5.7, and 8.0
Oracle	Oracle 9i, 10g, 11g, 12c, 18c, 19c, Data Guard 11g, and Data Guard 12c
SQL Server	SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016 (RTM), 2017, and 2019

For more information, see Database backup.

9.Supported regions

A region is a geographical area where data centers reside. If Hybrid Backup Recovery (HBR) is available in a region, all the features of HBR are available in the region. This topic describes the regions that are supported by HBR.

Notice The regions supported by backup features may vary with the data sources. You can log on to the HBR console to view the supported regions. If a new feature is available for public preview, the HBR console shows the regions where you can use the feature.

The following table shows the relationships between regions, cities, and region IDs.

Region	City	Region ID
China (Qingdao)	Qingdao	cn-qingdao
China (Beijing)	Beijing	cn-beijing
China (Zhangjiakou)	Zhangjiakou	cn-zhangjiakou
China (Hohhot)	Hohhot	cn-huhehaote
China (Hangzhou)	Hangzhou	cn-hangzhou
China (Shanghai)	Shanghai	cn-shanghai
China (Shenzhen)	Shenzhen	cn-shenzhen
China (Chengdu)	Chengdu	cn-chengdu
China (Hong Kong)	Hong Kong	cn-hongkong
Singapore (Singapore)	Singapore	ap-southeast-1
Australia (Sydney)	Sydney	ap-southeast-2
Malaysia (Kuala Lumpur)	Kuala Lumpur	ap-southeast-3
Indonesia (Jakarta)	Jakarta	ap-southeast-5
Philippines(Manila)	Manila	ap-southeast-6
India (Mumbai)	Mumbai	ap-south-1
Japan (Tokyo)	Tokyo	ap-northeast-1
US (Silicon Valley)	Silicon Valley	us-west-1
US (Virginia)	Virginia	us-east-1
Germany (Frankfurt)	Frankfurt	eu-central-1

Region	City	Region ID
UAE (Dubai)	Dubai	me-east-1

Before you use HBR to back up local servers, ECS files, or databases, you must install HBR clients on the objects that you want to back up. HBR clients are used to establish communication and transmit messages between HBR and the objects that you want to back up. For more information about the endpoints and ports that can be accessed by HBR clients, see What are the endpoints and ports that can be accessed by HBR clients?